



KRITIS-Dachgesetz und NIS2-Richtlinie prägen Zukunft der Unternehmenssicherheit

Hybride Risiken setzen Wirtschaft und kritische Infrastrukturen (KRITIS) immer stärker unter Druck: Der jährliche Schaden summiert sich auf mittlerweile 289 Milliarden Euro – mehr als das Doppelte des NRW-Landeshaushaltes. Um die Resilienz zu stärken, hat die Politik das KRITIS-Dachgesetz und die NIS2-Richtlinie verabschiedet. Diese verpflichten rund 30.000 Unternehmen und Betreiber zu Business Continuity Management (BCM) sowie integrierter Sicherheit – und stellen gerade den Mittelstand vor riesige Herausforderungen.

Die Gesetze werden damit maßgeblich die Zukunft der Unternehmens- und Betreiber-Sicherheit prägen. Sie verfolgen folgende Ziele: hohe und einheitliche Standards sowohl bei physischer Sicherheit (KRITIS-Dachgesetz) als auch bei Netzwerk- und Informationssicherheit (NIS2) zu implementieren sowie die beiden Sektoren gemäß Allgefahrenansatz eng zu verzahnen. So sollen Kernbereiche der Wirtschaft und öffentlichen Daseinsvorsorge umfassend gegen analoge und digitale Sabotage, Spionage etc. geschützt werden.

„BCM und ganzheitliche Sicherheit sind das Gebot der Stunde, um die eigene Resilienz zu forcieren“, unterstreicht Dirk H. Bürhaus, Geschäftsführender Direktor in der KÖTTER Security Gruppe. Denn acht von zehn Unternehmen, bei denen es z. B. durch Cybercrime zur Großschadenslage gekommen ist, melden binnen spätestens zwei Jahren Insolvenz an. „Jeder und jedem muss daher klar sein, was die Stunde geschlagen hat. Es geht nicht um einfache Versicherungsschäden. Es steht die Zukunft gesamter Firmen auf dem Spiel.“

Einhergehend damit appelliert KÖTTER Sicherheitsbeirats-Mitglied Fritz Rudolf Körper an Firmeninhaber und Führungsebenen, den hohen Stellenwert von Sicherheit mehr denn je anzuerkennen. „Statt Sicherheit nach Kostenaspekten zu bewerten, sollte sie als Wertschöpfungsfaktor verstanden werden“, erklärt der Staatssekretär a. D. „Das gerade in Zeiten von Künstlicher Intelligenz, die Kriminellen neue Angriffsmöglichkeiten verschafft“ (lesen Sie dazu bitte auch die Rückseite).

„Sicherheit schafft Wertschöpfung für Firmen und KRITIS-Betreiber“

Insolvenzen infolge von Cyberattacken, Produktionsstillstände nach Brandanschlägen. Wie groß sind die Bedrohungen?

Dirk H. Bürhaus: Gemäß Bitkom-Studie sind knapp neun von zehn Unternehmen in Deutschland durch analoge und digitale Spionage bzw. Sabotage betroffen. Das jährliche Schadensvolumen, von dem rund 70 % auf Cybercrime entfallen, hat sich in zehn Jahren mehr als verfünffacht auf 289 Milliarden Euro. Neben der immer größeren Schlagkraft krimineller Akteure, die sich KI zunutze machen, ergibt sich dieser Trend u. a. aus der fortschreitenden Vernetzung von Standorten, Anlagen und IT-Systemen.

Die Politik hat hierauf mit KRITIS-Dachgesetz und NIS2-Richtlinie reagiert. Worin liegt deren besondere Wichtigkeit?

Fritz Rudolf Körper: Mit dem im März in Kraft getretenen KRITIS-Dachgesetz und der bereits seit vergangenem Dezember geltenden NIS2-Richtlinie hat Deutschland EU-Vorgaben in nationales Recht überführt. Beide Gesetze senden das eindeutige Signal an Wirtschaft und KRITIS-Betreiber, dass Sicherheit oberste Priorität haben muss. Physischer Schutz und Cybersecurity sind jetzt Unternehmens-Kernpflicht.

Bürhaus: Lassen Sie mich dies bitte noch ergänzen. Mit dem KRITIS-Dachgesetz werden beide Sektoren erstmals eng miteinander verknüpft. Dieser Allgefahrenansatz hat größte Relevanz, da Sicherheit immer integrativ zu betrachten ist. Unternehmen müssen das Silodenken überwinden, bei dem eine Abteilung den physischen Schutz steuert und eine andere die Cyberabwehr übernimmt.

Wen betreffen die Gesetzeswerke?

Körper: Allein etwa rund 2.000 Betreiber kritischer Infrastrukturen in Deutschland fallen unter das KRITIS-Dachgesetz. Der

Wirkungskreis der NIS2-Richtlinie ist noch weitgehender: Sie betrifft hierzu-lande knapp 30.000 Unternehmen aus 18 Branchen und Sektoren.

Was sind die inhaltlichen Kernelemente?

Körper: Erstens: Alle betroffenen Akteure unterliegen einer Registrierungspflicht – gemäß KRITIS-Dachgesetz beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK, bzw. entsprechend NIS2 beim Bundesamt für Sicherheit in der Informationstechnik, BSI. Zweitens: Sie müssen über ein funktionierendes Business-Continuity-Management verfügen – also nachhaltige Strukturen zur Aufrechterhaltung des Betriebes in der Folge eines Notfalls implementieren. Und das inklusive aktivem Krisenmanagement. Drittens: Aus dieser Architektur resultieren konkrete Anforderungen an physischen bzw. IT-Schutz, aber auch Vorschriften zu Meldepflichten, Dokumentationen oder Audits.

„Physischer Schutz und Cybersecurity sind jetzt Unternehmens-Kernpflicht.“

Fritz Rudolf Körper

Gibt es weitere Faktoren?

Bürhaus: NIS2 richtet den Fokus zum Beispiel auf die häufig vernachlässigte Kontrolle von Beschaffungsprozessen. Sie ist gerade bei IT-Komponenten von elementarer Relevanz, da diese meist aus dem Ausland kommen und damit Einfallstor für Spionage sind. Weiteres Beispiel: NIS2 verpflichtet Firmen zu Kryptografie, also Verschlüsselung, als Bestandteil des Risikomanagements.

Lassen Sie uns dies noch stärker auf die Praxis münzen. Wie sehen Registrierung, Dokumentation und Meldepflichten konkret aus?

Körper: Die Frist zur NIS2-Registrierung beim BSI ist bereits Anfang März abgelaufen. Betroffene Unternehmen sollten diese also rasch nachholen, da Bußgelder drohen. Zudem steht gemäß KRITIS-Dachgesetz für Betreiber die Registrierung beim



Fritz Rudolf Körper, Mitglied des KÖTTER Sicherheitsbeirates und früherer Parlamentarischer Staatssekretär im Bundesministerium des Innern.

BBK an. Dokumentations-Vorgaben betreffen etwa bauliche Komponenten im Rahmen von Begehungsprotokollen. Ähnlich verhält es sich auch mit Blick auf das Archivieren von Schulungsprotokollen. Kommt es dann zu einem relevanten Vorfall, hat die Meldung binnen 24 Stunden an BBK oder BSI zu erfolgen – je früher, umso besser.

Und was müssen Resilienzanalysen sowie daraus folgende BCM-Bausteine zum Beispiel umfassen?

Bürhaus: Bevor Sicherheitsmaßnahmen greifen, braucht es ein präzises Bild der Ausgangslage. Basis ist daher immer eine Asset-basierte Risikoanalyse. Sie zeigt auf, welche Prozesse und Ressourcen – von Gebäudekomponenten bis zu IT-Systemen – verwundbar sind und wie sie abgesichert werden können. Daraus leiten wir passgenaue Schutzkonzepte ab. Diese reichen von Sicherheitsdiensten und -technik wie etwa Streifengängen und Zutrittskontrollsystemen über Social-Media-Monitoring und Cyber-Defense bis zu Awareness-Schulungen, Notfallübungen und Penetrations-Tests. Im Krisenfall können wir zudem die operative, reversionssichere Lageführung übernehmen, inklusive Notfallkommunikation.

Ergänzende Infos zur neuen NIS2-Richtlinie finden Sie hier:



Körper: Lassen Sie mich hier einhaken. All dies ist notwendig, weil der Nachholbedarf in Sachen Sicherheit gerade im Mittelstand riesig ist. Beispiele: Auf vielen Arealen weisen IP-Kameras solche Sicherheitslücken auf, dass Kriminelle sie hacken können, die Steuerung übernehmen oder sich im Zweifel weiteren Zugang zum Netzwerk verschaffen. Ähnlich sieht es bei digital gesteuerten Aufzügen aus. Gleichzeitig haben Brandanschläge auf Strommasten und Kabelbrücken nachhaltig verdeutlicht, wie physisch verwundbar unsere Infrastrukturen sind und welche weitgehenden Folgen daraus resultieren.

Sie sprechen den Blackout an. Welche physischen Schutzbausteine folgen daraus explizit – etwa für die Sicherheit von Umspannwerken oder Produktionen?

Bürhaus: Priorität hat die gezielte bauliche Sicherung durch Mauern, Zäune etc. mit geeigneter Sicherheitstechnik inklusive Leitstellen-Aufschaltung. Ziel: Tätern den Zugang zu erschweren und damit einen Sabotageakt zu behindern. Gleichzeitig gewinnen Verantwortliche so nach der Täter-Detektion wertvolle Zeit für Intervention und Notfallmaßnahmen. Dies reduziert Schadensrisiken genauso wie „Security by Design“, also Sicherheitsmaßnahmen bereits bei Standortplanungen. Diese Komponenten wirken nicht allein gegen physische Angriffe, sondern auch gegen Cybercrime und damit ganz im BCM-Sinn.

Spannender Brückenschlag. Worin liegt der hohe Stellenwert physischer Komponenten gegen Cyberangriffe, etwa bei einer Klinik?

Körper: Cybercrime erfolgt nicht allein aus dem Web heraus. Vielen Attacken gehen physische Delikte voraus: etwa, indem Kriminelle unzureichende Zugangskontrollen zu Stations- oder sogar Serverräumen ausnutzen und dort mit präparierten Sticks das Netz-

werk manipulieren. Nur einer von vielen Aspekten, weshalb ein krisensicheres BCM gerade für Krankenhäuser und Kliniken von höchstem Stellenwert ist – denn sowohl im Alltag als noch mehr in Krisensituationen sind sie elementar für die Versorgungssicherheit.

... und was ist zusätzlich gefordert?

Bürhaus: Direkten Netz-Angriffen muss ebenfalls größte Aufmerksamkeit gelten, da diese das Gesundheitswesen und andere KRITIS-Sektoren, aber auch Betriebe immer stärker treffen. Es geht darum, solche Attacken in Echtzeit zu registrieren und die Ausbreitung zu verhindern. Daher hat die 24/7-Überwachung von IT-Systemen, wie wir sie mit dem Security Operations Center bieten, zentrale Bedeutung. Im Sinne integraler Sicherheit kooperiert das SOC auch aufs Engste mit Werkschutz-Mitarbeitern, beispielsweise, wenn es Anomalien im Datenverkehr registriert und dann zur Gefahrenabwehr Serverräume zusätzlich gesichert werden.

„Bei den 360-Grad-Lösungen betrachten wir die einzelnen Gewerke im Zusammenspiel.“

Dirk H. Bürhaus

All diese Anforderungen bereiten vielen Unternehmern aber Sorge mit Blick auf die Umsetzbarkeit. Gleichzeitig drohen massive Haftungsrisiken. Was raten Sie Firmenchefs?

Körper: Umfassend in ganzheitliche Sicherheit zu investieren. Denn nicht oder nur halbherzig zu handeln, wird am Schluss doppelt so teuer – in Form massiver Schäden plus Haftungsfolgen, die bis zu 2% des weltweiten Umsatzes reichen können. Trotzdem ist die Unternehmer-Sorge nachvollziehbar: Zahlreiche Anforderungen sind gerade für kleine und mittelständische Firmen in Eigenregie kaum zu managen. Aber hier besteht gezielte externe Unterstützung.

Lassen Sie uns noch einmal das Schlagwort ganzheitliche Sicherheit betrachten. Was sind kurz gesagt die damit



Dirk H. Bürhaus, Geschäftsführender Direktor in der KÖTTER Security Gruppe und u. a. Geschäftsführer von German Business Protection (GBP).

verbundenen zentralen Pluspunkte für Unternehmen?

Bürhaus: Hier steht ein Aspekt klar im Fokus: Bei unseren integrierten 360-Grad-Lösungen betrachten wir die einzelnen Sicherheitsgewerke nicht isoliert, sondern stattdessen immer im Gesamtkontext und -zusammenspiel. Auf diese Weise werden Sicherheitslücken und Abstimmungsprobleme vermieden.

Gleichzeitig ergibt sich hieraus, dass Sicherheit Chefsache sein muss – egal, ob bei physischem Schutz oder Cybersecurity?

Körper: Exakt. Unternehmensschutz muss immer strategische Führungsaufgabe sein. Denn Prävention und integrierte Sicherheit stärken die Stabilität in einem immer unkalkulierbarer werdenden Umfeld. Sie zahlen damit ganz entscheidend auch auf das Kundenvertrauen ein.

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

Ergänzende Infos zum neuen KRITIS-Dachgesetz finden Sie hier:



Im Fokus: Zentrale Normen, BBK-Vorlagen, 360-Grad-Schutz

► Relevante Normen (Auswahl)

- DIN SPEC 14027 (Corporate Security – Anforderungen zur Stärkung physischer Resilienz von Organisationen)
- DIN EN ISO/IEC 27001 (Informationssicherheit)
- DIN-EN-ISO-22300er-Reihe (Fokus 22301, 22316, 22361)
- BSI-Standard 200-4 (BCM), BSI-IT-Grundschutz
- DIN EN 17483 (Private Sicherheitsdienstleistungen – KRITIS-Schutz)

► BBK-Vorlagen

- Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) wird Vorlagen, Muster und Vorgaben für Betreiber kritischer Anlagen gemäß KRITIS-Dachgesetz auf seiner Homepage zur Verfügung stellen.
- Mehr künftig unter: www.bbk.bund.de

► 360-Grad-Sicherheitslösungen (koetter.de/360)

- Consulting: u. a. Risiko- und Business-Continuity-Management(BCM)-Analysen
- Personelle Sicherheit: z. B. Werkschutz, Sicherheitsdienste gemäß DIN 77200
- Sicherheitstechnik: Zutritts-, Brand- und Einbruchmeldesysteme, Videotechnik etc.
- Notruf- und Serviceleitstelle: z. B. Aufschaltung, Alarmverifikation, Intervention
- Feuerwehr- und Rettungsdienst: Werk-/Betriebsfeuerwehren, Rettungs-/Sanitätsdienste etc.
- Cybersecurity: u. a. IT-Security Consulting, Security Operations Center (SOC)

► Sicherheit für Unternehmen und KRITIS in Zeiten von KI ist Thema unserer Sicherheitskonferenz am 3. Juni. Infos/Anmeldung:



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.
Die Zeitschrift und alle ihre für die externe Veröffentlichung bestimmten Beiträge sind urheberrechtlich geschützt. Das Copyright kann jedoch jederzeit bei der Redaktion eingeholt werden und wird in der Regel erteilt, wenn die Quelle ausdrücklich genannt und ein Belegexemplar zugestellt wird.
Fotos: S. 1, Titelmotiv Kraftwerk: © wilaiwan – stock.adobe.com; S. 1, Titelmotiv Schild: © MD NAZMUL – stock.adobe.com; S. 2, Herr Fritz Rudolf Körper: © Catrin Schmitt; S. 3, Herr Dirk H. Bürhaus: © KÖTTER Services/Sven Lorenz; S. 4, KRITIS/NIS2: © Aysel – stock.adobe.com

Sie lesen lieber digital?
Nutzen Sie unser E-Paper

 koetter.de/newsletter

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