KRITIS Expertentreff

„Sicherheit muss heute ganzheitlich gedacht werden“

Beim KRITIS Expertentreff, initiiert von TAS Sicherheits- und Kommunikationstechnik, ging es in erster Linie um Lösungen. Gemeinsam mit Kunden und Partnerunternehmen diskutierte man in Hamburg, Düsseldorf, Mainz und München einen ganzheitlichen Sicherheitsansatz, der sowohl Physical- als auch Cyber Security umfasst.

Sicherheit wird zur Chefsache

Im Oktober 2024 wird die europäische Gesetzgebung zur Erhöhung der Resilienz der Kritischen Infrastruktur auf nationaler Ebene umgesetzt. Wenn auch noch nicht final, so ist in den neuen Richtlinien bereits eine Dualität angelegt:

- Das NIS2UmsuCG hat den Fokus auf Cyber Security und Informationstechnik mit weitreichenden Folgen nicht nur für KRITIS-Betreiber, sondern große Teile der Wirtschaft. Ein Risikomanagement wird beispielsweise ebenso gefordert wie der Einsatz sicherer Produkte und die Meldung von Vorfällen – mit Sanktionen bei Nichteinhaltung bis hin zur persönlichen Haftung der Geschäftsführung.
- Im KRITIS-DachG wird der Schwerpunkt auf physische Sicherheitsmaßnahmen (Objektschutz, Zäune, Sperren, Zugangskontrollen u.a.) gelegt. Damit verbunden sind Risikoanalysen, Zugangsverwaltung und Krisenkommunikation.

Auch wenn die Richtlinien noch nicht final sind, eines ist klar: Die Folgen für Betreiber der Kritischen Infrastruktur, Unternehmen, Produkthersteller und Dienstleister der Sicherheitstechnik sind erheblich – und alle tun gut daran, sich bereits heute vorzubereiten.

Hybrider Sicherheitsansatz

Nur ein hybrides Schutzkonzept, bei dem neben der Cyber Sicherheit auch die physische Sicherheit geregelt wird,

gibt die Antwort auf die neuen Regelungen, ist Stephan Holzem, einer der Geschäftsführer der TAS, überzeugt. Auf die Dienstleister der Sicherheitstechnik kommen neue Anforderungen zu. Das Unternehmen TAS berät seine Kunden zu sinnvoll möglichen Schutzmaßnahmen, nimmt eine Risikobewertung vor und schlägt verhältnismäßige Maßnahmen unter Einbeziehung organisatorischer Aspekte vor. Die Umsetzung erfolgt nach aktuellem Stand der Technik unter Berücksichtigung von Normen und Richtlinien. Ein höherer Beratungs- und Planungsaufwand, das Einbinden verschiedener Abteilungen des Kunden und Kooperationen mit Unternehmen sind für das hybride Schutzkonzept unabdingbar.

Und wie lässt sich die Resilienz gegen Cyber-Angriffe erhöhen? Gehärtete Systeme sicherer Herkunft sind eine Grundlage für die Gesamtsicherheit. Nicht umsonst ist der Einsatz - z. B. von Videosystemen diverser Hersteller - im Bereich Kritischer Infrastrukturen in den USA verboten. Und die Bundesregierung hat erst kürzlich ein Verbot von Komponenten chinesischer Hersteller in 5G-Mobilfunknetzen spätestens Ende 2026 angekündigt. Auch Übertragungseinrichtungen bzw. Router sowie Alarmübertragungswege müssen gegen vielfältige Risiken wie einen Strom- oder Netzausfall gewappnet sein.

Eine weitere Grundlage ist die sichere Vernetzung, ob integriert in die IT des Unternehmens oder indem geschlossene Netzstrukturen für die Sicherheitstechnik geschaffen werden. Regelmäßige Updates und Patching aller Komponenten, ein sicherer Remote Access, Monitoring und Reporting sind ebenfalls Bestandteile des hybriden Schutzkonzepts, welches Carsten König, Bereichsleiter Systemgeschäft der TAS, anhand von Best Practice Beispielen aufzeigte.

> „Hybride Schutzkonzepte brauchen Klarheit in Bezug auf Verantwortlichkeiten, Kompetenz und Kooperation“

Der KRITIS-Expertentreff hat noch einmal deutlich gemacht: Ohne profundes Know-how in Cyber Security und Netzwerkstrukturen geht in Zukunft nichts in der Sicherheitstechnik.

www.tas.de