Vorteile kabelloser Zutrittslösungen

SYSTEM SCHLÄGT STÜCKWERK Bei der Auswahl einer elektronischen Zutrittslösung stehen die Leistungsmerkmale und das nahtlose Zusammenspiel unterschiedlicher Technologien, wie virtuelle Vernetzung, Funkvernetzung, Online-Verkabelung und Mobile Access, im Vordergrund. Für den reibungslosen Betrieb einer Anlage spielen aber auch viele Details eine entscheidende Rolle, die häufig wenig Beachtung finden.

AUF EINEN BLICK

VORTEILE Elektronische Zutrittslösungen bieten v.a. folgende Vorteile: Flexibilität bei der Berechtigungsvergabe, höhere Sicherheit und niedrigere Kosten

SICHERHEIT Sämtliche Kommunikation innerhalb der elektronischen Lösung sollte verschlüsselt stattfinden, und nicht nur die Daten verschlüsselt auf dem Identmedium gespeichert werden

Quelle: Salto Systems

Bild 1: Elektronischer Kurzbeschlag für die Sicherung von Innentüren in einem virtuellen Netzwerk oder mittels Funkvernetzung: Die Installation erfolgt auf der vorhandenen DIN-Rosettenbohrung

Elektronische Zutrittslösungen weisen vor allem in drei Punkten Vorteile gegenüber mechanischen Schließsystemen auf: Flexibilität bei der Berechtigungsvergabe, höhere Sicherheit und niedrigere Kosten.

Was wirkliche Flexibilität bei der Berechtigungsvergabe heißt, lässt sich z. B. am RheinMain CongressCenter in Wiesbaden zeigen, in dem rund 1000 Zutrittspunkte elektronisch ausgestattet sind. Für jede Veranstaltung werden unterschiedliche Räume zugewiesen und Bereiche abgetrennt. Das schließt Technikräume und Umkleiden ein, aber auch Catering, Gästegarderoben und Foyers. Kurzfristige Änderungen und Anpassungen sowie deren Dokumentation lassen sich mit einem mechanischen Schließsystem gar nicht abbilden. Folgerichtig haben die Planer des RheinMain CongressCenters von vornherein Mechanik ausgeschlossen.

Dieses Beispiel lässt sich auch auf klassische Bürogebäude übertragen. Hier finden häufig mehr Nutzungsänderungen statt als zunächst angenommen. Viele Anwender, die heute auf elektronische Zutrittskontrolle setzen, begründen ihren Verzicht auf Mechanik damit, dass sie bereits nach wenigen Monaten den Überblick verloren haben, wer welche Schlüssel besitzt und wo diese überhaupt schließen. Das ist nicht nur in der Verwaltung ein Albtraum, sondern auch ein Sicherheitsproblem. Dem lässt sich nur mit einem extrem aufwendigen und kostspieligen Schlüsselmanagement beikommen – oder eben mit Elektronik.

Zumal der zunächst äußerst günstige Anschaffungspreis einer mechanischen Schließanlage trügt: Aufgrund des typischerweise zügig notwendigen Nachbestellens von Schließzylindern und Schlüsseln ganzer Schließgruppen schnellen die Kosten für Mechanik rasch in die Höhe. Über den Lebenszyklus betrachtet, wird eine elektronische Zutrittskontrolle aufgrund der marginalen Folgekosten immer günstiger sein als eine mechanische Anlage.

Virtuelle Vernetzung

Wenn man mechanische Schließanlagen ersetzen möchte, stoßen klassische verkabelte Zutrittslösungen naturgemäß an ihre Grenzen. Wegen der baulichen Situationen und des Installationsaufwandes und damit zusammenhängender Kosten kann man Innentüren nicht alle verkabeln. Eine Möglichkeit, Zutrittspunkte kabellos, effizient und sicher elektronisch zu verwalten, ist z. B. das »Salto Virtual Network« (SVN) des gleichnamigen Herstellers. Denn mit der virtuellen Vernetzung hält sich der Installationsaufwand in Grenzen, gleichzeitig genießen Anwender jedoch die wesentlichen Vorteile einer elektronischen Lösung. Die Zutrittsrechte werden auf die Identmedien – RFID-Karten oder -Schlüsselanhänger – geschrieben (**Bild 1**). Die elektronischen Beschläge (**Bild 2**) und Zylinder (**Bild 3**) prüfen diese und gewähren Zutritt – oder eben nicht. Aufgrund der Schreib-Lese-Funktionalität können zugleich relevante Informationen aus den Türkomponenten bezogen werden, zum Beispiel Protokolldaten oder Batteriezustände. Das erleichtert das Management der Anlage erheblich, da bei Berechtigungsänderungen die Administratoren nicht sämtliche betroffenen Türen ablaufen und aktualisieren müssen, wie bei reinen Offline-Anlagen üblich (**Bild 4**).

Bild 2: Elektronische Beschläge lassen sich virtuell oder per Funk vernetzen

Hinsichtlich der Sicherheit ist elementar, dass sämtliche Kommunikation innerhalb der elektronischen Lösung verschlüsselt stattfindet – und nicht nur die Daten verschlüsselt auf dem Identmedium gespeichert werden. Hierbei gibt es wesentliche Unterschiede zwischen den Anbietern, denn nicht alle vermögen es, dieses Sicherheitsmerkmal praxisgerecht umzusetzen. Die meisten haben dabei ein Problem mit der Auslesegeschwindigkeit ihrer Hardware. Hersteller mit technologisch ausgereiften Systemen haben dieses Thema im Griff. Am einfachsten lässt sich das während einer Testinstallation samt Analyse der Datenströme herausfinden.

Darüber hinaus ist es wichtig zu beachten, dass ein elektronisches Zutrittssystem niemals nur die UID (die einmalige Identifikationsnummer des Ausweises) zur Identifikation von Personen nutzt. Dieses Vorgehen stellt ein enormes Sicherheitsrisiko dar, da die UID ohne Schwierigkeiten zum Klonen von Identmedien genutzt werden kann, wodurch Personen Zutritt zu Bereichen erlangen können, wo sie normalerweise nicht hinein dürfen. In einem virtuellen Netzwerk sollten daher immer die auf dem Ausweis gespeicherten Berechtigungen herangezogen und die Daten von allen Komponenten verschlüsselt übertragen werden.

Ein weiterer genereller Vorteil der virtuellen Vernetzung ist die Möglichkeit, z. B. Spinde, Möbel, Briefkästen oder Serverschränke in die Zutrittslösungen einzubinden (**Bild 5**). Dadurch kann man den Einsatz von unsicherer und teurer Mechanik noch einmal deutlich reduzieren.

Drahtlose Vernetzung

Ein virtuelles Netzwerk allein erfüllt allerdings nicht immer alle Anforderungen. An manchen Zutrittspunkten wird z. B. eine Echtzeit-Zutrittskontrolle gewünscht, auch wenn sich eine Verkabelung nicht umsetzen lässt. Hier bietet sich eine Funkvernetzung der kabellosen Türkomponenten an. Aufgrund seiner Eigenschaften eignet sich Bluetooth dafür gut als Basistechnologie. Denn damit kann man klassische Zutrittsdaten, wie Berechtigungen, Blacklists, Türstatus, Batteriestand etc. übermitteln. Bluetooth gewährleistet in erster Linie eine stabile Kommunikation zwischen der Hardware, eine hohe Übertragungsgeschwindigkeit, große Datenraten und geringe Latenz. Außerdem stellt die Technologie viele Sicherheitsmechanismen bereit. Entscheidend ist bei der Funkvernetzung, in welcher Form das Zutrittssystem die

Bild 3: Elektronischer Zylinder als Mechanik-Ersatz: Hier in den Schlüsselschaltern eines Fluchtwegsicherungssystems – und natürlich an den Außentüren.

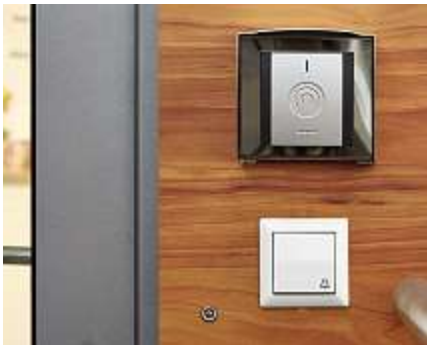

Bild 4: Verkabelter Wandleser für die Online-Zutrittssteuerung und das gleichzeitige Aktualisieren der Zutrittsrechte im virtuellen Netzwerk

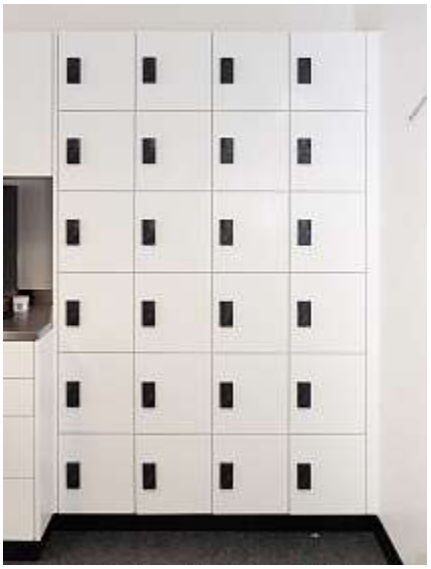

Bild 5: Elektronisches Spindschloss für die Sicherung von Schrankfächern

Daten übermittelt. Moderne Lösungen sichern die verbreiteten Daten mit einer AES-256-bit-Verschlüsselung (AES = Advanced Encryption Standard) – der höchsten derzeit verfügbaren Verschlüsselung.

Bild 6: Elektronisches Vorhangschloss für die Sicherung von Betriebstechnik; andere in der Praxis bereits umgesetzte Einsatzgebiete sind z.B. Container oder auch Sektkühler

Bluetooth als Übertragungstechnologie in drahtlosen Systemen weist gegenüber einer Vernetzung über WLAN deutliche Vorteile auf. Nicht immer ist gewährleistet, dass alle Elemente in einem WLAN reibungslos miteinander funktionieren. Änderungen an der Konfiguration einzelner Geräte, die eigentlich nichts mit der Zutrittskontrolle zu tun haben, können die Kompatibilität beeinträchtigen. Darüber hinaus verursachen die Sicherheitseinstellungen von WLANs häufig Probleme, wenn die Firewall Datenströme blockiert oder Ports an Routern nicht freigegeben wurden.

Obendrein kann in einem WLAN die Priorisierung der Datenpakete zu Verzögerungen beim Datentransfer führen. All diese Risiken schließt man mit einer Vernetzung über Bluetooth aus.

Nahtlose Systemarchitektur

Für einen reibungslosen Betrieb in der Praxis sind allerdings nicht nur die Leistungsmerkmale der einzelnen Technologien ausschlaggebend. Wichtig ist überdies die nahtlose Systemarchitektur, die online verkabelte, virtuell und über Funk vernetzte sowie mobil eingebundene Zutrittspunkte einbezieht. Gerade hier trennt sich die Spreu vom Weizen, denn insbesondere mobile Zutrittslösungen, in denen man mittels mobiler Schlüssel und dem Smartphone Türen öffnen kann, bieten nur wenige Hersteller aus eigener Entwicklung an. Entsprechend kritisch sollten Anwender solche »zusammengestückelten« Anlagen bewerten, um später nicht vor Problemen mit der Datenübertragung oder Kompatibilität zu stehen.

Ein wesentliches Entscheidungskriterium für kabellose elektronische Zutrittslösungen ist zudem das vielseitige Produktportfolio. Es lohnt sich, genau auf den Variantenreichtum der elektronischen Beschläge und Zylinder zu schauen – hinsichtlich Bauformen und Technologien (**Bild 6**). Üblicherweise besteht ein Zutrittsprojekt aus einer komplexen Zusammensetzung von Türsituationen. Dazu zählen Art, Material und Größe von Türen, deren Funktion und Benutzungsintensität, regulatorische Anforderungen (z.B. Brandschutz und Fluchtwege), die Gestaltung des Umfeldes, die Sicherheitsanforderungen für Räume und Bereiche oder auch die Integration mit anderen Gewerken.

Bei der Auswahl des passenden Anbieters sollte man vor allem das Leistungsspektrum der Lösungsplattform beachten.

AUTOR

Marc Rentrop
Vertriebsleiter und Prokurist bei der Salto Systems GmbH, Wuppertal