Hauskommunikation Wer – Wann – Wo?

Foto: pixabay

Was sich im ersten Moment so anhört wie ein Werbespruch einer Baumarktkette, sind in Wahrheit die drei Grundfragen an Systeme für die Zutrittskontrolle. Mit den Regeln, wer wann wohin darf, definiert der Betreiber den Kreis der berechtigten Personen in Gebäuden oder geschützten, eingegrenzten Bereichen.

Aber auch der Zugang zu Automobilen kann so geregelt werden. Und zugleich definiert der Betreiber oder Eigentümer, wenn er noch eine zeitliche Festlegung trifft, damit die Zugangsberechtigung von Menschen, die sich in diesen Bereichen aufhalten. Als relativ einfaches, herkömmliches und bewährtes System kennen wir Türschlösser mit Schlüssel und Schließzylinder. Als sogenanntes Identmittel, dem Mittel mit dem der Berechtigte sich identifiziert, dient hier der Schlüssel, der den Zutritt ermöglicht. Aber längst sind in einer komplexer werdenden Struktur auch die Anforderungen und damit die Regelwerke für den Zutritt komplexer geworden. Elektromechanische und elektronische Schlösser für Hochsicherheitsschlösser, physische und logische Zugangskontrollen mit Identitätsprüfung, Smartphone-Schlüssel oder NFC-Schlösser können heute für unterschiedlichste Anwendungen eingesetzt werden. Sie arbeiten aktiv oder passiv, kontaktlos oder kontaktbehaftet.

Bei aktiven Identmitteln versorgt eine Batterie zum Beispiel die Entscheidungselektronik des Verschlusssystems mit Energie und sendet Funk- oder Infrarotsignale an das System. Wir kennen das aus der Anwendung in Automobilen.

Bei den passiven Identmitteln finden die meisten unterschiedlichen Technologien ihre Anwendung. Die typischen Leseentfernungen von RFID-Transpondern sind wenige Zentimeter bis zu einem Meter. Auch Plastikkarte, Schlüsselanhänger oder Armbänder oder gar (zum Beispiel bei Tieren) unter die Haut transplantierte Transponder sind heute Stand der Technik ebenso wie das Mobiltelefon als Identmittel. Die Prüfung der Identität kann zusätzlich über biometrische Merkmale wie Fingerabdruck, Iris-Scan oder Gesichtserkennung erfolgen.

Sicherheit im und ums Haus ist in den vergangenen Jahren ein immer wichtigeres Thema geworden. Die Sicherheits-Expo im Juni in München hat es wieder gezeigt, dass hier auch der Elektroinstallateur sich durchaus einen lohnenden Marktanteil erarbeiten kann. Längst hat neben der Beschlagindustrie auch der VDE mit der VDE 0830 hier Standards gesetzt. Und der VdS hat mit den Richtlinien für die Anerkennung von Errichterfirmen schon 2004 klar formuliert, welchen Stellenwert auch die Auswahl der Planer und Errichter und die Interaktion unter den Sicherheitsanlagen für den Betreiber hat. Das hat das Bundesamt für Sicherheit in der Informationstechnologie (BSI) in seinen Technischen Richt- und Leitlinien BSI – TR 03126 und TL 03402, 3403 noch einmal eindrucksvoll unterstrichen.

Und nun kommt das Smart Home. Die Komplexität und das Nebeneinander von Zugangskontrolle, Brandmeldetechnik, Einbruchmeldetechnik und Videoüberwachung ermöglicht zwar unter Umständen die Nutzung gemeinsamer Sensorik, muss aber eindeutig definieren, welches System das führende ist. Zudem gilt: Mit einer einfachen Erweiterung eines Smart Home sind nicht alle Sicherheitsanforderungen zu realisieren – auch nicht ohne den entsprechenden Qualifikationsnachweis.

Die Zeiten, in denen der Elektroinstallateur eine einfache Gegensprechanlage “gleich mit installierte”, sind wohl endgültig vorbei. Allerdings hat die Schalterindustrie das umgehend aufgenommen. „Türkommunikation zum Minehmen” als Access Gate (Hager/Elcom) „Corridor Unit” (Jung/Assa Abloy) oder „Siedle Axiom” sind Beispiele, wie auch der Elektroinstallateur mit Energie und Kommunikation in der Gebäudeautomation für Personenschutz und Gebäudesicherheit Zeichen setzen kann.

Dipl. Wirtschaftsingenieur Peter Respondek