KRITIS-DACHGESETZ

Gefahren erkennen

KRITIS-Dachgesetz: Sicherheitsvorgaben für Betreiber kritischer Infrastrukturen werden strenger

Das Bewusstsein für die Sicherheit kritischer Infrastrukturen hat sich erheblich verstärkt – das hängt mit den Auswirkungen der Corona-Pandemie und dem Ukraine-Krieg, aber auch mit anderen Vorfällen in jüngster Zeit zusammen. Ende des letzten Jahres hat die Bundesregierung Eckpunkte für das „KRITIS-Dachgesetz“ beschlossen. Was können Betreiber kritischer Infrastrukturen bereits jetzt tun, um sich darauf vorzubereiten? Ein Beitrag von Johanna Wünsch von Advancis Software & Services.

Mit Beginn der Pandemie im Frühling 2020 wurden sicher geglaubte Lieferketten unterbrochen. Im Bereich der kritischen Infrastruktur waren zunächst insbesondere medizinische Güter betroffen – spätestens mit Beginn des Ukraine-Kriegs jedoch wurde offensichtlich, dass unsere gesamte Versorgungssicherheit nicht mehr durchgängig gewährleistet ist, ob mit Energie, Wasser, Lebensmitteln oder weiteren wichtigen Gütern und Leistungen. Hinzu kamen in den vergangenen Jahren weitere Störszenarien wie z. B. Angriffe auf Gaspipelines, das Ausspähen von Truppenübungsplätzen oder Versorgungsunternehmen mit Drohnen, die Sabotage an Kabeln der Deutschen Bahn oder das Eindringen von Demonstranten in Parlamentsgebäude wie in den USA oder im Irak. Die Anzahl der Sicherheitsvorfälle im KRITIS-Bereich ist gestiegen. Die Reaktion der Bundesregierung darauf war überfällig.

Cyberangriffe und physische Gefahren

Zwar wurden im Bereich der Cybersicherheit vor einigen Jahren bereits mit dem BSI-Gesetz (Bundesamt für Sicherheit in der Informationstechnik) sowie dem IT-Sicherheitsgesetz die Sicherheitsstandards für die kritischen Infrastrukturen verstärkt. Betreiber müssen die Einhaltung ihrer IT-Sicherheitsvorgaben nach dem Stand der Technik regelmäßig gegenüber dem BSI nachweisen sowie erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können.

Darüber hinaus gab es in Deutschland bis jetzt aber kein sektoren- und gefahren-

◀◀ zurück zum Inhaltsverzeichnis

© Advancis/chatree petjan

◄ Eine offene Integrationsplattform sorgt für ein umfassendes und effektives Gefahrenmanagement im KRITIS-Umfeld

übergreifendes Gesetz zum KRITIS-Schutz. Allein die Cybersicherheit zu gewährleisten ist jedoch kein umfassendes Konzept. Physische Angriffe wie Sabotage – auch innerhalb eines Unternehmens – oder einfache technische Störungen sowie Naturgefahren können ebenso erheblichen Schaden anrichten.

KRITIS-Dachgesetz

Mit dem KRITIS-Dachgesetz nimmt die Bundesregierung daher nun ergänzend zu den bestehenden Regelungen zum Cyberschutz das Gesamtsystem zum physischen Schutz kritischer Infrastrukturen in den Blick. Das Gesetz soll vor allem einheitliche Mindeststandards festlegen, wie sich Betreiber wichtiger Anlagen schützen und unter welchen Umständen sie Angriffe und Schäden melden müssen. Die Bundesinnenministerin Nancy Faeser erklärte, dass in allen Sektoren der kritischen Infrastruktur „die gleichen Mindestvorgaben im Bereich der physischen Sicherheit“ gelten sollen. Dazu sollen geeignete und verhältnismäßige technische, personelle und organisatorische Maßnahmen getroffen werden.

Was können Betreiber kritischer Infrastruktur bereits jetzt tun, um für diese übergreifenden Sicherheitsvorgaben gerüstet zu sein?

Offene Integrationsplattformen

Natürlich sind KRITIS-Unternehmen bereits umfangreich mit Hilfe technischer Systeme überwacht, doch gerade die Umsetzung übergreifender Aktionen im Gefahrenfall ist oft ein Problem: Was passiert zum Beispiel, wenn es nachts im Maschinenraum eines Heizkraftwerks brennt, während gleichzeitig ein Zaunalarm am rund einen Kilometer entfernten Nebeneingang gemeldet wird, die Sicherheitsleitstelle aber nur mit einem Verantwortlichen besetzt ist?

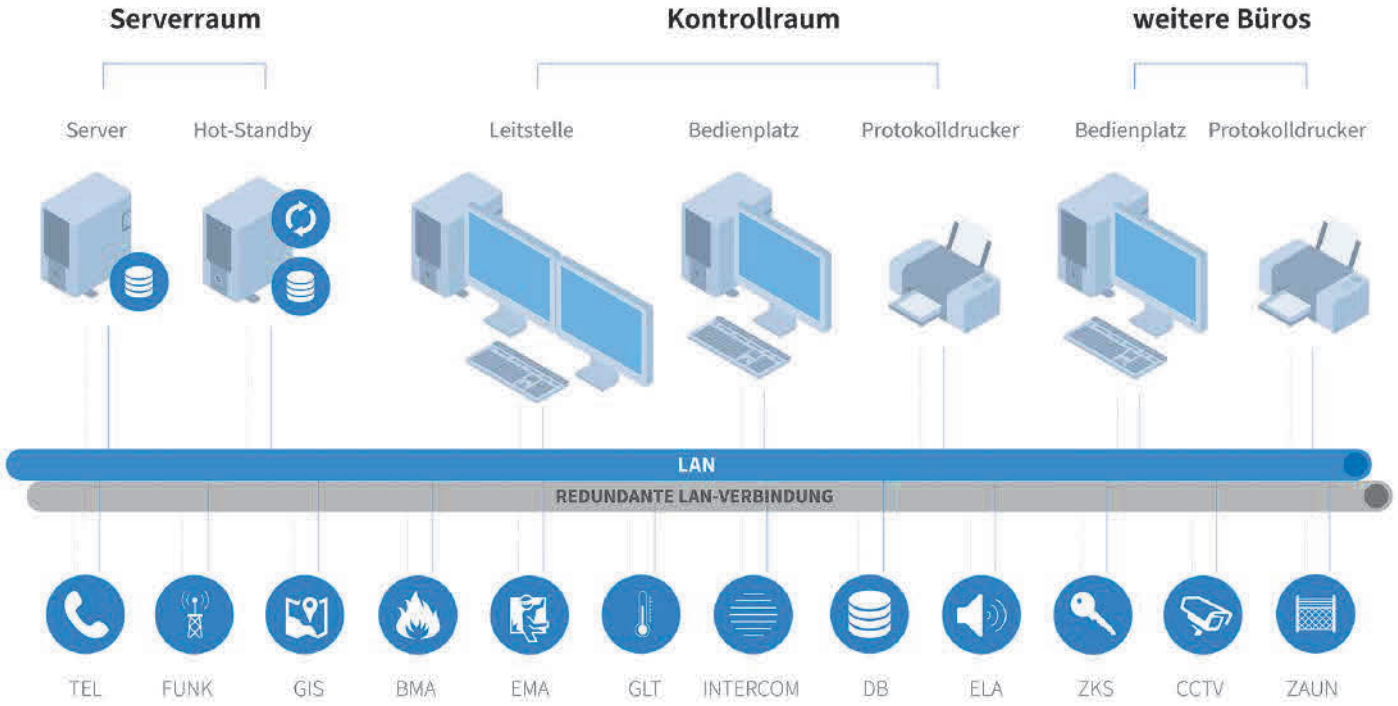
Eine offene Integrationsplattform, die das Gefahrenmanagement sicherstellt – zum Beispiel WinGuard von Advancis – bietet eine zuverlässige Lösung. Statt sich auf viele verschiedene Systeme wie Video- oder Zaunüberwachung, Brandmeldeanlage und Zutrittskontrolle zu konzentrieren, kann das Sicherheitspersonal sich in einer einheitlichen Benutzeroberfläche bewegen und darüber klar erkennen, welche Meldungen kritische Alarme sind. Alle technischen Systeme sind zur einheitlichen Steuerung über Schnittstellen an die Plattform angebunden.

Im Ereignisfall werden eindeutige und individuell auf das jeweilige Unternehmen abgestimmte Verfahrensanweisungen für den Bediener bereitgestellt. Einzelne vorgegebene Handlungsschritte muss er nacheinander abarbeiten, so dass er stets den Überblick behält und die Situation so schnell und sicher wie möglich lösen kann. Gleichzeitig interagieren alle an die Integrationsplattform angebundenen Systeme automatisch.

Systeminteraktion und eindeutige Handlungsanweisungen

Für das Beispiel eines Brandalarms in Verbindung mit einem weiter entfernten Zaunalarm bedeutet dies, dass zunächst über die ebenfalls angeschlossene Videoüberwachung die Kameras im Maschinenraum automatisch in der Benutzeroberfläche aufgeschaltet werden. So kann der Bediener prüfen, ob tatsächlich ein Brand vorliegt und Maßnahmen eingeleitet werden müssen.

Falls ja, bestätigt er dies über die dynamischen Handlungsanweisungen – dann schließen Brandschutztüren automatisch, die Beleuchtung wird eingeschaltet, eine Durchsage zur Evakuierung des Gebäudes wird über die Lautsprecheranlage ausgegeben, die Werkfeuerwehr wird informiert, Feuerwehrlaufkarten werden ausgedruckt usw. Eine direkte Kopplung zu Einsatzleitsystemen ist einfach möglich, wodurch im Notfall ein rasches sowie koordiniertes Eingreifen der Rettungskräfte sichergestellt wird. Hinsichtlich des gleichzeitig eingegangenen Zaunalarms wird der mobile Wachdienst oder der Werkschutz automatisch über eine Meldung auf Mobilgeräte informiert, Schleusen und Tore werden vom System geschlossen. Auch hier wird,



Beispiel-Systemskizze: Alle technischen Systeme sind zur einheitlichen Steuerung über Schnittstellen an die Integrationsplattform angebunden

Bitte umblättern ►

◄◄ zurück zum Inhaltsverzeichnis

falls vorhanden, die Kamera im betreffenden Bereich automatisch aufgeschaltet.

Die Unterscheidung sicherheitskritischer Alarme von Falschalarmen wird durch die Nutzung einer Integrationsplattform erheblich vereinfacht und beschleunigt. Auch Meldungen der Haustechnik oder Wartungsbenachrichtigungen erfolgen über die offene Integrationsplattform, z. B. können Unternehmen mit tausenden von Brandmeldern diese bei Wartungsarbeiten direkt über die Benutzeroberfläche mit Hilfe integrierter CAD-Grundrisspläne einzeln abschalten und nach Abschluss der Arbeiten wieder zuschalten, um Falschalarme zu vermeiden.


© Johanna Wünsch

Johanna Wünsch, Marketing Manager, Advancis Software & Services

Dokumentation und Berichterstattung

Die Dokumentations- und Meldepflicht bei Sicherheitsvorfällen bedeutet für Betreiber kritischer Infrastrukturen oft einen hohen Personal- und Zeitaufwand. Mit einem zentralisierten Gefahrenmanagement über eine offene Integrationsplattform wird die Erfüllung dieser Pflichten erheblich vereinfacht, da für jede Meldung automatisiert ein Bericht erstellt wird. Dieser enthält alle Informationen wie Uhrzeit und Dauer des Alarms, die automatischen Systemmaßnahmen sowie die Aktionen, welche der Bediener durchgeführt hat, usw. Anhänge wie Kamerasequenzen oder zugehörige Pläne werden mitgespeichert.

Der Bericht wird änderungsgeschützt archiviert und kann jederzeit abgerufen und weitergeleitet werden. Die detaillierte Dokumentation unterstützt den Betreiber außerdem bei der weiteren Prozessoptimierung.

Zukunftssicherheit durch technische Erweiterbarkeit

Eine offene Integrationsplattform ist hinsichtlich der Einbindung technischer Systeme flexibel und jederzeit erweiterbar. Auch sehr spezifische, individuelle Schnittstellen und Funktionen sind umsetzbar. WinGuard von Advancis bietet mit der Möglichkeit, dass auch Dritte wie beispielsweise der KRITIS-Betreiber selbst diese entwickeln und einfach in die Software implementieren können, die nötige Flexibilität zur zügigen Umsetzung geänderter Anforderungen in KRITIS-Unternehmen. ●

Advancis Software & Services GmbH
Langen
Tel. +49 6103 80735 0
information@advancis.de
www.advancis.de

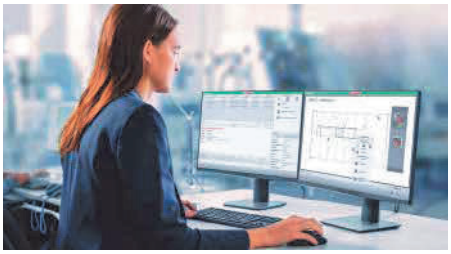
Konica Minolta setzt auf Mobotix

Für den Unternehmensschwerpunkt „Sicherstellung der sozialen Sicherheit“ kombiniert Konica Minolta Mobotix-Kameras mit KI-Apps. Das Unternehmen möchte durch seine Geschäftstätigkeit dazu beitragen, Herausforderungen wie das wachsende Risiko von Katastrophen aufgrund des Klimawandels oder das abnehmende Arbeitskräftepotenzial aufgrund alternder Gesellschaften zu lösen. Um die Sicherheit der Menschen zu gewährleisten und die Produktivität der Industrie zu verbessern, wird es immer notwendiger, soziale Probleme durch digitale Transformation (DX) zu lösen, ist Konica Minolta überzeugt. Die KI-unterstützte Echtzeit-Erkennung und -Beurteilung vor Ort unter Verwendung der bildgebenden IoT-Plattform FORXAI von Konica Minolta bietet Lösungsansätze. Konica Minolta setzt dabei auf die robuste, leistungsstarke sowie auf dezentrale Videotechnologie und hohe Cybersicherheit ausgerichtete Mobotix-Videotechnologie.

Die globalen Vertriebsunternehmen von Konica Minolta bieten die Videolösungsdienste auf der Grundlage von Mobotix-Produkten und Dienstleistungen an, um die Arbeitsabläufe bei Kunden zu digitalisieren. Bereits während der Corona-Pandemie in der ersten Hälfte des Geschäftsjahrs 2022 konnte Konica Minolta seine Umsätze in der Videotechnologie mit einer Lösung zum Körperoberflächentemperatur-Screening um 50 % steigern. Daraufhin hat das Unternehmen im April 2022 in Nordamerika begonnen, den Produktvertrieb mit dem von Mobotix zu integrieren. In Europa hat Konica Minolta ab Juni 2022 einen Showroom in Prag eröffnet und Dienstleistungen rund um die Forxai Video Analytic Solution und Forxai Visual Quality Inspection eingeführt. Darüber hinaus begann Konica Minolta im Oktober 2022 mit dem Aufbau einer Serviceeinheit für Videolösungen.

Die im Mai 2022 von Mobotix übernommene Vaxtor Ltd. (Vaxtor) bietet Lösungen zur automatischen Nummernschilderkennung (Automated Licence Plate Recognition, ALPR) und optischen Zeichenerkennung (Optical Character Recognition, OCR). Die Vaxtor OCR-Technologie kann beispielsweise zur Verwaltung, Überwachung und Kontrolle von Lastwagen und Containern in Häfen eingesetzt werden. Sie scannt und erkennt Nummernschilder aus mehr als 150 Ländern und kann Fahrer vor Ort leiten und Zugangsberechtigungen prüfen. Überdies will Konica Minolta durch die Zusammenarbeit mit Mobotix in neue Geschäftsbereiche expandieren, indem es seinen Kunden im Bereich der Verkehrs- und Logistikinfrastruktur mithilfe der KI-Technologie zum Scannen von Nummernschildern und Containern einen größeren Mehrwert bietet.

www.mobotix.com


© Securiton

Alarme und Störungen ▲ zuverlässig im Griff

Als übergreifendes Sicherheitsmanagement hilft SecuriLink UMS von Securiton, kritische Situationen hilfreich zu entschärfen. Das System stellt Informationen sinnvoll bereit und liefert Instruktionen zur Problemlösung. Detaillierte und zoombare Grafiken mit Fotos, Grundrissplänen und Melderpositionen sorgen für eine gute Übersicht. So können auch Mitarbeitende ohne Vorkenntnisse in der Sicherheitstechnik das System problemlos bedienen. SecuriLink UMS informiere übersichtlich, führe die Bediener direkt zu den richtigen Entscheidungen und ermögliche dadurch erfolgreiche Ereignisbewältigung, so Sascha Weis, Produktmanager bei Securiton Deutschland. SecuriLink UMS biete eine intuitiv bedienbare Benutzeroberfläche, die die Informationen auf das Wesentliche reduziert. Das Ergebnis seien schnelle Reaktionszeiten dank definierter Lösungswege, die für jeden Fall individuell hinterlegt sind.

www.securiton.de

◄◄ zurück zum Inhaltsverzeichnis