Vernetzte Sicherheit in Smart Buildings

Klimawandel, knapper werdende natürliche Ressourcen, stetiger Zuzug in Metropolen: die Herausforderungen der Zukunft lassen sich nur mit intelligenten und vernetzten Gebäuden („Smart Buildings“) lösen. Die Vernetzung umfasst dabei sämtliche Bestandteile eines Gebäudes – von der Energieversorgung, unter Einbeziehung regenerativer Energien („Smart Grid“), über die Sicherheitstechnik und die Regelung im Betrieb durch vernetzte Gebäudeautomatisierung bis hin zur Steuerung durch Mobilgeräte. Voraussetzung dafür ist die Interoperabilität der Systeme. Nur so können die Risiken der Vernetzung beherrscht werden.

Mehr Sicherheit und Wirtschaftlichkeit

Die Vernetzung sicherheitstechnischer Systeme untereinander und mit anderen gebäudetechnischen Anlagen eröffnet darüber hinaus neue Funktionalitäten und führt zu mehr Sicherheit und Wirtschaftlichkeit. Die Ferninspektion von Gefahrenmeldeanlagen durch den Instandhaltungsdienstleister über das Internet beispielsweise erhöht die Verfügbarkeit und vermeidet überflüssige Serviceeinsätze. Bereits heute können personalisierte Zugangskontrollsysteme so mit Brandmeldesystemen verbunden werden, so dass im Alarmfall sofort festzustellen ist, welche Mitarbeiter sich noch in der Gefahrenzone befinden.

Noch Zukunftsmusik sind andere denkbare Szenarien: Gebäudenutzer mit Mobilgeräten oder anderen vernetzten „Wearables“ erhalten im Gefahrenfall eine personalisierte Warnung und das mit der Gebäudeautomatisierung verbundene Smartphone weist mittels Indoor-Navigation einen sicheren Fluchtweg aus dem Gebäude. Ein adaptives Fluchtweglenkungssystem wertet die Informationen der vernetzten Mobilgeräte aus und vermeidet durch intelligentes Umsteuern der dynamischen Fluchtwegkennzeichen gefährliche Stauungen in den Fluchtwegen.

Rückwirkungen verhindern

Die gemeinsame Nutzung der Sensoren von sicherheits- und gebäudetechnischen Systemen hat darüber hinaus positive Auswirkungen auf einen wirtschaftlichen Gebäudebetrieb. So können Informationen der Bewegungsmelder einer Einbruchmeldeanlage und die Temperatursensoren von Brandmeldern zur kontrollierten natürlichen Lüftungssteuerung des Gebäudes genutzt werden. Wie komplex die Wechselwirkungen dabei allerdings werden können, zeigt bereits das einfache Beispiel eines automatisierten Fensters: Die Einbruchmeldetechnik verlangt ein geschlossenes Fenster zur Scharfschaltung der Einbruchmeldeanlage, während die Gebäudeleittechnik das Fenster zur Nachtauskühlung öffnen möchte. Das natürliche Rauch- und Wärmeabzugsgerät schließlich muss das Fenster im Brandfall mit Vorrang vor allen anderen Gewerken – einschließlich der Jalousiensteuerung – sofort öffnen. Zahlreiche Sensoren und Aktoren setzen an denselben Stellen an, was zu Konflikten

führt und nach Priorisierung sowie dem Aufstellen von Szenarien verlangt. Auch hieran wird deutlich, dass an einer gemeinsamen digitalen Planung kein Weg vorbeiführt.

Cybersicherheit und Datenschutz sind Pflicht

Auch bei Sicherheitssystemen läuft der Datenfluss zukünftig verstärkt über allgemein genutzte Datenleitungen des Gebäudes und über das Internet. Eine starke IT- und Cybersicherheit sowie ein starker Datenschutz sind daher unabdingbare Voraussetzungen, um Sicherheitsanlagen vor ungewollten Rückwirkungen aus dem Netz und vorsätzlichen Cyber-Attacken zu schützen. Ein hohes und für Sicherheitsanlagen neues Risiko stellt dabei die zunehmende Vernetzung mit Mobilgeräten und anderen „embedded devices“ des IoT dar. Diese kompakten und im Regelfall per Funk angebundenen Geräte sind heute häufig nur unzureichend gegen unberechtigte Angriffe geschützt. Übernimmt ein Angreifer das „embedded device“, erhält er ohne besondere Sicherheitsvorkehrungen Zugriff auf das gesamte angebundene interne Netz, da die heutigen Firewalls eher auf Angriffe von außen und nicht für solche aus dem internen Netz ausgelegt sind.

Weltweit sind die Schäden durch Cyberkriminalität bereits heute stark angestiegen. Nach einer Studie des Beratungsunternehmens Accenture drohen Unternehmen weltweit in den kommenden fünf Jahren Mehrkosten und Umsatzverluste durch Cyberangriffe in Höhe von rund 5,2 Billionen US-Dollar. Unternehmen und Gebäudebetreiber sind sich der Gefahren dabei zunehmend bewusst. So sind Cybervorfälle laut Allianz Risk Barometer 2019 der am meisten gefürchtete Auslöser von Betriebsunterbrechungen (50 Prozent der Antworten), gefolgt von Feuer/Explosion (40 Prozent) und Naturkatastrophen (38 Prozent). Erstmals gehören Cybervorfälle damit weltweit zu den größten Geschäftsrisiken.

Chancen nutzen

Chancen für interdisziplinäre Expertengespräch und zum Austausch von Informationen zum Branchenstatus bietet die Light + Building. Als zentrales Anliegen von Branche und Anwendern wird „Vernetzte Sicherheit“ zur Light + Building im März 2020 eine prominente Position innerhalb des Top-Themas „Connecting“ einnehmen. Die Navigation zu sicherheitsspezifischen Angeboten garantiert ein exklusiver Guide. Hierin sind nicht nur alle Anbieter von Sicherheitstechnik gelistet und innerhalb der Fachmesse verortet, sondern auch spezifische Angebote beschrieben und terminiert. „Vernetzte Sicherheit ist integraler Bestandteil der technischen Gebäudeinfrastruktur. Auch deshalb findet sie sich im Produktportfolio einer ganzen Reihe von Ausstellern überall auf der Light + Building. Gleichzeitig kondensieren wir mit einigen Hot-Spots sicherheitstechnisches Angebot und Know-how“, so Iris Jeglitza-Moshage. Damit stellt die Geschäftsleiterin der Messe Frankfurt unter anderem auf das Special-Interest-Thema „Notfallbeleuchtung“ in Halle 8.0 ab oder auch auf die internationale Plattform für vernetzte Sicherheitstechnik in der Halle 9.1 – „Intersec Building“.