WHITE PAPER

GEBÄUDESICHERHEIT

Schutz kritischer Infrastrukturen

Stand: 08.03.2023

www.pcs.com

Inhalt

1 Einleitung

Die Resilienz von KRITIS Organisationen ist für den Schutz und die Handlungsfähigkeit von Bevölkerung, Wirtschaft und Staat in Deutschland essentiell. Das stellte das Bundesministerium des Inneren im Eckpunkte-Papier zum KRITIS-Dachgesetz im Dezember 2022 fest.

Betreiber von KRITIS-Infrastrukturen tragen eine besondere Verantwortung. Durch die Zuspitzung der politischen Lage und mehreren Sabotagefällen in der Verkehrsinfrastruktur werden die Schutzmaßnahmen für KRITIS-Organisationen neu bewertet. Es rückt die Risikobewertung des Gesamtsystems mit allen relevanten Gefahren stärker in den Fokus (All-Gefahren-Ansatz). Während es für Cybersecurity-Maßnahmen bereits gesetzliche Regelungen gab, fehlen bisher verbindliche Maßnahmenkataloge zur Umsetzung des physischen Schutzes, an denen sich die Betreiber orientieren können. Das Eckpunkte-Papier des Innenministeriums skizziert jetzt vorab den Rahmen, der im Laufe des Jahres 2023 zu einem KRITIS-Dachgesetz erweitert werden wird.

Bereits jetzt wird deutlich, dass der Schutz kritischer Infrastrukturen eine gesamtstaatliche Aufgabe ist und der Staat stärker eingreifen wird. Es werden daher verpflichtende Schutzstandards vorgeschrieben werden, die dann von den Organisationen umzusetzen sind. Eine übergreifende Behörde soll physische Schutzmaßnahmen koordinieren und mit europäischen Regelungen in Einklang bringen. Desweiteren wird ein neu einzuführendes Meldesystem dabei helfen, rechtzeitig andere Institutionen vor Angriffen zu warnen. Trifft eine KRITIS-Institution keine Vorsorgemaßnahmen, wird das als mangelnde Sorgfaltspflicht ausgelegt und kann als Ordnungswidrigkeit mit empfindlichen Geldbußen geahndet werden.

Die neue KRITIS Dachverordnung legt den Fokus stark auf die physische Sicherheit einer Organisation. Alle Betreiber werden Mindestvorgaben auferlegt bekommen, wie die Umsetzung technischer, personeller und organisatorischer Maßnahmen zum physischen Schutz ihrer Organisation. Definierte Schutzstandards werden Orientierung und Handlungssicherheit geben und das Schutzniveau verbindlich erhöhen.

Ein Sicherheitskonzept für eine KRITIS-Institution lässt sich heute schon nach folgenden Richtlinien strukturieren:

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

Die Dokumentation der anwesenden Personen ist notwendig, da im Falle von Störungen und Alarmierungen eine Meldepflicht besteht, die auch Auskunft über personenbezogene Daten beinhaltet (BSI-KritisV Vorgaben Paragraf §8b (4a) sowie §9). Durch die Meldung von Sicherheitsvorfällen können andere KRITIS-Betreiber gewarnt werden, begründet das Bundesministerium des Innern die Meldepflicht.

2 Physische Gebäudeabsicherung

PCS Systemtechnik ist als einer der führenden Lösungsanbieter für physische Gebäudesicherheit Experte für die Planung und Realisierung von umfassenden Schutzmaßnahmen für Organisationen. Zahlreiche Unternehmen aus den Sektoren Energie, Verkehr, Bankwesen, öffentliche KRITIS-Verwaltung oder Lebensmittelproduktion zählen zu den langjährigen Kunden von PCS. Als ausgewiesener Projektspezialist unterstützt PCS Betreiber mit einem breiten Portfolio an einzelnen Bausteinen zur Umsetzung von Gebäudesicherheit.

Dabei werden die einzelnen Komponenten nicht isoliert funktionieren, sondern interagieren im übergreifenden Schutznetz.

Die Realisierung solcher umfassenden Sicherheitsprojekte begleitet PCS von Anfang an mit einem umfangreichen Dienstleistungsangebot. Dies beginnt mit einer Vor-Ort-Begehung, Ausarbeitung eines Konzepts, Erstellen von Plänen oder Türenlisten bis zur Prüfung der Installationsvoraussetzungen vor der eigentlichen Montage. Der laufende, störungsfreie Betrieb des Zutrittssystems wird mit Wartungsverträgen, regelmäßigem Tausch von Verschleißteilen und Software-Updates gewährleistet.

2.1 Zutrittskontrolle

2.1.1 Online-Zutrittskontrolle

Eine einfache Schließanlage ist für KRITIS-Unternehmen nicht geeignet, denn sie ermöglicht keine Dokumentation oder Alarmierung bei auffälligen Ereignissen. Nur ein Zutrittssystem auf Basis von RFID-Ausweisen ermöglicht jederzeit Transparenz über alle Zutritte und gibt im Alarmierungsfall Rückschluss auf die zuletzt anwesenden Personen. Für einen störungsfreien Betrieb ist die Qualität solcher RFID-Zutrittssysteme ausschlaggebend. Die INTUS Terminals und Leser mit dem Siegel „Made in Germany“ erfüllen diesen hohen Qualitätsanspruch durch besondere Langlebigkeit und Robustheit.

Die INTUS Zutrittsleser sind besonders widerstandsfähig gegen Angriffe und zeichnen sich durch folgende Eigenschaften aus:

- Beständigkeit gegen Chemikalien und Lösungsmittel, auch aggressive Reinigungsmittel.
- Unempfindlichkeit gegen Temperaturschwankungen, z.B. in Lagern.
- Schmutztoleranz und Feuchtigkeitsschutz bis zur Schutzklasse IP68.
- Vandalismusschutz und Sabotagekontakt im Bedrohungsfall.
- Besonders robuste Glasoberfläche mit Schlagschutz von IK09.

Die vorgesehene Installationsumgebung zu berücksichtigen. RFID-Leser erhalten Sie in verschiedenen Modellen: Auf- oder Unterputzmontage, für den Außeneinsatz mit Heizung oder vorbereitet für den Einbau in Gegensprechanlagen. Fachkundig gewählte Leser steuern über lange Jahre störungsfrei den Zutritt zu Gebäude und Gelände.

Gesteuert werden die Zutrittsleser über Zutrittskontrollmanager. Bei PCS Systemtechnik erhält ein Akku-unterstützter Notfallbetrieb die volle Funktion auch bei Stromausfall, wie bei einem Blackout.

2.1.2 RFID-Kartenmanagement

Zur Abwehr potentieller Angreifer ist es notwendig, regelmäßig die eingesetzten Technologien auf Aktualität zu überprüfen. Dies gilt auch für die verwendete RFID-Technologie in der Zutrittskontrolle. Seit dem 01.01.2017 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 RFID-Technologie entsprechen den geänderten VdS-Anforderungen nicht. Nur aktuelle RFID-Verfahren, wie Mifare DESFire EV3 oder Legic advant, arbeiten mit aktueller Verschlüsselung und werden als sicher eingestuft.

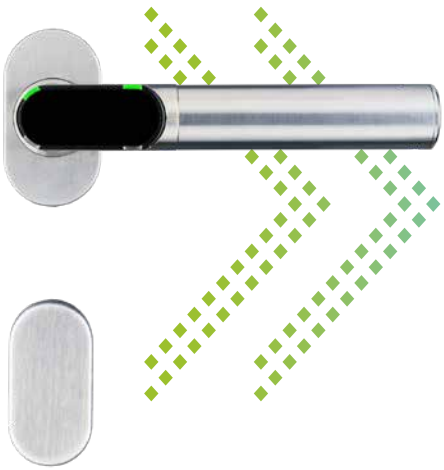
Diese RFID-Generation bietet wichtige Sicherheitsfunktionen:

- 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.
- Ein weiterer Vorteil ist die Nutzung von mechatronischen Schließzylindern zur Absicherung von einzelnen Türen.

PCS bietet Ihnen einen kostenlosen Test Ihrer verwendeten Transponder an. Falls in Ihrem Unternehmen noch eine ältere RFID-Generation im Einsatz ist, empfiehlt PCS den Umstieg auf sichere, verschlüsselte Verfahren. Ein möglicher Weg zur Nutzung aktueller Technologien ist zum Beispiel die Nutzung von hybriden Ausweisen. Gerne unterstützen wir Sie bei der Migration auf aktuelle Technologie.

2.1.3 Offline-Zutrittskontrolle

Durch die Ausweitung der KRITIS-Definition wurden weitere Sektoren als KRITIS eingestuft. Diese Einrichtungen müssen jetzt nachträglich die KRITIS-Vorgaben umsetzen und zum Beispiel Bestandsgebäude mit Zutrittskontrolle ausrüsten. Hier bietet sich der Einsatz von mechatronischen Schließsystemen an.



Sie werden direkt in der Tür installiert und funktionieren batteriebetrieben unabhängig von einer Stromversorgung. Wenn die Schließsysteme über ein Bluetooth© Funk-Gateway an die Zutrittskontrolle angeschlossen werden, verfügen sie jederzeit über aktuelle Zutrittsprofile. Auch alle Zutrittsereignisse werden im übergeordneten System gespeichert - ein wichtiges Sicherheitsplus.

Schließzylinder oder digitale E-Handle sind für alle Arten von Türen geeignet, egal ob Rundrosette, Ovalrosette, Kurz-Lang-, oder Schmalschildbeschlag. In KRITIS Betrieben werden oft Brand- und Rauchschutztüren sowie einbruchhemmende Türen eingesetzt. Auch BSI-empfohlene digitale E-Zylinder sind im Programm. PCS empfiehlt, sich genau beraten zu lassen, welche mechatronischen Schließsysteme geeignet sind und dokumentiert auf Anfrage für jede Tür das geeignete Modell.

2.2 Zufahrtskontrolle

2.2.1 Weitbereichsleser im Außenbereich

Nicht nur der Zugang zum Gebäude muss abgesichert werden, auch für die Zufahrt aufs Gelände ist eine Kontrolle unabdingbar. Damit die Absicherung komfortabel und reibungslos abgewickelt werden kann, sorgen Longrange-Leser auf Basis von UHF-Technologie für eine automatisierte Zufahrtsgenehmigung aus dem Auto heraus. Die UHF-Tags lassen sich am Fahrzeug befestigen. Für externe Fahrzeuge kann das Freigeben einer Schranke über eine Kombination mit Videoüberwachung erfolgen, z.B. durch einen Pförtner in der Zentrale. Weitbereichslösungen eignen sich auch für die Ansteuerung von Rolltoren oder Schranken z.B. vom Gabelstapler aus. Sie lassen sich aus einer Entfernung von bis zu 15 Metern bedienen.

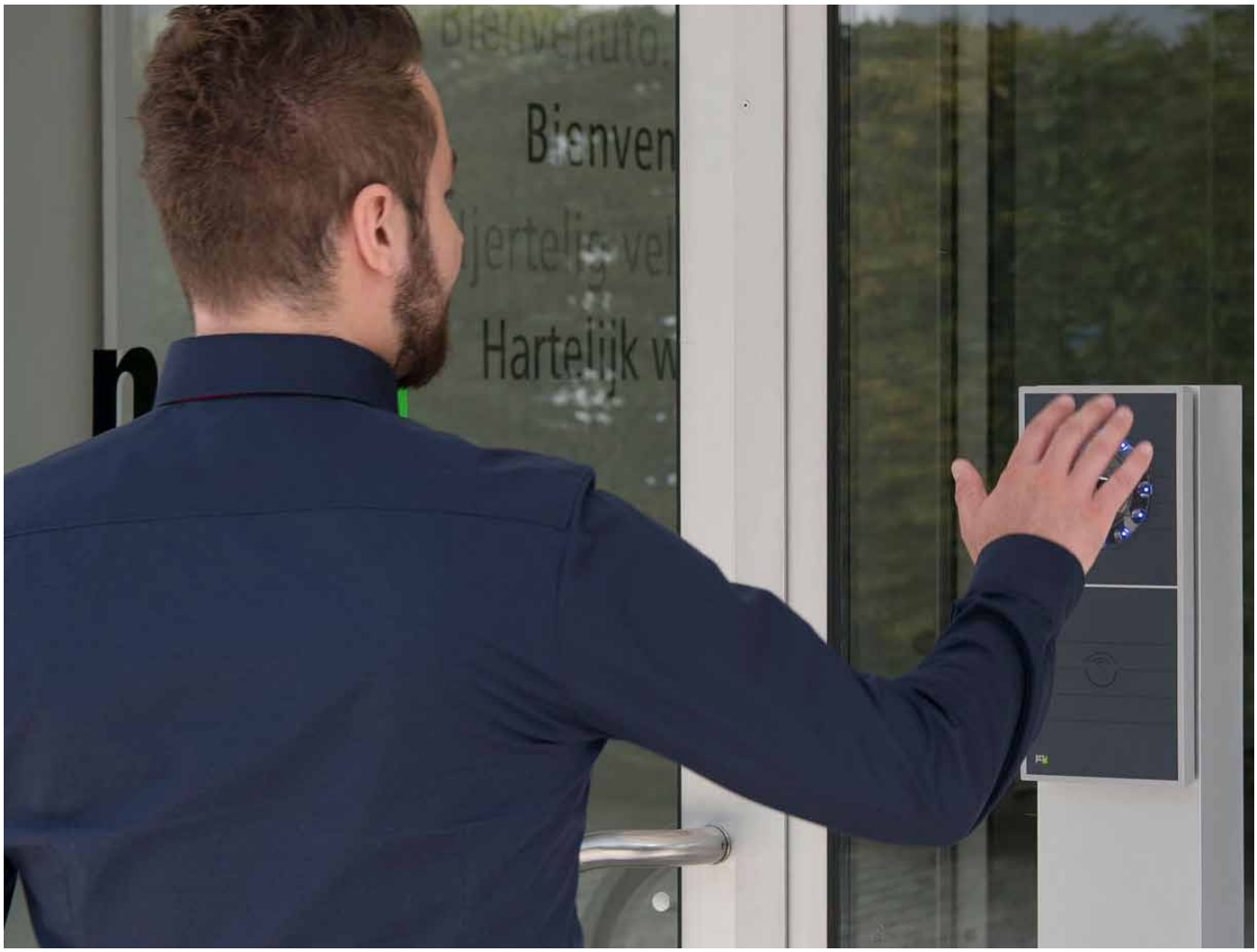
2.2.2 Kennzeichenerkennung

Eine Zufahrtskontrolle für Fahrzeuge lässt sich auch mit automatisierter Kennzeichenerkennung umsetzen. Dazu werden Nummernschilder der registrierten Fahrzeuge in der Datenbank hinterlegt. Die Kennzeichenerkennungssoftware extrahiert aus den Videobildern die Autokennzeichen, sendet sie zur Überprüfung an die Zutrittskontrollsoftware und diese öffnet die Schranke. Dazu werden Nummernschilder der registrierten Fahrer in der Zufahrtskontroll-Datenbank hinterlegt.

2.3 Biometrische Hochsicherheitslösungen

Das IT-Sicherheitsgesetz fordert dazu auf, die Bestandteile der Infrastruktur zu definieren, die besonders sicherheitskritisch sind. In der Regel sind das zum Beispiel die Rechenzentren oder der Kernbereich eines Betriebs, wie die Schaltzentrale eines Energieunternehmens. Für diese hochsensiblen Bereiche wird die Risikobewertung ergeben, dass ein einfacher Schutz mit Zutrittskontrolle nicht ausreichend stark und präventiv schützt. Schließlich können Firmenausweise gestohlen oder weitergegeben werden. Ein Zutrittskarten-Nutzer ist nicht unbedingt gleich zusetzen mit der ursprünglich autorisierten Person.

Hier erhöht eine Multifaktor-Authentifizierung die Sicherheit durch das Abfragen eines weiteren Identifizierungsmerkmals. Besonders gut eignet sich hierfür eine Verifzierung mit Hilfe von Biometrie, speziell der Handvenenerkennung. Das biometrische Merkmal des individuellen Handvenenmusters identifiziert den Kartennutzer zweifelsfrei und eindeutig. Sie funktioniert mit Hilfe eines Infrarotsensors, der aus dem Venenmuster der Handfläche ein Template generiert. Dieses Muster ist bei jedem Menschen einzigartig und verändert sich im Laufe des Lebens nicht. Die Methode ist fälschungssicher und deshalb für Zutrittskontrolle in Hochsicherheitszonen besonders gut geeignet. Durch das Speichern des Musters auf der individuellen Mitarbeiterkarte werden die biometrischen Daten nicht zentral gespeichert, sondern nur auf der Karte des Mitarbeiters selbst. Ein Vorteil für den Datenschutz. Die Handvenenerkennung kann als ein Zutrittsleser im Zutrittssystem betrieben werden oder als Stand-Alone-Lösung. So kann situations- und bedarfsgerecht geplant werden.



2.4 Videoüberwachung

Um das Schutzniveau verbindlich zu erhöhen, ist es sinnvoll, Systeme zur Angriffserkennung zu installieren. Im Bereich der physischen Sicherheit eignen sich intelligente Videolösungen zur Prävention. Mit Videoanalyse werden Personen auf dem Gelände erkannt, auch wenn kein Personal anwesend ist. Über virtuelle Stolperdrähte werden Eindringlinge in geschützten Bereichen entlarvt. Wird über das Netzwerk eine sofortige Aktion initiiert, z.B. ein Lautsprecher oder eine Beleuchtung aktiviert, kann der Angreifer wirkungsvoll abgeschreckt werden.

Bei der Einrichtung einer Videoüberwachung ist es notwendig, dass Modell nach dem Einsatzort auszusuchen. Dreh-, schwenk- und zoombare PTZ-Dome-Kameras bis hin zu speziellen Kameras, wie Wärmebildkameras oder explosionsgeschützten Kameras stehen zur Wahl. Bei schlechten Lichtverhältnissen verbessern Kameras mit Lowlight die Sicht. Bei Dome-Kameras schützt die Glaskuppel die Kamera gegen beabsichtigtes oder unbeabsichtigtes Verdrehen, gegen mechanische Angriffe und Verstellen der Kamera. Sie bieten durch ihre Bauform einen guten Sabotageschutz. Netzwerkkameras können in das Netzwerk einer Firma eingebunden, so dass von jedem beliebigen Ort und Gerät auf die Bilder zugegriffen werden kann. Dies ist im Einsatzfall von großem Vorteil. Die Videomanagement-Software Qognify VMS bündelt übersichtlich alle Kamerabilder und verwaltet die Installation. Als Ergänzung zur Zutrittskontrolle liefert die Videoüberwachung immer dann Bildsequenzen, wenn auffällige Zutrittsereignissen dies erfordern, zum Beispiel im Zusammenhang mit Straftaten. Für die Aufklärung in kritischen Situationen ein wichtiger Pluspunkt.

2.5 Besuchermanagement

2.5.1 Dokumentation aller Besucher

Als verantwortungsvoller Betreiber schützen Sie Gelände und Gebäude vor nichtbefugten Personen. Besucher sind als potenziell unbekannte Personen als Risiko einzustufen. Besuchsvorgänge müssen dokumentiert werden, damit jederzeit nachvollziehbar ist, wer sich wann auf dem Gelände befunden hat. Das Besuchermanagement VISIT unterstützt bei der Administration aller Besuchsvorgänge durch transparente Prozesse. Voranmeldung, Registrierung, Genehmigungsworkflows werden für einzelne Besucher oder Besuchergruppen im System hinterlegt. Ein Workflow regelt auch die Ausgabe von Besucherausweisen mit temporären Zutrittsrechten.

2.5.2 Sanktionslistenüberprüfung

Nicht alle Besucher, die sich anmelden, dürfen tatsächlich ein KRITIS-Unternehmen betreten. Stellen Sie sicher, dass Sie nur mit Firmen und Personen zu tun haben, mit denen Sie gemäß den Verordnungen des EU-Sicherheitsrates in Geschäftsbeziehung treten dürfen. Personen, die in verdächtig eingestuften Unternehmen arbeiten, muss aus Sicherheitsgründen der Besuch untersagt werden. Die Sanktionslistenüberprüfung von VISIT übernimmt den Abgleich gegen aktuelle Sanktionslisten, gibt Warnmeldungen bei Treffern aus und der Besuchsvorgang wird abgelehnt.

2.5.3 Ausweisüberprüfung

Für kritische Infrastrukturen reicht die Voranmeldung eines Besuchers manchmal nicht aus. Eine Identitätsfeststellung überprüft, dass sich Personen mit den korrekten Personendaten anmelden. Das PCS Besuchermanagement VISIT bietet die Möglichkeit, Ausweisdokumente von Besuchern über einen Ausweisscanner zu registrieren. Mit Hilfe des Scanners erfolgt eine Echtheitsüberprüfung des Ausweisdokumentes mittels UV-Licht. Nach der Ausweisüberprüfung werden die persönlichen Angaben automatisiert in die Datenbank des Besuchermanagements übernommen.

3 Lösungsplattform Zutrittssteuerung

Diese umfangreichen Bausteine zur Realisierung eines physischen Sicherheitssystems werden unter der professionellen Zutrittskontroll-Software DEXICON gebündelt. Die Software DEXICON übernimmt die Rolle einer Lösungsplattform für die Gebäudesicherheit. Sie verwaltet alle Personen mit ihren Zutrittsprofilen, aber auch die physischen Zutrittskomponenten wie Zutrittsleser oder übergeordnete Steuereinheiten. Mit intelligenten Funktionen wie Türoffenzeitüberwachung, Anti-Passback oder Aufenthaltsdauerüberwachung werden ganz explizit die Anforderungen vor Ort umgesetzt. So unterstützen z.B. Lagepläne mit Anzeige des aktuellen Türstatus die Einschätzung der Risikolage.

3.1 Rollenprofile zur Verwaltung

Um die Zutrittsprofile der Mitarbeiter effektiv zu verwalten, nutzt DEXICON Rollenkonzepte und Berechtigungsworkflows, die mit wenigen Klicks gesteuert werden. Damit umgeht die Lösungssoftware die starre Zuordnung einer Person zu einer Gruppe. Jede Person, die eine Rolle einnimmt, hat die gleichen Rechte. Dies gilt für Mitarbeiter*innen, aber auch für Fahrzeuge oder Benutzer. Rollen setzen sich aus räumlichen und zeitlichen Zutrittsrechten zusammen. Ein Mitarbeiter kann mehrere Rollen zugeteilt bekommen, für die unterschiedliche Zutrittsrechte vorgesehen sind. Dies ist ein großer Vorteil, wenn durch Urlaube, Fluktuation oder Umstrukturierungen ein Wandel im Unternehmen auch im Sicherheitssystem abgebildet werden muss. Eigene Anpassungen der Zutrittsprofile zur Abbildung individueller Fälle sind selbstverständlich möglich.

3.2 Zutritt für Hygiene- und Notfallmaßnahmen

Da die Zugänge zu KRITIS-Institutionen besonders intensiv kontrolliert werden müssen, unterstützt DEXICON die Gefährdungsprävention mit besonderen Funktionen: Eine Online-Zutrittskontrolle mit einer Türstatus- und Türoffenzeit-Überwachung minimiert menschliches Fehlverhalten. So werden z.B. mit einem Keil blockierte Türen schnell ausfindig gemacht.

In der KRITIS-Dachverordnung werden die Maßnahmen nach den Anforderungen der jeweiligen Sektoren definiert. Gerade im Bereich der Lebensmittelproduktion sind besondere Sicherheitsvorkehrungen notwendig, um die Nahrungsmittelproduktion zu schützen. Zutrittskontrolle lässt sich nutzen, um Sicherheits- und Hygienemaßnahmen durchzusetzen. Ein mögliches Instrument dafür ist die Nutzung einer Raumzonenwechselkontrolle: Sie stellt z.B. sicher, dass zunächst die Hygieneschleuse durchschritten werden muss, bevor ein Produktionsraum betreten werden kann. RFID-Leser eignen sich für Positiv-Buchungen. Sie können z.B. zur Personenzählung für eine Raumzone genutzt werden. Dafür erhält ein Bereich jeweils einen Eintritts- und Austrittsleser, den jede Person nutzt. Ist der Raum vollzählig besetzt, ist kein weiterer Zutritt mehr möglich. Diese sogenannte „Bilanzierung“ ist auch für den Notfall geeignet, z.B. für eine Evakuierung. Gibt es an einem offiziellen Sammelplatz einen Notfall-Leser, so können die geretteten Mitarbeiter ihre Anwesenheit buchen und müssen nicht einzeln gezählt werden.

3.3 Alarmierung

Ein Sicherheitssystem muss im Notfall aktiv einschreiten und aktiv auf Ereignisse in der Zutrittskontrolle reagieren. DEXICON aktiviert eine Alarmierung bei Abweichungen oder Auffälligkeiten in der Zutrittskontrolle. Das kann zum Beispiel die Ablehnung eines unberechtigten Zutrittsversuchs sein. Für die Benachrichtigung des Wachdienstes gibt es in DEXICON mehrere Möglichkeiten. Dies kann eine Email-Benachrichtung auf einem Smartphone sein, das ein Wachdienst immer bei sich hat. Ein sogenannter HTTP-/TCP-Trigger eignet sich dann, wenn ein automatischer Start einer Alarmaufzeichnung im Videomanagement durchgeführt werden soll. Auch das Anschalten eines Weißlichtscheinwerfers oder die akustische Alarmierung (Lautsprecher) mit gleichzeitiger Abschreckungswirkung ist über Trigger aktivierbar. Mit diesen Alarmierungsfunktionen sind Sie vorbereitet auf die zukünftige Meldepflicht für die physische Sicherheit.

3.4 Schnittstellen

Besonders wichtig ist, dass DEXICON als Lösungsplattform mit anderen Gewerken der Sicherheitstechnik kommuniziert. Kennzeichenerkennung, Besuchermanagement und Videoüberwachung werden angebunden. Eine Aufzugsteuerung mit Stockwerksfreigabe kann realisiert werden, zum Beispiel im Zusammenspiel mit dem KONE Access Interface. Auch die Ansteuerung der Einbruchmeldeanlage kann über das Zutrittssystem erfolgen. DEXICON integriert über seinen OPC-Server auch das Gefahrenmanagement-System (GMS) und übermittelt den Türstatus an diese übergreifende Sicherheitsanwendung. Die Software ermöglicht diese kombinierten Funktionen durch eine Vielzahl von Schnittstellen, z.B. Webservice-Interface, zertifizierte SAP-Schnittstelle oder Interface zur Kennzeichenerkennung für die Zufahrtskontrolle. Diese Standard-Schnittstellen zur Anbindung externer Systeme helfen, die Zutrittskontrolle in bestehende Infrastrukturen und Alarmierungsstrukturen zu integrieren. Dies unterstützt KRITIS Institutionen bei der Administration der verschiedenen Sicherheitsgewerke.

4 Umsetzung des Sicherheitskonzepts

4.1 Planung und Konzepterstellung

Um ein tragfähiges Sicherheitskonzept für den physischen Schutz von KRITIS-Organisationen zu realisieren, ist es sinnvoll, die PCS Experten frühzeitig in die Planung miteinzubeziehen. Gemeinsam mit Ihnen klären wir die technischen Anforderungen und bauseits zu erbringenden Leistungen. Wir unterbreiten Ihnen Vorschläge, mit welcher INTUS Hardware und welcher Lösungssoftware Ihr physisches Schutzsystem BSI-konform am besten realisiert werden kann.

Haben Sie sich für Produkte zur Absicherung Ihres Geländes entschieden, erstellen wir eine Liste der benötigten INTUS Hardware mit Angaben zu Produkttyp und Mengengerüst. Auf Wunsch verwenden wir Lagepläne zur Planung oder erstellen Ihnen Installationsschemata. Zur Vorbereitung Ihres Technik-Teams stellen wir Ihnen bereits dann die technischen Handbücher als PDF zur Verfügung. So haben Sie zu diesem Zeitpunkt bereits Transparenz über die notwendige Hardware-Basis.

4.2 Installation

Wir empfehlen Ihnen vor der tatsächlichen Installation, die bauseits zu erbringenden Voraussetzungen für die Installation zu überprüfen. Bei der Installationsprüfung wird eruiert, ob die Verkabelung für die geplante Inbetriebnahme ausreicht. Eine Abschlussdokumentation mit Anschluss-Schemata, Verkabelungsplänen usw. des Projektes gewährleistet die Nachvollziehbarkeit und erfüllt die Dokumentationspflicht des Sicherheitssystems. Sie dokumentiert alle Fakten und ist die Voraussetzung für Nachrüstungen, Anschlussprojekte oder Erweiterungen.

4.3 Wartung und Service

Die PCS Zutrittssysteme sind auf eine langjährige Betriebsdauer angelegt. Viele Geräte von PCS sind bei unseren Kunden 15 Jahre und länger im Einsatz. Als wichtigen Baustein für einen störungsfreien Betrieb empfiehlt PCS die regelmäßige präventive Wartung, die als Dienstleistung angeboten wird. Verschleißteile wie Folientastaturen werden bei Bedarf ausgetauscht, Batterien, Akkus und Speichermedien rechtzeitig ersetzt. Regelmäßig aktualisierte Geräte und Software sind die Basis für einen störungsfreien Betrieb. Ein feinmaschiges Sicherheitsnetz von PCS sorgt für Risikominimierung und einen starken physischen Schutz für jede KRITIS-Institution. Das Schutzniveau Ihrer Organisation wird verbindlich erhöht.

Zeit für Sicherheit.

made in germany

PCS Systemtechnik GmbH
Pfälzer-Wald-Str. 36
81539 München
Tel. +49 89 68004 – 0
intus@pcs.com
www.pcs.com

Ruhrallee 311
45136 Essen
Tel. +49 201 89416 – 0