Physikalische Grundlagen der Technik unverändert

stock.adobe.com / Urheber: HNFOTO

Schutz Kritischer Infrastrukturen erfordert maximale Anwendungskompetenz

Die Absicherung von Kritischen Infrastrukturen ist mehr denn je in aller Munde. Das EU-Parlament hat die neue CER-Richtline (Critical Entities Resilience) verabschiedet und die Bundesregierung verständigte sich auf die Eckpunkte des KRITIS-Dachgesetztes, dessen inhaltlicher Entwurf in wenigen Monaten erwartet wird.

Betreiber, die bisher schon zu den Kritischen Infrastrukturen zählen und Betreiber, die künftig neu dazugerechnet werden, sollen aller Voraussicht nach für ein höheres Maß an Absicherung und somit für angemessenen Selbstschutz vor Angreifern verpflichtet werden. Was dies im Einzelnen bedeutet, ist heute noch nicht abzusehen. Die gute Nachricht für die Betreiber ist, dass sich Safety- und Security-Fachfirmen bereits seit vielen Jahren mit Schutzkonzepten für Kritische Infrastrukturen beschäftigen. Das Know-how ist immens. Die physikalischen Grundlagen der Technik verändern sich nicht und Alarmierungs- und Sicherheitssysteme beinhalten etablierte Standards für Hochsicherheitsbereiche.

Bereits seit zwei Jahrzehnten bestehen seitens einzelner Betreiber von Kritischen Infrastrukturen erhöhte bzw. hohe Anforderungen speziell für integrierte Objekt- und Perimeterschutzmaßnahmen. Diese bestanden schon früher nicht nur aus Wassergräben, Mauern und Zäunen mit Stacheldraht als mechanische Barrieren. Vielmehr haben Verantwortliche schon früh darauf abgezielt, dass intelligente Detektionssysteme zur Absicherung von Grundstücken und Arealen, von Objekten und Einrichtungen oder auch von sensiblen Bereichen zum Einsatz kommen. Diese haben die Aufgabe, eine lückenlose Erfassung und Verifikation von Gefahren und Angreifern zu gewährleisten. Und damit einhergehend eine höchstmögliche technische Unterstützung für das eingesetzte Sicherheitspersonal zu bieten – mit akzeptabler Täuschungsalarmrate.

Videosicherheitssysteme als Basis der Absicherung

Securiton Deutschland hat im Hochsicherheitsbereich schon sehr früh begonnen, intelligente Videoanalyse als primäres Detektionssystem für den Objekt-

und Perimeterschutz zu qualifizieren. Mit Hilfe von Überwindungsversuchen, durchgeführt von Dritten (beispielsweise TÜV Süd), wurde diese Pionierarbeit ergänzend etabliert. Durch die Abhandlung verschiedener Testszenarien in unterschiedlichen Anwendungsumgebungen hat sich die Videointelligenz

> „Betrachtung von Risiken und Wahrscheinlichkeiten die Schutzziele zu bestimmen."

schon damals den hohen Anforderungen gestellt. Daraus hervor ging speziell für Kritische Infrastrukturen der seit vielen Jahren betriebsbewährte Videoanalysesensor CIP (Critical Infrastructure Protection) als fester Bestandteil in Perimeterschutzkonzepten bei zahlreichen Endanwendern – nicht nur im Bereich Kritischer Infrastrukturen.

Sowohl in kerntechnischen Anlagen, im Umfeld von Energieerzeugern und Energieverteilern als auch bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) überzeugt die Videointelligenz CIP in vielen Anwendungen. Die Bedrohungsszenarien sind individuell. Im Kern geht es jedoch immer darum, unbefugtes Eindringen und somit Angriffe zu verhindern und darüber hinaus die Sicherheitstechnik selbst zu sichern, sodass Sabotageangriffe schon bei deren Versuch automatisch erkannt werden. Zudem geht es auch um die wirksame Überwachung des Umfeldes, denn herumlungernde Personen bringen ein erhöhtes Bedrohungspotenzial mit sich.

Technik ist für KRITIS bereit

Sicherheitsexperten bzw. Anbieter von integrativen Lösungen warten mit gefestigten Grundlagen und gelernten Prozessen auf und werden damit den Anforderungen für KRITIS gerecht. Physische Absicherung und IT-Sicherheit stellen in Kombination keine technischen Herausforderungen dar. Zu erwarten sind dennoch neue Definitionen und Grundlagen. Bisher werden die Konzepte gemeinsam mit und für die Kunden entwickelt, künftig wird es in einer erweiterten Konstellation möglicherweise noch eine Behörde und einen Gutachter geben – ähnlich wie bisher in speziellen Teilbereichen von Kritischer Infrastruktur. Nach wie vor gilt es, durch Betrachtung von Risiken und Wahrscheinlichkeiten die Schutzziele zu bestimmen und die erforderlichen Maßnahmen dahingehend auszulegen. Daneben gilt es zu berücksichtigen, was technisch möglich ist und was Betreiber dafür investieren können, sowohl in Bezug auf Planungs-, Personal- und Kapitalressourcen.

Technik unterstützt das Sicherheitspersonal maßgeblich

In der zurückliegenden Pandemie resultierten teils Zwänge bei Objektschutzmaßnahmen. Die Verfügbarkeit von ausreichendem Sicherheits- und Wachpersonal war teilweise erheblich eingeschränkt. Es hat sich gezeigt, dass gerade in solchen Ausnahmesituationen beträchtliche Engpässe zustande kommen können. Zum Teil fand eine rettende Substitution von Personal durch Technik statt, da Systeme über Standorte hinweg vernetzt werden konnten. Mittels Multi-Site-Management (MSM) wird für eine übergeordnete Vernetzung von eigenständigen Videosicherheitssystemen gesorgt. MSM unterstützt die zentrale Verwaltung, Steuerung und Konfiguration einer unlimitierten Anzahl von Liegenschaften. Zusätzlich wird eine übergreifende Alarmbearbeitung gewährleistet und so der sichere Aufbau und Betrieb von Sicherheitszentralen zur weltweiten Fernüberwachung unzähliger Liegenschaften ermöglicht.

Dank intelligenter Videoanalyse und Videomanagement aus einem Guss lässt sich eine lückenlose Absicherung gewährleisten. Dennoch können die Systeme das Wachpersonal vor Ort nicht vollumfänglich ersetzen. Stellen wir uns nun vor, dass aufgrund der neuen KRITIS-Vorgaben eine Vielzahl neuer Sicherheitsanlagen entstehen, muss dafür gleichzeitig auch für genügend

Wach- und Sicherheitspersonal und die erforderliche Alarmorganisation gesorgt werden. Mit MSM ist eine Aufschaltung der Videoanlage auf eine ständig besetzten Notruf- und Serviceleitstelle (NSL) möglich, welche notwendige Rechte zur Bedienung der Videosicherheitssysteme unbegrenzter Liegenschaften erhält. Diese Berechtigungen können im Ruhezustand der Anlage eingeschränkt sein und im Störungs- oder Alarmfall entsprechend der Aufgaben erweitert werden. So kann die ausgelagerte NSL eingehende Alarme verfolgen, die notwendigen Schritte für die Intervention ausführen, das Wachpersonal vor Ort mit Live-Informationen unterstützen und insgesamt eine Entlastung für die eigene Organisation schaffen.

Nicht auszuschließen sind durch das neue KRITIS-Dachgesetz die Anforderungen an betroffene Betreiber, eine 24/7-Interventionsverfügbarkeit zu gewährleisten. Was im Bereich Safety – am Beispiel Brandschutz – durch die 24/7-Alarmierung der Feuerwehr (betriebseigen oder kommunal) bereits etabliert ist, kann nun auch für bestehende und neue Anlagen im Bereich Security – Objekt- und Perimeterschutz – zum Tragen kommen. Das bedeutet für viele Betreiber eine Investition in Technik und Personal. Der Einsatz der Technik wird voraussichtlich kein Hindernis darstellen. Das Bereitstellen des erhöhten Personalbedarfs hingegen schon, was aber durch eine Auslagerung von Organisationsmaßnahmen abgefangen werden kann und so das eigene Sicherheitspersonal maßgeblich entlastet. Als Sicherheitspartner arbeitet Securiton Deutschland grundsätzlich an einem Gesamtpaket mit, und zwar von Anfang an. Beginnend mit der Konzeption und Detailplanung unterstützen Experten bundesweit mit Anwendungs-Know-how, mit intelligenten und integrativen Alarm- und Sicherheitssystemen und mit organisatorischen Maßnahmen durch die eigene NSL.

▲ **MICHAEL HARTER,** Strategischer Vertrieb Securiton GmbH

Keine physische Sicherheit ohne IT-Sicherheit

Um die physische Absicherung von Objekten durch Einsatz intelligenter Systeme zu gewährleisten, ist mittlerweile auch ein gewisses Maß an IT-Sicherheit zwingend erforderlich. So ist es unabdingbar, neben den baulichen sowie elektronischen Sicherheitseinrichtungen auch den Aspekt der IT-Sicherheit in Verbindung mit den eingesetzten IT-basierten Systemen zu betrachten. Denn schlussendlich müssen robuste Objekt- und Perimeterschutzsysteme selbst auch IT-Angriffen standhalten. Dafür bieten solche Systeme, die für den Hochsicherheitsbereich konzipiert und gleichzeitig gegen Angriffe gehärtet sind, eigene Bordmittel. Es werden u. a. DoS-Attacken (Denial of Service) vom System selbst bemerkt und abgewehrt, wenn ein Server gezielt mit so vielen Anfragen bombardiert wird, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall droht auszufallen. Auszugsweise gilt es weiter, greifende Schutzmechanismen gegen Man-in-the-Middle-, Brute-Force- oder Phishing-Angriffe bereitzustellen. Besonderes Augenmerk muss dafür auch auf das Videonetzwerk gelegt werden. Client-Server-Kommunikationen müssen verschlüsselt werden, beispielsweise mittels VPN-Zertifikaten. In Hochsicherheitsbereichen sind zudem zwingend Hardwareredundanzen mittels weiterer Server vorzusehen, sodass eine höchstmögliche Verfügbarkeit – sowohl in Verbindung mit drahtgebundener als auch kabelloser Übertragung – gewährleistet wird. Aufgrund solcher Zusatzanforderungen an die IT- Sicherheit werden die Systeme im Umfeld der Kritischen Infrastrukturen bereits seit einiger Zeit mit diesen systemeigenen IT- Sicherheitskomponenten ausgerüstet. Früher teils noch von Drittanbietern in die Systeme implementiert sind sie heute als zentrale Systembestandteile integriert.

Auch die Non-KRITIS-Kunden partizipieren von den Entwicklungen für den Hochsicherheitsbereich, denn die Lösungen stehen allen zur Verfügung.

Dies gerade auch im Hinblick auf aktuelle Problemstellungen, beispielsweise durch die Energieknappheit. So sind Strommangellagen laut Netzbetreibern nicht auszuschließen. Ein sog. „Brownout“ erfordert kontrollierte Rationierungen, mit denen auch und vor allem energiehungrige Unternehmen rechnen müssen. Meist sind zwischen der Ankündigung seitens des Netzversorgers und dem kontrollierten Abschalten der Energieversorgung viele Minuten Reaktionszeit gegeben. Durch eine kontrollierte Trennung vom Energienetz könnten z. B. laufende Produktionen unterbrochen werden, Materialschäden entstehen und das spätere Wiedereinschalten nicht mehr ohne weiteres möglich sein. Um hier den Schaden zu minimieren, können betriebsbewährte elektroakustische Systeme zum Einsatz kommen, welche im Ereignisfall einer bevorstehenden Energieabschaltung unmittelbar das Betriebspersonal informieren und evtl. sogar Handlungsanweisungen geben, z. B. Werkstücke aus den Fertigungsprozessen zu entfernen und Anlagenteile und Maschinen kontrolliert herunterzufahren. Securiton hat solche Anlagen in den letzten Monaten bereits erfolgreich installiert und in Betrieb genommen.

www.securiton.de

> „Systeme können das Wachpersonal vor Ort nicht vollumfänglich ersetzen.“