Wie KRITIS-Institutionen physische Sicherheitsmaßnahmen zur Gefahrenabwehr umsetzen können

Mit dem Inkrafttreten der neuen KRITIS-Verordnung wurden die Regulierungen deutlich erweitert. Trifft eine KRITIS-Institution keine Vorsorgemaßnahmen, wird das als mangelnde Sorgfaltspflicht ausgelegt und kann als Ordnungswidrigkeit mit Geldbußen geahndet werden. Grund genug, als betroffene Einrichtung ein physisches Schutzsystem zur Gefahrenabwehr umzusetzen, am besten mit aktueller RFID-Technologie, Biometrie, Besuchermanagement und einer Software als Lösungsplattform.

Von Susanne Plank, PCS Systemtechnik

Bei der Umsetzung einer umfassenden Zutrittskontrolle ist es wichtig, dass die einzelnen Komponenten nicht isoliert funktionieren, sondern in einem Schutznetz untereinander interagieren. Das Sicherheitskonzept für eine KRITIS-Institution sollte sich an folgenden Richtlinien ausrichten:

_____ Nur autorisierte Personen dürfen auf dem Gelände sein.
_____ Es muss zu jeder Zeit Transparenz bestehen über alle anwesenden Personen auf dem Gelände.
_____ Alle Zutritts- und Alarmereignisse sollten revisionssicher und nachvollziehbar dokumentiert werden.
_____ Besucher und der Lieferverkehr sollten dokumentiert werden.

Eine RFID-Zutrittskontrolle dokumentiert alle Zutrittsereignisse.

Die Dokumentation der anwesenden Personen ist notwendig, da im Falle von Störungen und Alarmierungen eine Meldepflicht besteht, die Auskunft über personenbezogene Daten beinhaltet (BSI-KritisV Vorgaben § 8b (4a) sowie § 9). Aus der Dokumentationspflicht leitet sich ab, dass eine reine Schließanlage für KRITIS-Einrichtungen nicht geeignet ist. Nur ein Zutrittssystem auf Basis von RFID-Technologie gibt im Alarmierungsfall Rückschluss auf die zuletzt anwesenden Personen.

Für einen störungsfreien Betrieb in kritischen Infrastrukturen sollten RFID-Zutrittssysteme hochwertig sein, sodass sie lange ausfallsicher betrieben werden können. Die INTUS-Terminals und -Leser mit dem Siegel „Made in Germany“ erfüllen diesen Qualitätsanspruch durch Langlebigkeit und Robustheit. Sie zeichnen sich durch folgende Eigenschaften aus:

_____ Beständigkeit gegen Chemikalien und Lösungsmittel, auch aggressive Reinigungsmittel
_____ Unempfindlichkeit gegen Temperaturschwankungen
_____ Schmutztoleranz und Feuchtigkeitsschutz bis zur Schutzklasse IP68 für besonders herausfordernde Umgebungsbedingungen
_____ Vandalismusschutz und Sabotagekontakt im Bedrohungsfall
_____ robuste Glasoberfläche mit Schlagschutz von ITK09

Nur aktuelle RFID-Technologie erfüllt Sicherheitsstandards

Regelmäßig sollte man den Stand der eingesetzten RFID-Technologie überprüfen. Seit dem Januar 2017 gelten geänderte VdS-Anforderungen für Einbruchmeldetechnik und Zutrittssteuerung. In Anlagen der VdS-Klassen B und C muss auf der Luftstrecke zwischen Karte und Leser eine verschlüsselnde Technologie eingesetzt werden, die einen „erhöhten Schutz gegen Fernkopieren und Abhören“ erfüllt. Ältere RFID-Systeme mit 125-kHz-Technologie ent-

sprechen den geänderten VdS-Anforderungen nicht. Nur moderne RFID-Verfahren, wie Mifare DESFire EV2 oder Legic advant, arbeiten mit aktueller Verschlüsselung. Diese RFID-Generation bietet wichtige Sicherheitsfunktionen:

_____ Die Datenkommunikation zwischen Transponder und Lesegerät wird verschlüsselt.
_____ Der Speicher auf dem Medium (Karte oder Schlüsselanhänger) ist kopiergeschützt und so nicht auszulesen.
_____ Hohe Lese- und Schreibgeschwindigkeit sorgt für komfortable Bedienung ohne Fehlermeldungen.

Schließsysteme, Zutrittskontrolle und Besuchermanagement

Durch die veränderte Gesetzeslage wurden weitere Betriebe als KRITIS eingestuft. Diese Einrichtungen müssen jetzt die Vorgaben umsetzen und Bestandsgebäude mit einer Zutrittskontrolle nachrüsten. Hier bietet sich der Einsatz von mechatronischen Schließsystemen an. Sie werden direkt in der Tür installiert, unabhängig von einer Stromversorgung. Wenn die Schließsysteme über ein Funk-Gateway an die Zutrittskontrolle angeschlossen werden, verfügen sie über aktuelle Zutrittsprofile – ein wichtiges Sicherheitsplus. Schließzylinder oder digitale E-Handle sind für alle Arten von Türen erhältlich, auch für einbruchhemmende Türen.

Das neue IT-Sicherheitsgesetz fordert auch dazu auf, die sicherheitskritischen Bestandteile der Infrastruktur zu definieren. Für hochsensible Bereiche reicht eine einfache Zutrittskontrolle nicht aus, denn Firmenausweise können gestohlen oder weitergegeben werden. Eine Multifaktor-Authentifizierung erhöht die Sicherheit durch die Abfrage eines weiteren Merkmals. Die Handvenenerkennung INTUS PS kann hier gut eingesetzt werden, sie nutzt neben RFID die biometrische Erkennung zur Verifizierung des Kartennutzers. Das ist hochsicher, denn das Handvenenmuster ist bei jedem Menschen einzigartig und verändert sich im Lauf des Lebens nicht. Die Methode ist fälschungssicher und für die Zutrittskontrolle in Hochsicherheitszonen sehr gut geeignet. Durch ein Speichern des Musters auf der Mitarbeiterkarte erfolgt keine zentrale Datenspeicherung. Die biometrische Handvenenerkennung kann als ein Zutrittsleser im Zutrittssystem oder als Stand-alone-Lösung betrieben werden.

Darüber hinaus müssen verantwortungsvolle Betreiber ihr Gelände und Gebäude vor nicht befugten Personen schützen. Ein Besuchermanagement unterstützt bei der Administration aller Prozesse rund um die Besuchsvorgänge. Denn nicht alle Besucher, die sich anmelden, dürfen tatsächlich ein KRITIS-Unternehmen betreten. Mithilfe von VISIT lässt sich sicherstellen, dass man es nur mit Firmen und Personen zu tun hat, mit denen

Bei einer Multifaktor-Authentifizierung werden zwei Merkmale zur Zutrittskontrolle abgefragt, hier das individuelle Handflächenvenenmuster und ein PIN.

man gemäß den Verordnungen des EU-Sicherheitsrats in Geschäftsbeziehung treten darf. Die Sanktionslistenüberprüfung übernimmt den Abgleich mit aktuellen Sanktionslisten und gibt bei Treffern Warnmeldungen aus. Für KRITIS reicht die Registrierung eines Besuchers manchmal nicht aus – für diesen Fall kann man mithilfe eines UV-Licht-Scanners die Ausweisdokumente des Besuchers auf ihre Echtheit überprüfen.

Alle Anwendungen in einer Lösungsplattform

Diese umfangreichen Bausteine zur Realisierung eines physischen Sicherheitssystems werden unter der professionellen Zutrittskontroll-Software DEXICON gebündelt. Die Software übernimmt die Rolle einer Lösungsplattform für die Gebäudesicherheit. Sie verwaltet Zutrittsprofile von Personen, aber auch die physischen Komponenten wie Zutrittsleser. Mit intelligenten Funktionen, wie Türoffenzeitüberwachung oder Anti-Passback, werden Sicherheitsanforderungen umgesetzt. Lagepläne mit Anzeige des aktuellen Türstatus unterstützen die Einschätzung der Risikolage. Ein Sicherheitssystem muss im Notfall aktiv einschreiten und bei Auffälligkeiten eine Alarmierung aktivieren. Die Benachrichtigung des Wachdienstes erfolgt über eine E-Mail. Ein HTTP-/TCP-Trigger eignet sich, wenn ein automatischer Start einer Alarmaufzeichnung im Videomanagement durchgeführt werden soll. Auch das Aktivieren eines Scheinwerfers oder Lautsprechers zur Abeschreckung ist möglich.

Die Software DEXICON kommuniziert als Lösungsplattform mit anderen Gewerken. DEXICON integriert über seinen OPC-Server das Gefahrenmanagement-System (GMS). Auch die Ansteuerung der Einbruchmeldeanlage kann über das Zutrittssystem erfolgen. Die Software ermöglicht diese kombinierten Funktionen durch eine Vielzahl von Schnittstellen zur Anbindung externer Systeme. So unterstützt DEXICON die KRITIS-Institutionen bei der Administration der verschiedenen Sicherheitsgewerke.