

Vernetzte Gebäudesicherheit

Wie fortschreitende Digitalisierung und zunehmende Konnektivität Gebäude sicherer machen

Die Digitalisierung und Vernetzung von Gebäuden steht zwar noch am Anfang, aber bereits jetzt eröffnet sie neue Möglichkeiten für die Gebäudesicherheit. Gleichzeitig stehen Betreiber und Eigentümer vor neuen Herausforderungen, denen sie sich stellen müssen.

Zum einen können vernetzte Tür-, Zutritts-, Rauchmelde- und andere smarte IoT-Systeme die Sicherheit von Menschen und Material auf ein neues Level heben. Zum anderen macht die steigende Vernetzung und Verschmelzung von IT (Informational Technology) und OT (Operational Technology) Gebäude auch anfälliger für Cyberangriffe, gegen die man sich absichern muss.

Hinzu kommen die Vorgaben von Versicherern, zunehmende Sicherheitsansprüche und die steigende Komplexität der technischen Möglichkeiten, die es nicht gerade einfacher machen. Wir verraten, worauf es ankommt, werfen einen Blick auf das, was heute schon möglich ist, und wagen einen Ausblick darauf, was morgen möglich sein wird.



Wenn aus Daten Insights werden

Das IoT wird als ein Netzwerk physischer, mittels Sensorik und Software über das Internet verbundener Geräte verstanden, um Daten zu sammeln und auszutauschen. Die dabei generierten Mengen sind gewaltig.

Mit den rohen Informationen allein kommt man allerdings nicht weit. Nur im richtigen Kontext können die Daten den Mehrwert liefern, den es für smarte Use Cases braucht. So kommen spezielle Tools und Algorithmen zum Einsatz, die die in unterschiedlichsten Formaten vorhandenen Daten auslesen, auswerten und visuell aufbereiten. Künstliche Intelligenz (KI) und maschinelles Lernen treiben die Entwicklung voran, indem die Analyseprozesse selbsttätig immer weiter trainiert, verfeinert und verbessert werden.

Letztendlich entstehen nutzbare Insights, die auf Dashboards dargestellt bei der Verwaltung und (automatisierten) Steuerung wichtiger Gebäudesysteme helfen. Und die die Möglichkeit bieten, neue Anwendungen, Services und Geschäftsmodelle zu entwickeln, die heute noch gar nicht denkbar sind.

Wie Vernetzung und Digitalisierung die Gebäudesicherheit revolutionieren

Das Internet der Dinge (engl. Internet of Things bzw. IoT) bildet das Fundament für digitalisierte und vernetzte Gebäude. Zusammen mit modernen Analyse-, Steuerungs- und Automatisierungstechnologien macht es viele smarte und auch sicherheitsrelevante Funktionen möglich.

Denn als Teil des IoT sammeln Geräte und Sensoren wie z. B. Präsenz- und Bewegungsmelder, Kameras, Temperaturfühler oder Lichtmesser unzählige Daten, damit Gebäudemanagementsysteme diese analysieren und mit Aktoren gezielt auf dynamische Ereignisse reagieren können. Dabei erfolgt die Kommunikation der einzelnen adressierbaren Geräte über vereinheitlichte Standards und Protokolle (KNX, BACnet, LonWorks etc.), die Daten und elektronische Impulse wie auf Nervenbahnen übertragen.

Vernetzte Türen fürs Condition Monitoring

Und wenn das Internet der Dinge die Grundlage für ein umfassendes Gebäudemanagementsystem (GMS) bildet, dann sind vernetzte Türen ein wichtiger Teil davon. Denn in ihrer Funktion als Gebäudezugang, Notausgang oder geschützte Verbindung zu Räumen leisten sie einen entscheidenden Beitrag zur gesamten Gebäudesicherheit. Zusätzlich erfüllen sie wichtige technische Vorgaben zum Brand- und Schallschutz sowie zur Barrierefreiheit.

Sind die Zutrittsanlagen via Schnittstellen (Application Programming Interface, API) in die Gebäudeautomation eingebunden, kommen weitere sicherheitsrelevante Vorteile hinzu:

- Türen lassen sich aus der Ferne überwachen und gezielt steuern.
- Durch das sogenannte Condition Monitoring können sie selbstständig und proaktiv Warn- und Zustandsmeldungen senden.
- Leistungsanalysen lassen sich in Echtzeit durchführen.
- Die vorausschauende Wartung (Predictive Maintenance) minimiert Ausfallzeiten und erhöht die Sicherheit.
- Die Gebäudesicherheit beeinflussende Defekte können durch remote durchführbare Maßnahmen vermieden oder durch schnellere Reaktionszeiten besser eingedämmt werden.

Vorausschauende Wartung für zukunftssichere Planung

Eine moderne Monitoring-Software sorgt also dafür, dass weniger Mängel auftreten – sei es durch Materialdefekte, Fehlfunktionen oder Verschleiß. Vor allem die dadurch mögliche vorausschauende Wartung (Predictive Maintenance) spielt eine entscheidende Rolle für die Gebäudesicherheit: Indem sich mögliche Probleme schon beheben lassen, bevor sie überhaupt akut werden, lassen sich Ausfallzeiten gezielt minimieren.

Betreiber können den Servicestatus jeder Tür einfach verfolgen und Ersatzteile rechtzeitig bestellen. Die Wartung läuft durch den digitalen Ansatz zudem koordinierter und zeitsparender ab. Dazu kommt noch der große Vorteil, dass in Zeiten erhöhten Fachkräftemangels der Dienstleistungs- und Personaleinsatz effektiv minimiert wird.

Personenströme und Raumauslastung managen

Ganz aktuell zeigt auch der Blick auf die gestiegenen Hygiene- und Infektionsschutz-Anforderungen, wie wichtig es ist, die Personenströme und Raumauslastungen im Betriebsalltag von Gebäuden zu verwalten. Auch bei Großveranstaltungen oder der Gebäudeentfluchtung kommt es auf eine zuverlässige Steuerung an. Das vernetzte Asset Management spielt hier seine Stärken voll aus, da man in Echtzeit auf spezielle Gegebenheiten reagieren und steuernd eingreifen kann.

Zudem spielt die Normenkonformität im Gebäudebetrieb eine wichtige Rolle. Und wenn historische Daten z. B. für Sicherheitsaudits zur Verfügung stehen, sind diese digital umso effizienter bewältigt. Hinzu kommt: Wer stets die geforderte Compliance einhält oder durch digitale Lösungen einen sichereren Gebäudebetrieb vorweisen kann, spart mit günstigeren Versicherungspolizen auch noch Kosten ein.



Zutrittssysteme stets up to date halten

Natürlich dienen auch Zutrittssysteme der Gebäudesicherheit. Da sich die jeweiligen Rechte meist aus der Ferne vergeben und wieder entziehen lassen – z. B. via digitalen Smartphone-Schlüssel über Mobile Access –, sind auch sie vernetzt. Und dabei können sie immer nur so gut abgesichert sein, wie es die aktuellen Sicherheitsstandards sind, die sich fortlaufend ändern. Ob es also um die elektronische Zutrittskontrolle, Zeit- und Betriebsdatenerfassung oder das komplette, zugrundeliegende Betriebssystem geht – höchste IT-Sicherheit erreicht man nur, wenn man sie kontinuierlich hinterfragt, kontrolliert und überwacht.

Den wichtigsten Punkt kann man dabei nicht oft genug wiederholen: Nur wer seine Software regelmäßig updatet, profitiert von den neuesten Erkenntnissen und den umfangreichen internen und externen Tests zur IT-Sicherheit von Zutrittslösungen, die auch wir regelmäßig durchführen.

Natürlich liefert dabei schon die Technik viele Angriffspunkte. Was aber viele vergessen, ist die Tatsache, dass oft der Mensch das schwächste Glied in der Sicherheitskette ist. Deshalb ist es genauso wichtig, die eigenen Mitarbeiter und Kunden immer wieder für die möglichen Gefahren zu sensibilisieren.

Funkrauchmelder und vernetzte Feststellanlagen

Auch in Sachen vorbeugender Brandschutz schreitet die technische Entwicklung voran. Dabei verlieren Stand-alone-Rauchmelder zunehmend an Bedeutung. An ihre Stelle treten vernetzte Funkrauchmelder, die mit sogenannten Gateways kommunizieren, Alarmer direkt an definierte Stellen weiterleiten und schnellere Reaktionen ermöglichen. Ein weiterer Faktor sind Feststellanlagen:

- Damit diese im Alarmfall sicher schließen, müssen Errichter und Betreiber gewährleisten, dass sie mit Brandmeldern und Handauslösetastern ausgestattet sind.
- Die dafür nötige Verkabelung stellt aber oft eine unflexible Lösung dar.
- Deutlich komfortabler sind moderne Funk-Feststellanlagen, die unabhängig von vorgelagerten Gewerken funktionieren und bei denen keine Eingriffe in die Bausubstanz nötig sind.

So lassen sich Feststellanlagen um die Möglichkeit erweitern, mehrere drahtlose Funkteilnehmer an den Alarmeingang von Auslösevorrichtungen anzuschließen. Im Ernstfall schließen die Türen dann automatisch, um die Verbreitung von Rauch und Feuer zu verhindern.

Blickt man weiter in die Zukunft, werden Rauchwarnmelder wohl nicht nur verstärkt mit elektronischen Systemen, sondern zunehmend auch mit Menschen kommunizieren. Sie geben dann ihren jeweiligen Status verständlich aus und vereinfachen die Bedienung. Indem sie eine ständige Eigendiagnose betreiben, wird es durch die Wartungsfreiheit vielleicht auch eine Sache weniger geben, um die man sich sorgen muss. Oder zumindest wird es auch hier durch die Predictive Maintenance möglich sein, die Sicherheit vorausschauend zu steigern und den Personalaufwand für Serviceeinsätze zu reduzieren.

Cyber Security für Smart Buildings

Das Internet der Dinge strukturiert also viele Aspekte eines Gebäudes neu. Die zunehmende Vernetzung smarter Gebäude lässt allerdings auch das Bedrohungsrisiko steigen. Das liegt in erster Linie daran, dass durch die erhöhte Konnektivität verschiedenster Systeme mit unterschiedlichen Schnittstellen bis ins Internet auch die Angriffsfläche steigt. Vereinfacht gesagt, haben Hacker einfach mehr Möglichkeiten und Ziele, die sie attackieren können.

Besonders prekär wird es, wenn sich nicht nur private oder gewerbliche Gebäude immer mehr vernetzen, sondern auch sicherheitssensible Einrichtungen wie Krankenhäuser, Flughäfen oder andere öffentliche Gebäude immer smarter werden. Neben Datenverlusten und manipulierten Systemen können hier auch Menschenleben gefährdet sein.

Innere Werte nach außen absichern

So liegt der wichtigste Aspekt bei der Cybersicherheit darin, die Absicherung nach außen zu gewährleisten:

- Virtual Private Networks (VPNs) und Access Gateways können dafür sorgen, dass das Gebäudenetzwerk über die gesamte Infrastruktur geschützt und sämtliche Verbindungspunkte abgesichert sind.



- Zudem verhindert die virtuelle Sicherheitsschicht des VPNs, dass einzelne IoT-Komponenten von außen sichtbar und damit gezielt angreifbar sind.
- Damit sich ins Netzwerk eingedrungene Schadsoftware nicht weiter ausbreitet, kommt die Technologie der Mikrosegmentierung zum Einsatz, mit der einzelne Gebäudesysteme in Subnetze zusammengefasst werden, die mit zusätzlichen Barrieren einzeln abgesichert sind.
- Auch ist es unumgänglich, Nutzerrollen klar zu definieren und Zugriffe zu authentifizieren. Das Prinzip ähnelt ein wenig der Zutrittskontrolle, nur eben in virtueller Form. Eine gute Nachricht zumindest lautet, dass auch die Hersteller von Technologien für die Gebäudeautomation das Thema verstärkt im Fokus haben: Moderne Verschlüsselungstechnologien werden für die geschützte Datenübertragung bereits hardwareseitig in einzelne Komponenten integriert.

Pentests und Security Operations Center

Eine der wirkungsvollsten Strategien gegen Cyberangriffe sind sogenannte Penetrationstests oder kurz Pentests. Dabei werden unabhängige IT-Experten von Unternehmen beauftragt, die Sicherheit ihrer Software-Systeme zu testen. Die auf derartige Angriffe spezialisierten Partner arbeiten mit den gleichen Mitteln und Methoden, die Cyberkriminelle einsetzen würden, um unautorisiert z. B. in Zutrittslösungen einzudringen. So können Pentests dabei helfen, schnell auf neue Angriffsmuster zu reagieren und mögliche Schwachstellen frühzeitig zu identifizieren.

Wer über das nötige Budget verfügt oder spezielle Sicherheitsanforderungen hat, kann auch ein Security Operations Center (SOC) einrichten, in dem sämtliche Sicherheitsoperationen sowohl der Information Technology als auch der Operational Technology zusammenlaufen. Hier arbeiten Security-Analysten mit ausgewählten Tools und Prozessen zusammen, um jederzeit ein umfassendes Bild der Gefährdungslage zu haben und entsprechend reagieren zu können.

Umfassende Transparenz für mehr Sicherheit

Der Vorteil digitaler Gebäudekonnektivität liegt vor allem in der erhöhten Transparenz begründet, die in Echtzeit Einblicke in Leistungsdaten, Zustände und weitere Bereiche gibt. Im Bereich der Cyber Security spricht man von einer gesteigerten Visibility, die mehr denn je auch für vernetzte Gebäude gewährleistet sein muss.

Dabei machen IoT-Lösungen und deren zugrundeliegende Datenanalysen völlig neue Interaktionen und damit Anwendungen möglich. Die Vorteile reichen von vereinfachter Wartung über erhöhte Kontrolle und gesteigerte Energieeffizienz bis hin zu mehr Gebäudesicherheit. Dazu müssen digital vernetzte Gebäudelösungen die anfallenden Betriebs- und Leistungsdaten nicht nur

sammeln, sondern auch analysieren, auf übersichtlichen Dashboards visuell aufbereiten und für den Endanwender nutzbar machen. Nicht nur am Ort des Geschehens, sondern im besten Fall über die Cloud auch Remote, sofort über mehrere Standorte oder auch über einen längeren Zeitraum hinweg. Praktikable Lösungen gibt es dafür schon heute – und sie entwickeln sich rasant weiter.

Wenn sich dann digitale Ökosysteme ausbilden, in denen vielleicht nicht nur einzelne Gebäude, sondern ganze Viertel oder sogar Smart Cities miteinander vernetzt sind und Transparenz der vorherrschende Zustand ist, sind die vielfältigsten Anwendungen denkbar. Wir jedenfalls denken sie mit Sicherheit mit.

Sie möchten Gebäude sicherer gestalten?

Oder haben weitere Fragen? Kontaktieren Sie uns für alles rund um den Betrieb und Zutritt zu Gebäuden und Räumen aus einer Hand.

Über dormakaba

Die dormakaba Deutschland GmbH bietet ein umfassendes Portfolio an Produkten, Lösungen und Services rund um die Tür sowie den sicheren Zutritt zu Gebäuden und Räumen aus einer Hand. Dies umfasst Schließsysteme, voll vernetzte elektronische Zutrittslösungen, physische Zugangs- und automatische Türsysteme, Türbänder, Beschläge, Türschließer und -stopper, Zeiterfassung, Betriebsdatenerfassung, Hotelschließsysteme und Hochsicherheitsschlösser.

Mit mehr als 16.000 Mitarbeitenden und zahlreichen Kooperationspartnern stehen wir Ihnen vor Ort in über 130 Ländern zur Seite. So profitieren Sie weltweit von zukunftsfähigen Produkten, Lösungen und Services, die Ihnen ein nachhaltiges Gefühl der Sicherheit geben.

Technische Änderungen vorbehalten.
© 2021 dormakaba. Stand 12/2021

Haben Sie Fragen? Wir beraten Sie gerne und freuen uns auf Sie.

dormakaba Deutschland GmbH | DORMA Platz 1 | DE-58256 Ennepetal | T +49 2333 793-0 | info.de@dormakaba.com | www.dormakaba.de
dormakaba Luxembourg SA | Duchscherstrooss 50 | LU-6868 Wecker | T +352 26710870 | info.lu@dormakaba.com | www.dormakaba.lu
dormakaba Austria GmbH | Ulrich-Bremi-Strasse 2 | AT-3130 Herzogenburg | T +43 2782 808-0 | office.at@dormakaba.com | www.dormakaba.at
dormakaba Schweiz AG | Mühlebühlstrasse 23 | CH-8620 Wetzikon | T +41 848 85 86 87 | info.ch@dormakaba.com | www.dormakaba.ch