Pressemitteilung

Kritische Infrastrukturen: „Jeder KRITIS-Betreiber muss Sicherheit ganzheitlich denken und zur Chefsache machen“

- **Über 100 Teilnehmer diskutierten bei der Sicherheitskonferenz STATE OF SECURITY am Brandenburger Tor über aktuelle und künftige Sicherheitsherausforderungen**
- **Verwaltungsrat Friedrich P. Kötter: „Die Gefährdungslage ist klar beschrieben. Jetzt geht es um die konsequente Umsetzung ganzheitlicher Sicherheitslösungen“**
- **KRITIS-Dachgesetz: Verbindliche Empfehlung an KRITIS-Betreiber zur Anwendung von Qualitätsnormen bei Kooperation mit Sicherheitsdienstleistern aufnehmen**

Berlin/Essen (05.06.2024). Die Kritischen Infrastrukturen (KRITIS) stehen auch in Deutschland einer nicht gekannten Bedrohungslage gegenüber. Diese resultiert gleichermaßen aus physischen Angriffen z. B. auf Stromversorgung und Verkehrsinfrastruktur wie aus stetig steigenden Cyberattacken, denen Unternehmen, Behörden, Krankenhäuser etc. ausgesetzt sind. Angesichts dessen forderten hochrangige Politiker, Sicherheitsexperten, Unternehmens- und Behördenvertreter sowie Wissenschaftler bei der heutigen Sicherheitskonferenz STATE OF SECURITY von KÖTTER Security und German Business Protection (GBP) in Berlin einhellig die Ausweitung von Investitionen in den KRITIS-Schutz sowie eine Aufwertung von Sicherheits- und Risk Management zur „Chefsache“.

„Die Nachrichten sind voll von Berichten über erfolgte bzw. drohende Angriffe auf KRITIS-Einrichtungen. Auch die Behörden warnen seit Langem nachdrücklich vor dem Risikopotenzial. Die Gefährdungslage ist somit klar beschrieben, jetzt geht es um die konsequente Umsetzung ganzheitlicher Sicherheitslösungen durch KRITIS-Betreiber aller Größen und Sektoren“, sagte Friedrich P. Kötter, Verwaltungsrat der KÖTTER Security Gruppe, bei der Veranstaltung mit über 100 Teilnehmern im Allianz Forum am Brandenburger Tor.

Die Konzerne in Deutschland sieht Friedrich P. Kötter dabei in Sachen KRITIS-Schutz gut aufgestellt. Damit seien sie gleichzeitig Vorbild für viele öffentliche Institutionen und Mittelständler hinsichtlich der Umsetzung und fortlaufenden Optimierung umfassender KRITIS-Schutzmaßnahmen in Kooperation mit qualifizierten Sicherheitsdienstleistern. Mit Blick auf Letzteres wird die im künftigen KRITIS-

Pressemitteilung

Dachgesetz vorgesehene Implementierung sektorenübergreifender Mindeststandards beim KRITIS-Schutz nach Einschätzung des Verwaltungsrates eine wichtige Basis schaffen.

Gleichwohl geht das von der Bundesregierung bis Oktober umzusetzende KRITIS-Dachgesetz aus seiner Sicht nach wie vor nicht weit genug. „Dies betrifft speziell die auch im überarbeitenden Referentenentwurf erneut nicht enthaltene verbindliche Empfehlung an KRITIS-Betreiber, bei der Kooperation mit Sicherheitsdienstleistern Qualitätsnormen anzuwenden, wie sie auf EU-Ebene in der entsprechenden CER-Richtlinie bereits längst nachdrücklich empfohlen wird“, erklärte Friedrich P. Kötter. „Es wäre daher wünschenswert, wenn der Gesetzgeber diesen Schritt im laufenden Gesetzgebungsprozesses noch zügig nachholt. Die Umsetzung verlässlicher Qualitätsstandards etwa bei Personaleinsatz, Infrastruktur und organisatorischen Prozessen, wie sie z. B. die mit Unterstützung unseres europäischen Dachverbandes CoESS entwickelte Normenreihe EN 17483 definiert, hat für den KRITIS-Schutz und die Einbindung geeigneter Dienstleister zentrale Relevanz“, so der Familienunternehmer. Gleichzeitig appellierte er auch an die Eigenverantwortung der KRITIS-Betreiber: „Sollte unser angeführter Wunsch im abschließenden Gesetz keine Berücksichtigung erfahren, möchte ich Sie umso mehr in Ihrer Ausrichtung bestärken, diese Qualitätsanforderung konsequent in Eigenregie an den jeweiligen Sicherheitsdienstleister zu stellen“, verdeutlichte Friedrich P. Kötter im Rahmen der zehnten Sicherheitskonferenz, die von Fritz Rudolf Körper, Staatssekretär a. D. und Mitglied des KÖTTER Sicherheitsbeirates, moderiert wurde.

Cyber-Security: Umsetzung der NIS2-Richtlinie darf keine zusätzliche Bürokratielast schaffen

Zusätzlich richtete Friedrich P. Kötter einen Blick auf die „Network and Information Security Directive“, kurz NIS2-Richtlinie, mit der Deutschland bis Oktober eine weitere EU-Richtlinie in nationale Gesetzgebung aufnehmen muss. Hieraus resultierend wird somit künftig das „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“, das sich aktuell ebenfalls im Status eines Referentenentwurfs befindet, die Cyber- und Informationssicherheit von Unternehmen und Institutionen federführend regeln. Das mit großem Radius: Denn die NIS2-Richtlinie geht weit über die bisherigen klassischen KRITIS-Sektoren hinaus und bezieht auch zahlreiche neue Bereiche ein. Summa summarum wird die Gesetzgebung allein in Deutschland rd. 30.000 Firmen betreffen. Gleichzeitig steigen auch die inhaltlich-organisatorischen Anforderungen an die Unternehmen. Sie müssen Methoden für die Cybersicherheit entwickeln, die im künftigen Gesetz festgelegten Verfahren für das Gefahrenmanagement einführen und sich an Meldepflichten halten – ansonsten drohen entsprechende Sanktionen.

Dabei richtete der Verwaltungsrat einen nachdrücklichen Appell an die Politik: „Jedes Unternehmen wird, schon aus Eigeninteresse, jegliche politische Anstrengung für mehr Cyberschutz unterstützen. Aber diese Gesetzgebung muss sich gleichzeitig immer an der Lebenswirklichkeit der Unternehmen

Pressemitteilung

orientieren. Und dies heißt heutzutage vor allem: Aus der NIS2-Regelung darf sich keine neue riesige Bürokratielast entwickeln. Hierfür ist u. a. unabdingbar, dass Unternehmen ihren Melde-, Nachweis- und Registrierungspflichten volldigital entsprechen können, Kompetenzen zwischen Bundes- und Landesbehörden überlappungsfrei geregelt werden sowie europaweit agierende Unternehmen nur in einem Mitgliedsstaat gebündelt für die gesamte EU ihren Melde-, Nachweis- und Registrierungspflichten nachkommen müssen."

Sicherheitskonvergenz soll Trennung speziell von physischer und IT-Sicherheit überwinden

Ähnliches unterstrich im Anschluss Alexander Frank, Deputy Director General bei der CoESS, in seinem Vortrag „KRITIS in der EU: Learnings aus den Erfahrungen unserer Nachbarländer". Dabei plädierte er u. a. für die Umsetzung einer strategischen Sicherheitskonvergenz seitens der KRITIS-Betreiber: mit dieser soll die aktuell vielfach noch vorherrschende Aufgaben- und Verantwortungstrennung für die verschiedenen Sicherheitssektoren wie speziell physische und IT-Sicherheit gezielt überwunden werden. „Eine solche Splittung ist schon längst nicht mehr zeitgemäß. Und je weiter die Vernetzung u. a. durch Digitalisierung und KI in Wirtschaft, Staat und Gesellschaft voranschreitet, umso mehr werden solche überholten Strukturen unsere Anfälligkeit für hybride Angriffe erhöhen", warnte Alexander Frank. Entsprechende Handlungsempfehlungen für integrierte Schutzmaßnahmen bietet das neue CoESS-Whitepaper „Physische Cybersicherheit und kritische Infrastrukturen".

Einheitliche Standards schaffen / Kooperation von Staat und Privat ausbauen

Sebastian Fiedler, Mitglied des Deutschen Bundestages (MdB), hob im Rahmen seines Vortrages „Aktuelle kriminalpolitische Entwicklungen und ihre Bedeutung für deutsche Wirtschaftsunternehmen" u. a. hervor, „dass wir es durchaus mit außerordentlich ernstzunehmenden Bedrohungssituationen zu tun haben, die die Wirtschaftsunternehmen auf ganz unterschiedliche Weise treffen". Dabei bestehe mit Blick auf „gerade eben die Wirtschaftsunternehmen, bei denen wir einig sind, dass wir sie wegen ihrer existenziellen Relevanz besonders schützen müssen", aus seiner Sicht, „Common sense, dass wir hier zu einheitlichen Standards kommen müssen", so das Mitglied des Ausschusses für Inneres und Heimat und Sprecher der Arbeitsgruppe „Kriminalpolitik" im Deutschen Bundestag.

Christian Hochgrebe, Staatssekretär in der Senatsverwaltung für Inneres und Sport des Landes Berlin, verwies in seinem Vortrag „Das KRITIS-Dachgesetz: Der Status Quo aus politischer Sicht" u. a. auf die vielfältigen und weiter steigenden Herausforderungen für Unternehmen aufgrund der hybriden Bedrohungslage. Er plädierte vor diesem Hintergrund nachhaltig für einen weiteren Kooperationsausbau von öffentlicher Hand und Wirtschaft: „All diese Dinge gehen nur gemeinsam miteinander. Wir müssen sowohl behördlich als auch privat zusammendenken. Wir müssen horizontal und vertikal übergreifend uns diesen Herausforderungen stellen." Zumal es neben dem konkreten

Pressemitteilung

KRITIS-Schutz zusätzlich auch „um das wichtige Vertrauen in die Schutzfähigkeit und das Vertrauen in die Leistungsfähigkeit des Staates“ gehe.

Weitere namhafte Referenten und Diskussions-Teilnehmer zeigen KRITIS-Bedeutung auf

Dem Status Quo aus unternehmerischer Sicht zum KRITIS-Dachgesetz widmete sich in seinem Vortrag Alexander B. Krause, SIEMENS Energy Global & Hub Security (Senior Security Manager). Mit der Konvergenz von Cyber-Security und physischer Sicherheit befasste sich außerdem Prof. Dr. Sachar Paulus, Professor für IT-Sicherheit und Studiengangleiter „Cyber Security“ an der Hochschule Mannheim. Er gab dabei u. a. einen Überblick über die Auswirkungen im Kontext des KRITIS-Dachgesetzes, der europäischen CER-Richtlinie sowie der EU-Cyber-Security-Richtlinie NIS 2. Der Bedeutung von KRITIS für die öffentliche Sicherheit widmete sich gleichzeitig Martin Zeidler, Leiter der Abteilung I - Krisenmanagement im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Welche weiteren Anforderungen sich für die Wirtschaft ergeben, stand darüber hinaus im Mittelpunkt der von Prof. Dr. Harald Olschok, Mitglied des KÖTTER Sicherheitsbeirates und Honorarprofessor am Fachbereich Polizei und Sicherheitsmanagement der HWR Berlin, in der Diskussionsrunde mit Dr. Peter Schwark, Hauptgeschäftsführer des Bundesverbandes der Sicherheitswirtschaft (BDSW), MdB Leon Eckert und Dr. Kay Ruge, stellvertretender Hauptgeschäftsführer des Deutschen Landkreistages, sowie Alexander B. Krause.

Mit unserem Newsletter bleiben Sie auf dem Laufenden: www.koetter.de/newsletter

Kontakt:
KÖTTER GmbH & Co. KG Verwaltungsdienstleistungen
Carsten Gronwald, Pressesprecher, Tel.: (0201) 2788-126, Carsten.Gronwald@koetter.de