Bild: peshkov/stock.adobe.com

IOT UND SICHERHEIT

Digital und vernetzt – aber sicher

Sicherheitstechnik wird digitaler und vernetzter, auch wenn bislang noch gerne in die Bereiche „Safety", „Security" und „Komfort" unterschieden wird. Und vor jeder Überlegung, wie die zahlreichen Informationen rund um die Zutrittskontrolle miteinander zu verknüpfen sind, steht die Datensicherheit.

Bei Safety geht es mit Brandmeldeanlagen, Fluchtwegesicherung, Sprachalarmierung sowie Rauch- und Wärmeabzug um die Sicherheit der Gebäude und Menschen. Den Schutz vor Angriffen oder Anschlägen soll die Security mit Videosicherheitsanlagen, Zutrittskontrollanlagen oder Einbruch- oder Störmeldeanlagen gewährleisten. Der Bereich Komfort beschreibt insbesondere die Mensch-Maschinen-Schnittstellen. Gegensprech- oder Beschallungsanlagen gehören dazu.

Digitalisierung und Vernetzung zielen darauf ab, Entscheidungen zu automatisieren oder zumindest zu erleichtern. Je vielfältiger die vorliegenden Informationen sind, umso leichter fallen die Entscheidungen über Zutritt oder Alarme. Informationen liefern vernetzte Geräte, die mit der Zutrittskontrolle zusammenarbeiten und miteinander kommunizieren. Der Kontakt an der Tür gibt

Rückmeldung, ob die Tür geöffnet oder geschlossen ist. Arbeiten alle Gewerke zusammen, lassen sich Aktionen automatisch ausführen – zum Beispiel einen Ausweis sperren, eine Grafik anzeigen oder eine Videokamera aufschalten und steuern. Bei Türen sind bereits eine Menge Gewerke involviert: Video-Sprechanlage, Zutrittskontrolle, optische und akustische Alarmierung, Umfeld-Kamera, Verschluss- und Öffnungsüberwachung, Personenzählung und die Beleuchtung. In Bürogebäuden, in denen viele einzelne Unternehmen ihre Zutrittsberechtigungen über das System selbst steuern, dokumentiert solch eine Zutrittsanlage alle Zutritte, während das Videobild erkennen lässt, wer den QR-Code tatsächlich nutzt.

Auf dem Weg zum schlüssellosen Zutrittssystem

Um sich den Anforderungen an ein Zutrittssystem zu nähern, sind folgende Fragen zu beantworten: „Haben wir Kunden mit digitalen Infrastrukturen, die womöglich für verschiedenartige Zugangsmöglichkeiten Lösungen benötigen?" und „Wie können wir Zutrittslösungen effektiv und effizient managen, nutzen oder vermarkten?" Es geht um mehr als das reine Öffnen und Schließen von Türen. Idealerweise ist das System offen für ergänzende Anwendungen und Nutzungsformen. Nach der elektronischen Türzutrittslösung kommt die mit digitalem Schlüssel, die sich mit dem Smartphone bedienen lässt. In einem nächsten Schritt ist die Verwaltung gemeinschaftlich genutzter Fahrzeuge denkbar. Auch Pool-Cars lassen sich mit virtuellen Schlüsseln ausstatten. Und stets ist es das Ziel, zeitraubende Übergaben von Schlüsseln zu vermeiden und Berechtigungen leichter und flexibler managen zu können. Hat das Unternehmen außerdem in einer Parkgarage Plätze angemietet, so lassen sich dort die Berechtigungen ebenfalls zentralisiert regeln.

Sicherheit in Cloud-Infrastrukturen

Auf den Unterschied zwischen digitalen und mechanischen Sicherheitskonzepten geht Markus Minichmayr, CTO der Tapkey GmbH, ein. Das Unternehmen entwickelt, produziert und vermarktet mit der gleichnamigen Plattform eine Smartphone- und Cloud-basierte Zutrittslösung. Dahinter steht eine patentierte Technik, die auf der persönlichen Identität der Nutzer aufbaut. „Vergleicht man elektronische, Cloud-basierte Schließsysteme mit den mechanischen, so ist offensichtlich, dass nun ganz andere Bedrohungen vorherrschen, die es abzuwehren gilt", erläutert Minichmayr. Mechanische Schließsysteme müssen sich besonders durch eine robuste Konstruktion auszeichnen, um Einbruchsversuche kurzfristig abzuwehren oder zu verhindern. Es gibt viele potenzielle Täter mit umfassenden und langjährigen Erfahrungen mit dem Knacken von Schlössern.

Als Hauptgrund, warum Cloud-basierte Sicherheitssysteme weitaus schwieriger zu knacken seien, nennt Minichmayr, dass es eine geringere Anzahl an Experten gibt, die das Know-how hierfür besitzen. Bedarfskriminalität in der Cloud sei unrealistischer, weil es schwieriger ist, die vielfachen Sicherheitsvorkehrungen zu umgehen. Er nennt drei Säulen, auf denen sich sichere Cloud-Infrastrukturen aufbauen und betreiben lassen:

Lösungsansatz: Begrenzter Zutritt

In Büro- oder auch Wohngebäuden ist eine sichere und personalisierte Zustellmöglichkeit für Lieferdienste hinter die erste Tür eine interessante Lösung: Zusteller erhalten einen einmaligen, zeitlich begrenzten Zutritt. Die Zustellung kann am zentralen Eingang erfolgen, in einem speziellen Zustellraum oder sogar – weiter personalisiert – hinter der ersten Tür der jeweiligen Büro- oder Wohneinheit. Das ist einerseits komfortabel für die Empfänger, die Zeit und Kosten sparen. Andererseits profitieren auch die Immobilienbesitzer von einer solchen Investition, weil dadurch der Wert ihrer Immobilie steigt.

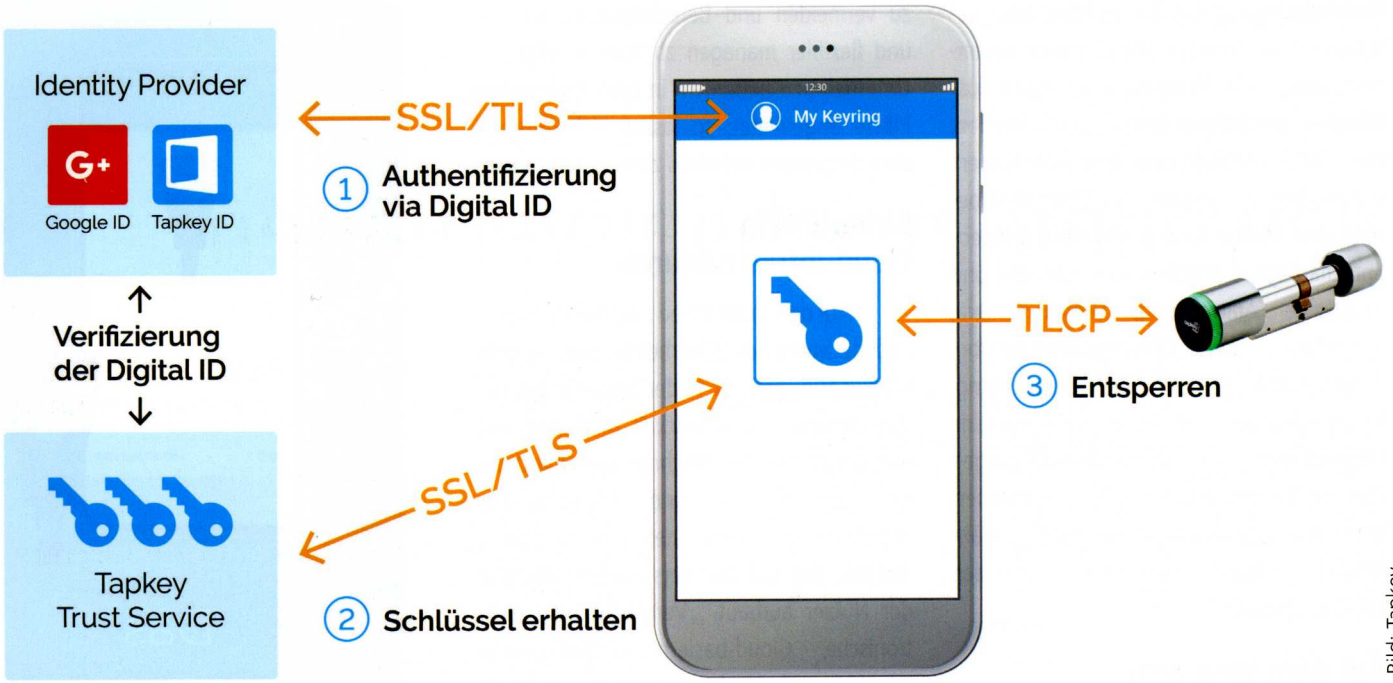

Bild: Tapkey

Der Verschlüsselungsmechanismus von Tapkey sieht die Schritte Authentifizierung, Erhalten des Schlüssels und Entsperren vor. TLS steht dabei für „Transport Layer Security (Transportschichtsicherheit), SSL für „Secure Sockets Layer" (Vorgängerbezeichnung von TLS) und TLCP, das firmeneigene Tapkey Lock Control Protocol.

Fünf Empfehlungen für Endanwender

Organisatorische und technische Richtlinien für digitale Sicherheitssysteme

1) Starke Kennwörter nutzen und gegenüber jeder anderen Person geheim halten
2) Aktivieren von Mehrfaktor-Authentifizierung (Wenn zum Beispiel ein neues Smartphone für den mobilen Zugriff genutzt würde, wird eine SMS an das alte Mobiltelefon gesendet)
3) Endgeräte auf dem neuesten Stand halten und Updates aktivieren
4) Smartphones nicht routen, weil dadurch (voreingestellte/eingebaute) Sicherheitsmechanismen umgangen werden
5) Keine Apps aus fremden Quellen installieren (also nur aus dem jeweils genutzten regulären App-Store oder Play-Store)

- Rechenzentren, in denen die Cloud betrieben wird,
- Schließsystem-Sicherheitsarchitektur, wozu unter anderem die verwendeten Verschlüsselungsmechanismen zählen,
- die organisatorischen und technischen Richtlinien, die von den Benutzern befolgt werden müssen.

Tapkey empfiehlt, die Cloud auszulagern – also von einem externen, professionellen Anbieter hosten zu lassen. Anbieter wie Windows Azure, AWS oder T-Systems brächten dem Cloud-Nutzer mehrere Vorteile – nicht zuletzt aufgrund des Größeneffekts. Sie verfügten über große, erfahrene Teams mit enormem Know-how, um einerseits Angriffe auf die Security abzuwehren und andererseits auch Katastrophenschutzmaßnahmen einzuleiten.

Die zweite Säule bildet ein starker Verschlüsselungsmechanismus. Das gesamte System besteht aus einer Kette von Komponenten, wobei jedes einzelne Element sicher sein muss. Den Basisblock bilden die AES-Verschlüsselung (Advanced Encryption Standard) und die TLS-Webverschlüsselung (Transport Layer Security). Die zweite Schicht umfasst die eigentliche Lösung des Herstellers, die idealerweise aus wiederverwendeten, oft getesteten Komponenten besteht. Dazu zähle zum Beispiel eine Funktion für das Managen von Zutrittsberechtigungen.

Schwachstelle Mensch

Drittens sind eine Reihe operativer Maßnahmen wichtig, um Sicherheit in die Lösung einzubauen. Ihre Entwicklung selbst muss ebenfalls sicher ablaufen. Hierbei gilt es, das Wissen der Mitarbeiter zu steuern, spezielle Aufgaben sollten mit Experten diskutiert werden, und außerdem müssen potenzielle Angriffe getestet werden.

Die größte Schwachstelle in einer Cloud-basierten Infrastruktur ist und bleibt der Endanwender, weshalb es ratsam ist, Regeln aufzustellen und eine Reihe von Empfehlungen zu befolgen – siehe Kasten. Der disziplinierende Effekt, den die Videoüberwachung sensibler Bereiche auslöst, wirkt ergänzend: In vernetzten Lösungen erinnert sie auch Mitarbeiter daran, die Regeln einzuhalten.

Detlef Hinderer ■