Die Welt in einer digitalen Nussschale

Infolge einer schier unaufhaltsam wachsenden Anzahl krimineller Handlungen wie Cybercrime oder Spionageakten sind Unternehmen heute mehr denn je gefordert, ihre Firmengebäude zuverlässig abzusichern. Welche digitalen Zutrittskontrollen bieten sich da schon heute an?

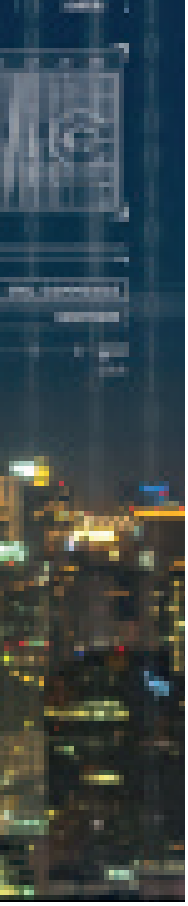
Wir verstehen: Personen, Eigentum und Räumlichkeiten gehören zuverlässig geschützt – in unserer digitalen Zeit gilt es folglich, neue Herausforderungen zu meistern. Wir verstehen weiters: Für Bürogebäude und Gewerbeimmobilien ist darüber hinausgehend eine „verschärfte Sicherheitsstufe" – im Vergleich zum Eigenheim – notwendig: Denken wir nur an haftungsrechtliche Fragen. Was sind also die gewerblichen State-of-the-Art-Sicherheitslösungen?

Zukunft der Zutrittskontrolle

Wer wettet dagegen? Die Zutrittskontrolle der Zukunft ist digital. Gebäude und Anlagen werden heutzutage schon zunehmend mittels digital gestützter Systeme gesichert und diese Zutrittslösungen werden häufig mit einer Zeiterfassung bzw. einem Workforce Management („Wer muss bzw. darf wann wo sein?") verbunden. Radio-Frequency Identification (RFID) – also die Identifizierung mit elektromagnetischen Wellen – ist hier das Stichwort: Berührungslos buchen Mitarbeiter mit RFID-Identifikationsmedien ihre Arbeits- und Pausenzeiten oder starten ihren PC (auch im mobilen Office). Bei „höheren Sicherheitsanforderungen" wird mitunter sogar auf eine biometrische Zutrittskontrolle gesetzt – auch berührungslose Varianten gibt es mittlerweile, etwa die 3D-Fingerabdruckerkennung.

Jedenfalls, so viel lässt sich heute schon sagen, zeichnet sich eine bedeutende Zeitenwende am Horizont ab: Der Schlüsselbund war gestern, der Multifunktionsausweis ist das Aufschließmedium („Masterschlüssel": Chip oder Karte) von morgen. Bei neuartigen „integrierten Sicherheitssystemen" benötigen Mitarbeiter beispielsweise nicht mehr eine Vielzahl unterschiedlicher ID-Karten, PIN-Codes, Passwörter oder Schlüssel, stattdessen befinden sich alle benötigten Applikationen auf einem Multifunktionsausweis. Mit diesem lässt sich etwa der PC-Arbeitsplatz sperren, sobald es an die gemeinschaftliche Zigarette geht, die bargeldlose Bezahlung in der Firmenkantine ist selbstverständlich mit dabei, logischerweise auch der Zutritt zum Personenlift sowie das Ausleihen bzw. Auftanken eines Fahrzeugs aus dem firmeneigenen Fuhrpark. Apropos: Heutzutage können auch schon Kfz-Nummernschilder als Berechtigungsnachweise für einen Zutritt genutzt werden.

Rudolf Preyer



© iStock – Tzido

Es ist immer noch der Zeigefinger auf dem Display, der Smart Office Buildings steuert.

Digitale Sicherheitssysteme brauchen eine klare Hierarchie – sonst verlieren die Benutzer den Überblick.

© Siemens

Das den Mitarbeitern entgegengebrachte Vertrauen

Was passiert aber im Verlustfall? Sollte der Multifunktionsausweis einmal verloren gehen, wird dieser im System gesperrt und allenfalls neu ausgestellt. Der gerechtfertigte Einwand lautet folgerichtig: Was aber, wenn ich meinen Multifunktionsausweis vergessen habe? Hier bietet sich eine Alternative an, denn ohne dieses „Ding" gehen die wenigsten Menschen außer Haus. Erraten: das Smartphone. Darauf haben firmenmäßige Apps klarerweise auch noch Platz. Und schließlich haben Aufschließmedien auch einen insgeheimen Vorteil: Tritt der Mitarbeiter aus dem Unternehmen aus, passen sich seine Zutrittsberechtigungen automatisch und in Echtzeit dem Mitarbeiterstatus an.

Inzwischen kommen verstärkt Sicherheitssysteme zum Einsatz, die die drei Gewerke Alarmtechnik, Zutrittskontrolle und Videoüberwachung von vornherein vereinen. In hochqualitative Alarmmodule lassen sich überdies sowohl hauseigene Komponenten als auch jene von anderen Herstellern einbinden. Damit wäre auch die Frage nach der Kompatibilität angeschnitten: Im Design der Sicherheitsarchitektur gilt es unbedingt, auch die „Verträglichkeit" verschiedener Systeme untereinander anzusprechen.

Authentifizierung anhand mehrerer Merkmale

Auch Systeme mit Zwei-Faktor-Authentifizierung sind schon gang und gäbe, etwa die Kombination von Biometrie („Fingerabdruck") und Besitz („Bestätigung am Handy"). Stichwort Cyber Security: Zwei oder drei der folgenden Methoden können verbunden werden: Etwas wie ein Passwort, das der Nutzer weiß; eine einzigartige Eigenheit des Nutzers wie sein Fingerabdruck; und etwas, das er hat, etwa in Form eines Smartphones. Fürs Protokoll: Bei Systemen mit Alarmfunktionen löst das System – eben ereignisabhängig – einen Alarm aus: Die erforderlichen Maßnahmen können dann von mehreren Orten oder einer übergeordneten Zentrale aus erfolgen. Der Vollständigkeit halber sei hier erwähnt, dass punkto Alarmierung auch die Themen Brand- bzw. Schallschutz mitzudenken sind.

Nochmals: Sicherheit muss tatsächlich für das jeweilige Unternehmen maßgeschneidert werden. Was den Sicherheitsaufwand betrifft, gilt auch hier die Regel: so wenig wie möglich, aber so viel wie nötig.

Jetzt müssen wir natürlich über die Sicherheit digitaler Systeme sprechen. Die zentrale Frage ist hier: Sind diese auch wirklich vor Hackern sicher? ➔

Fernüberwachung von Aufzügen durch den „digitalen Aufzugwärter"

© KONE / Grafik Fotolia

© Telenot Alarmsysteme

Zertifizierte Fachbetriebe konzipieren Smart-Home- und Alarmanlagensysteme für höchste Sicherheitsanforderungen.

Perimeter Protection 2020

Von 14. bis 16. Jänner 2020 öffnet die Perimeter Protection, Internationale Fachmesse für Perimeter-Schutz, im Messezentrum Nürnberg ihre Tore. Sie präsentiert das gesamte Angebotsspektrum an mechanischen, elektrischen und elektronischen Sicherheitslösungen.

perimeter-protection.de

Wie sicher ist cyber?

So viel sei vorneweg festgestellt: Den „einen Schlüssel zur Sicherheit" gibt es in der digitalen Welt bislang noch nicht. Sogenannte Smart Homes sind an das Internet of Things (IoT) angebunden, weil etwa die Heizung, die Klimaanlage oder eine Alarmanlage über das Internet erreicht werden können. So individuell diese Konfiguration sind, so individuell müssen ergo auch die Sicherheitsschlüssel sein.

Bei einer Cloud-Lösung muss die Datensicherheit zwischen den eigenen Anlagen und den externen Servern sichergestellt sein: Experten schwören eben auch auf die Variante, Daten redundant in verschiedenen – örtlich getrennten – Rechenzentren zu speichern. Den Architekten der Cloud Computing Solution sollte man daher unbedingt auf konkrete Zertifizierungen und Normen ansprechen, andernfalls steigt im Schadensfalle – zu allem Überdruss – auch noch die Versicherung aus (und jede würde das). Jedenfalls ist zu beachten, dass der Datentransport im Internet über verschlüsselte Verbindungen funktioniert, Hackerangriffen wird so effektiv entgegengewirkt. Wichtig sind für alle Systeme in Smart Buildings außerdem regelmäßige Updates, um dauerhaft sicher zu bleiben. Kurzum: Denken wir Zutrittslösungen nicht nur komplett neu – sondern vor allem auch digital. •