ZK-Spezial | Juni 2021

sicherheits.berater

Informationsdienst für Sicherheit in Wirtschaft und Verwaltung

Themen-Special
Zutrittskontrolle mit Marktübersicht

Übergreifendes Zutrittsmanagement

Mittels unterschiedlichster Zutrittstechnologien kann geregelt werden, *wer* sich *wann wohin* bewegen darf. Doch nicht alle Zutrittsmittel sind gleichermassen geeignet, eine Zutrittsorganisation im Sinne der Qualitätssicherung kontrollierbar zu gestalten. Mithilfe eines Medien- und herstellerübergreifenden Zutrittsmanagements können auch eigentlich weniger geeignete Zutrittsmittel in eine Compliance-konforme organisationsweite Gesamtlösung integriert werden.

Lutz Rossa

Bei Audits zur Überprüfung der Einhaltung von gesetzlichen Regelungen, unternehmensinternen Bestimmungen oder durch dritte Parteien auferlegte Regularien muss davon ausgegangen werden, dass auch immer die Zutrittsorganisation Untersuchungsbestandteil innerhalb einer Zertifizierung oder Überprüfung ist.

Mechanische Schliessanlagen

Eine mechanische Schliessanlage kann sehr gut regeln, *wer wohin* gehen darf. Der Faktor Zeit ist mit reiner Mechanik zunächst nicht kontrollierbar. In der Praxis ist die Dokumentation ebenfalls lückenhaft, sodass Auditoren hier in der Regel immer fündig werden.

Mechatronische Schliessanlagen

Mechatronische Schliessanlagen bieten den Vorteil, auch den Faktor Zeit (wann) bei Zutrittsberechtigungen einzubeziehen und diesen auch dokumentieren zu können. Wobei die Auswertung mitunter nicht immer komfortabel und zentral an einem Softwaresystem erfolgen kann. Abfragen der Protokollinformationen vor Ort an den Zylindern bzw. den einzelnen mechatronischen Identifikationsmerkmalträgern (IMT) ist durchaus mit Aufwand verbunden.

© depositphotos

Elektronische Schliesssysteme

Auch bei den elektronischen Offline-Systemen erfolgt die Abfrage der Zutrittsprotokollierungen oftmals noch immer am Zylinder selbst. Mittels Network-on-Card bzw. Access-on-Card können die Protokollierungsdaten je nach Konzeption der Zutrittskontrollanlage in das Netzwerk geholt werden und somit zentral erfasst und ausgewertet werden.

Protokollierungsdaten sind bei elektronischen Online-Systemen systembedingt unmittelbar verfügbar und stellen so hinsichtlich der Dokumentation von WER, WANN, WOHIN das Optimum dar.

Dieses Optimum kann allerdings auch durch Anpassung von Betriebs- und Organisationsprozessen für die weniger intelligenten Schliesssysteme fast erreicht werden:

Schliessanlagenverwaltung

Die Dokumentation einer mechanischen Schliessanlage kann mit einer IT- und datenbankgestützten Schliessanlagenverwaltung revisionsfest realisiert werden. In einer solchen Software zur Schliessanlagenverwaltung werden die Schliesszylinder den Türen zugeordnet, in denen sie eingebaut sind. Eine Schnittstelle zu einer Gebäudemanagementsoftware ist hilfreich, eine saubere Türdokumentation inkl. Änderungsprozessen unter Einbeziehung der zuständigen Abteilung (z.B. Bauabteilung) unabdingbar. Die Schliesszylinder bzw. modularen Teile zur Herstellung

eines Zylinders werden in verschlossenen Behältnissen geschützt aufbewahrt. Auch für diese ist eine Zutritts- und Zugriffskontrolle empfehlenswert. In der Regel werden die eindeutig identifizierbaren Schlüssel Personen dauerhaft ausgehändigt. Um Schlüsselverlusten vorzubeugen bzw. die Überprüfung der Existenz von Schlüsseln zu vereinfachen, kann es zielführend sein, die althergebrachte personenbezogene Ausgabe von Schlüsseln an Personen zu überdenken. Dicke Schlüsselbunde am Hosengurt sollten der Vergangenheit angehören.

Schlüsseldepot

Schlüsseldepots können an strategisch sinnvollen Standorten innerhalb eines Unternehmens installiert werden. Benötigt werden ein Strom- und ein Datenanschluss und vielleicht eine Videokamera zur Dokumentation der Schlüsselausgaben. In einem solchen – gegebenenfalls einbruchhemmend – ausgeführten Schlüsseldepot werden Schlüssel auf definierte Steckplätze bestückt. In der zum Schlüsseldepot gehörenden Software wird genau hinterlegt, welche Schliessung und welcher Schlüssel an welchem Steckplatz zu finden ist. Wird nun ein Schlüssel benötigt, so kann sich die berechtigte Person beispielsweise mittels einer RFID-Prozessor-Chipkarte authentisieren und den Schlüssel entnehmen. Eine Rückgabefrist kann in der Software definiert werden. Bei Überschreitung erfolgen entsprechende Eskalationsprozesse.

Eine solche elektronische Verwaltung kann bei Bedarf nicht nur mit mechanischen, sondern auch mit mechatronischen IMT durchgeführt werden.

Dicke Schlüsselbunde ade: Die bewährte RFID-Chipkarte kann auch intern zur Verwaltung von Schlüsseldepots genutzt werden.

© depositphotos

Aufladestationen

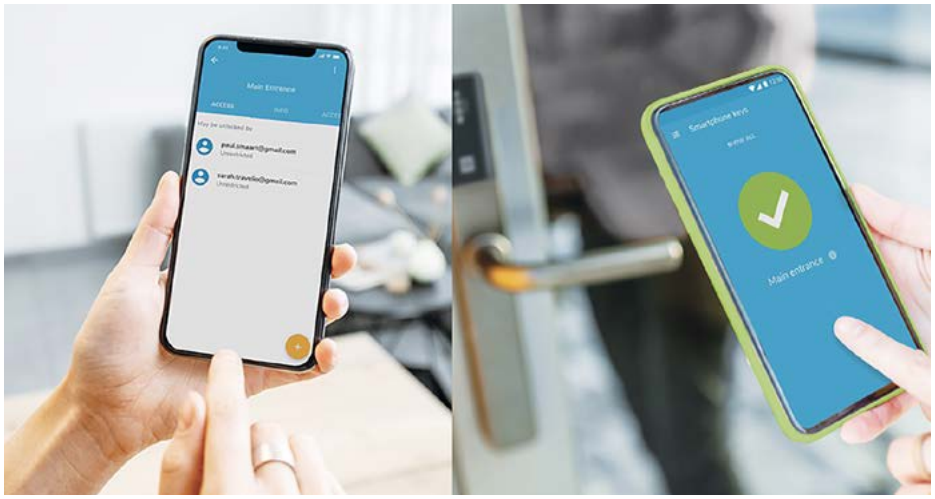
Allerdings besteht bei mechatronischen Systemen die Möglichkeit, Berechtigungen beispielsweise tagesgenau zu vergeben. Weiterhin können IMT ohne elektronische Berechtigungen dokumentiert ausgegeben und die Berechtigungen an Aufladestationen oder inzwischen auch per Smartphone und entsprechender App abgeholt werden. Prozesse und konkrete Ausführungsabläufe können auch hier individuell durchdacht werden: Zwischen fester Ausgabe der IMT ohne ständig zugewiesene Berechtigungen bis zu täglicher Ausgabe der mechatronischen IMT mit bereits definierten elektronischen Berechtigungen ist alles denkbar und in der Praxis Realität.

Elektronische Zutrittskontrollanlagen

Sowohl Online- als auch Offline-Systeme bieten die Möglichkeit, Berechtigungen zu Zutrittsbereichen (wohin) mit Personen (wer) zu verknüpfen und dies auch zeitbasiert (wann) zu gestalten. Bei Off-

Schliessanlagenverwaltung trotz Abstand

Mobilität und soziale Interaktion werden heute immer wichtiger. Von Unternehmen auf der ganzen Welt wird verlangt, dass sie sicheren Zutritt zu ihren Räumlichkeiten für ihre Kunden schaffen und gleichzeitig einen sicheren physischen Abstand zwischen ihnen praktizieren. Eine aus der Ferne steuerbare Zutrittskontrolle kann eine ausgezeichnete Antwort auf diese Herausforderung sein.



Mit DOM Tapkey verwalten Sie Ihre Schliessanlage aus der Ferne. Mit Ihrem Smartphone erteilen Sie den Zutritt zu Ihren Räumlichkeiten ganz einfach.

Vorteile der Cloud-basierten Zutrittskontrolle DOM Tapkey

Kontaktlose Vergabe von Zutrittsberechtigungen: Erleben Sie mit DOM Tapkey den Komfort, Ihr Eigentum von überall aus zu verwalten. Sie können für Ihre Kunden und Mitarbeiter Zutrittsrechte vergeben oder auch wieder entziehen. Sie benötigen dafür nur Ihr Smartphone. Ausserdem können Sie die OTA- bzw. Over-the-Air-Mobile Keys von derselben App aus zustellen. Sie müssen sich nicht physisch in Ihrem Eigentum aufhalten, sondern können aus der Ferne alles überwachen.

Flexibilität mit Transpondern oder mit dem Smartphone: Ermöglichen Sie Ihren Mietern und Mitarbeitern flexiblen Zugang mit einem Transponder oder einem Smartphone. Programmieren Sie die Transponder aus Ihrer Tapkey-App, und Sie können sie sofort für den Zugang zu Ihren Räumlichkeiten verwenden. Wenn Sie es vorziehen, ein Smartphone als mobilen Schlüssel zu verwenden, brauchen Sie nur die Tapkey-App herunterzuladen, sich mit Ihrer Tapkey/Google/Apple ID anzumelden, und schon haben Sie Zutritt.

DOM Schweiz AG
8852 Altendorf
Telefon +41 55 451 07 07
www.dom-group.ch
info@dom-group.ch

line-Systemen kann hier ähnlich wie bei den mechatronischen Systemen vorgegangen werden: Die Ausgabe von IMT kann mit oder ohne Berechtigungen erfolgen, wobei dann bei Letzteren die Berechtigungen an entsprechenden im Netzwerk befindlichen Lesern auf die Karte gespielt werden. Die Verwaltung von Berechtigungen erfolgt in der Software der Zutrittskontrollanlage.

Schutzzonenkonzept

Unternehmens- und organisationsweit wird ein Schutzzonenkonzept entwickelt, das Anforderungen an die Übergänge von etwa Schutzzone A nach Schutzzone B definiert. Hierbei sind neben Brand- und Rauchschutz, Einbruch- und Durchschusshemmung etc. auch Anforderungen an die Protokollierung bzw. Dokumentation der Zutritte zu stellen. Auf diese Weise wird auch schnell deutlich, welche Ausführungen von Schliesssystemen jeweils denkbar sind und welche Rolle im Unternehmen (wer) zu welchem Zeitpunkt (wann) welche Schutzzone (wohin) betreten darf.

Berechtigungsverwaltung

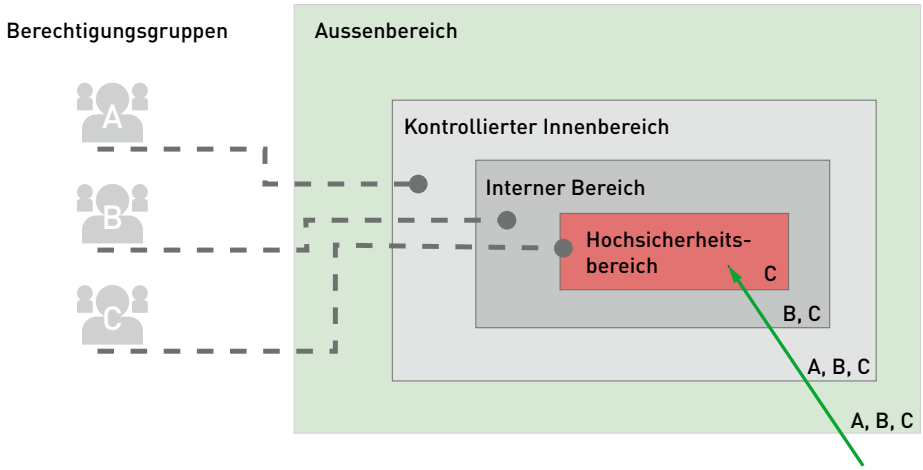
Zutrittsberechtigung zu einer oder mehreren definierten Schutzzonen wird entsprechend der Betriebsprozesse an Rollen gebunden. Mitarbeitern (intern wie auch extern) sowie Besuchern werden eine oder mehrere Identitäten zugewiesen. Den Identitäten wiederum werden idealerweise nur Rollen zugeordnet. Die Zuweisung von Einzelrechten lässt sich allerdings leider nie gänzlich vermeiden, sollte aber auf ein Mindestmass reduziert werden. Rechte werden mit Schutzzonen verknüpft.

Ein solches Rechte-Rollen-Konzept für den physischen Zutritt kann nach obigen Ausführungen nun zunächst unabhängig vom Schliesssystem durchgeführt werden.

Da nun in der Regel verschiedene Schliesssysteme vorzufinden sind, muss dieses Rechte-Rollen-Konzept auf alle angewendet werden: In jedem eingesetzten System sind dieselben Rechte und Rollen zu hinterlegen.

Physical Identification and Access Management System

Ein Physical Identity and Access Management System (PIAM) kann als zentrale Instanz workflow-orientiert und Compliance-konform helfen, Identitäten innerhalb eines Unternehmens Rollen und somit Zutrittsrechte zuzuweisen. So werden diese IMT- und plattformübergreifend an die darunter angeordneten Systeme mit dem Ziel übertragen, auch mechanische IMT in eine informationstechnische Sicherungsebene zu heben. Ein PIAM wirkt wie ein Regenschirm als Ebene über den verschiedenen Ausprägungen von Schliessanlagen und gibt Rechte bzw. Rollen über Schnittstellen weiter an die einzelnen Systeme. Mitarbeiter und Besucher können nun die ihnen zugewiesenen Rollen und ggf. Einzelberechtigungen mit ihrer Chipkarte an Online-Lesern zum Öffnen von Türen nutzen, aber auch um z.B. der Zutrittsrolle entsprechende mechanische Schliessungen aus einem Schlüsseldepot zu entnehmen oder mit einem Badge (Key Fob) oder auch einem Smartphone andere Schliesssysteme bedienen zu können. Gemäss einer Lebenszyklusbetrachtung werden so bei Bedarf oder zeitgesteuert Berechtigungen entzogen, Rollen geändert und somit der Zutritt für Identitäten gesperrt. Darüber hinaus kann das PIAM zentral als Schnittstelle zur Personalstammdatenverwaltung genutzt werden. Im PIAM werden zentral personenbezogene Daten hinterlegt. Den darunterliegenden Systemen sind nur die im PIAM erzeugten Identitäten ohne Bezug zu Name, Abteilung oder Ähnlichem bekannt, was eine Vereinfachung für Datenschutzanforderungen sein kann.



© Redaktion

Identifikationsmerkmalträger

Ein IMT als Prozessor-Chipkarte mit RFID-Interface dient als primäres Zutrittsmedium für alle Nutzer und alle Schliesssysteme. Alternativ kann bei Nutzung einer mechatronischen Schliessanlage ggf. die Schlüsselreide mit RFID-Chip ausgeführt werden oder es müssen dann doch zwei IMT mitgeführt werden. Wichtig hierbei ist, dass auf dem IMT nun weitere Segmente für Anwendungen erforderlich werden: Nämlich für das Schlüsseldepot zum Zugriff auf die mechanischen Schlüssel, auf elektronische «Offline»-Zylinder und natürlich für die elektronische «Online»-Zutrittskontrollanlage.

Fazit

Gemäss dem in diesem Artikel dargestellten Lösungskonzept respektive der Vorgehensweise kann ein organisationsweites medien- und herstellerübergreifendes Zutrittsmanagement realisiert werden. Da dieses Konzept aus vielen Bausteinen besteht, die auch als Einzelanlagen einen Mehrwert erzeugen, können entsprechend dem Schutzbedarf der bereits identifizierten Schwachstellen sowie der verfügbaren Ressourcen zunächst einzelne Aspekte umgesetzt werden. Ein Projektplan für das grosse Ganze kann einzelne Pakete priorisieren und umsetzen, um so zunächst schnelle Erfolge mit grosser Wirkung auf dem doch längeren Weg zum Gesamtziel zu erreichen. ■

LUTZ ROSSA
Dipl.-Ing. (FH) Nachrichtentechnik Sicherheitsberater der VON ZUR MÜHLEN'SCHEN (VZM) GmbH, Spezialist für Leitstellen, Zutrittskontrolle, Videotechnik, ISO 27001 Lead-Auditor