Offene Integrationsplattformen schützen Personen und Sachwerte

Schutz kritischer Infrastruktur durch zentralisiertes Sicherheits- und Identitätsmanagement

Die Entwicklung seit Beginn der Pandemie hat die Sorge um die Sicherheit kritischer Infrastruktur (KRITIS) in den Fokus gerückt. Insbesondere seit Beginn des Krieges in der Ukraine mehren sich die Befürchtungen und Bedrohungsszenarien werden immer realistischer. Wie können Betreiber kritischer Infrastrukturen Ausfällen vorbeugen, um die Grundversorgung der Bevölkerung zu gewährleisten?

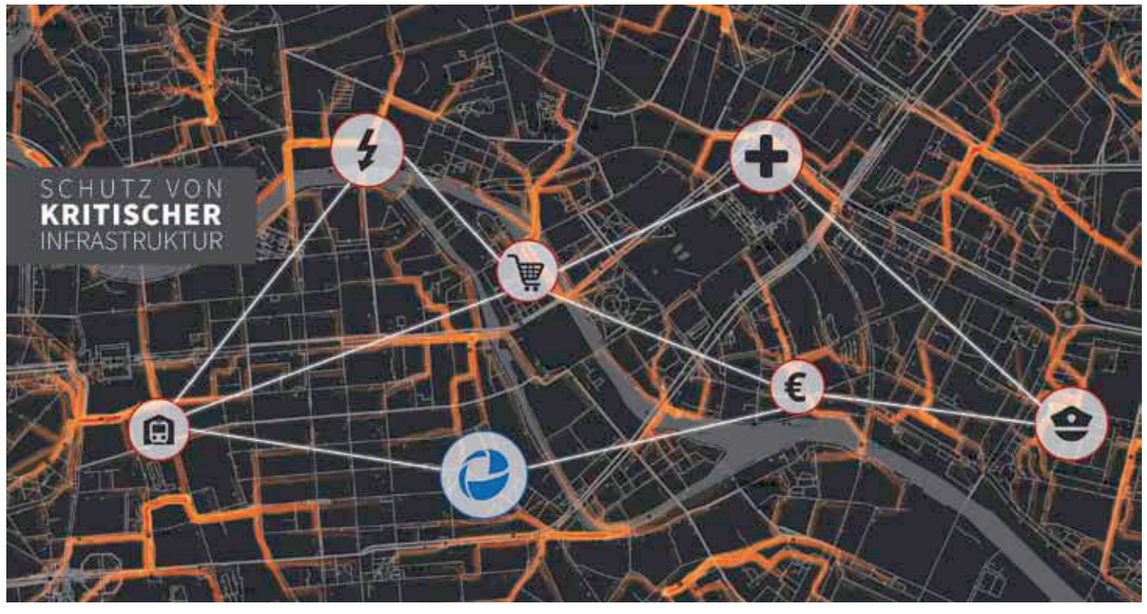

Foto: Advancis Software & Services GmbH

Unternehmen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen wie z. B. Energie- und Wasserversorger, Kliniken, Verkehrsbetriebe, Finanzinstitute oder die Lebensmittelindustrie müssen zuverlässig zur Verfügung stehen, damit die öffentliche Sicherheit nicht beeinträchtigt wird. Diese Verfügbarkeit zu gewährleisten ist Aufgabe der jeweiligen Betreiber. Anders als bei normalen Wirtschaftsunternehmen ist die Risikoanalyse weit umfangreicher, da nicht nur die Auswirkungen von Bedrohungsszenarien für das eigene Unternehmen

berücksichtigt werden müssen, sondern darüber hinaus auch mögliche Beeinträchtigungen auf die Versorgung der Bevölkerung. Neben organisatorischen Sicherheitsmaßnahmen müssen KRITIS-Betreiber über moderne technische Systeme verfügen und diese regelmäßig überprüfen lassen. Nicht nur Cyberangriffen ist vorzubeugen, sondern auch die physische Sicherheit muss ständig im Blick behalten werden.

Bedrohung kritischer Infrastruktur nicht nur durch beabsichtigte Attacken

Ein metallbeschichteter Ballon, wie er z. B. auf einer Kirmes verkauft wird, hatte beispielsweise im September 2021 in Dresden sowie im Dresdner Umland dafür gesorgt, dass es einen stundenlangen Stromausfall für über 300.000 Haushalte gab. Der Ballon war im Umspannwerk an einem sensiblen Punkt in einer Schaltanlage gelandet und löste dort einen Kurzschluss aus. Dieser noch nicht einmal vorsätzlich herbeigeführte Zwischenfall macht deutlich, wie wichtig eine umfassende Sicherheitsüberwachung im KRITIS-Bereich ist. Der betroffene Netzbetreiber kündigte damals an, die Videoüberwachung aufzurüsten und zusätzliche Sicherheitsvorkehrungen prüfen zu wollen.

Integrationsplattformen unterstützen bei der Steuerung verschiedener Sicherheitssysteme

Die Vielzahl der eingesetzten technischen Systeme in einem KRITIS-Unternehmen ist meist jedoch so umfangreich, dass auch der Bediener bzw. das Personal in der Sicherheitszentrale der neuralgische Punkt sein können. Eine offene Integrationsplattform für das Gefahrenmanagement bietet eine zuverlässige und einfach bedienbare Lösung, da der Bediener statt mit unterschiedlichen Einzelsystemen verschiedener Hersteller (wie z. B. Videoüberwachung, Zutrittskontrolle, Einbruchmeldeanlage) nur noch mit einer einheitlichen Benutzeroberfläche zur Steuerung aller Anlagen arbeitet.

Der Schulungsaufwand wird erheblich reduziert, darüber hinaus bietet eine solche Softwareplattform für den Ereignisfall individuell auf das Unternehmen abgestimmte Handlungsanweisungen. Die Plattform unterstützt dabei, wichtige Alarme von Falschalarmen und täglichen Routine- oder Wartungsbenachrichtigungen zu unterscheiden, so dass der Bediener die Informationsflut besser bewältigen kann. Eine direkte Kopplung zu Einsatzleitsystemen ist einfach möglich, wodurch in Notfallsituationen ein rasches und koordiniertes Eingreifen von Einsatz- und Rettungskräften sichergestellt wird.

Flexibel konfigurierbar und erweiterbar

Aufgrund sich dynamisch ändernder Anforderungen zum Schutz kritischer Infrastruktur muss eine solche Integrationsplattform flexibel konfigurierbar und erweiterbar sein, so dass der Betreiber zukunftssicher aufgestellt ist. Insbesondere sehr spezifische sowie individuelle Schnittstellen und Funktionen der Software müssen zügig realisierbar sein, um jederzeit Anpassungen vornehmen zu können. Hier bietet z. B. die offene Integrationsplattform WinGuard X5 von Advancis nahezu unbegrenzte Möglichkeiten. Erstmals basiert diese neue Version auf einem neuen „Plattform-Unterbau“ (Advancis Open Platform), einem innovativen Komponentenmodell. Dieses ermöglicht es Anwendern, die Software basierend auf vorhandenen Konzepten beliebig um eigene Funktionalitäten, Schnittstellen sowie individuelle UI-Komponenten zu erweitern – fast jede Programmiersprache kann genutzt werden. Dem Einsatz eigener, unternehmensspezifischer Komponenten sind dabei kaum Grenzen gesetzt. Die Entwicklung beschleunigt sich, da drittentwickelte Funktionen oder Schnittstellen zu technischen Systemen einfach in die Plattform zur einheitlichen Steuerung der Unternehmenssicherheit integriert werden. Sie können dann entweder nur im eigenen Unternehmen oder im Rahmen einer Entwicklercommunity auch bei anderen KRITIS-Betreibern zum Einsatz kommen.

Einheitliches Identitätsmanagement

Auch ein einheitliches Identitätsmanagement kann KRITIS-Betreiber dabei unterstützen, Personen und Sachwerte zu schützen und Ausfälle zu vermeiden. Insbesondere bei einem KRITIS-Unternehmen mit mehreren nationalen oder internationalen Standorten sind oft unterschiedliche Zutrittskontroll-, Identitäts- oder Biometriesysteme vorhanden, welche einzeln gepflegt werden müssen. Mit einer einheitlichen Zutritts- und Identitätsverwaltung wie dem Advanced Identity Manager „AIM“ von Advancis wird sichergestellt, dass die logischen und physischen Zugriffsrechte, welche mit der Rolle eines Mitarbeiters oder Mitarbeitergruppen verbunden sind, stets synchronisiert werden – dies über alle Bestandssysteme, Standorte und Zutrittskartenformate hinweg.

Resilienz steigern

Die Bündelung verschiedener Sicherheitssysteme und deren einheitliche Steuerung mit Hilfe von Integrationsplattformen trägt entscheidend dazu bei, dass kritische Infrastruktur resilienter wird. Durch die flexible Anpassbarkeit und Erweiterbarkeit solcher Plattformen kann den stetig steigenden Herausforderungen an die Sicherheit im KRITIS-Bereich zukunftssicher begegnet werden.

Autorin: Johanna Wünsch,
Marketing Managerin Advancis Software & Services GmbH