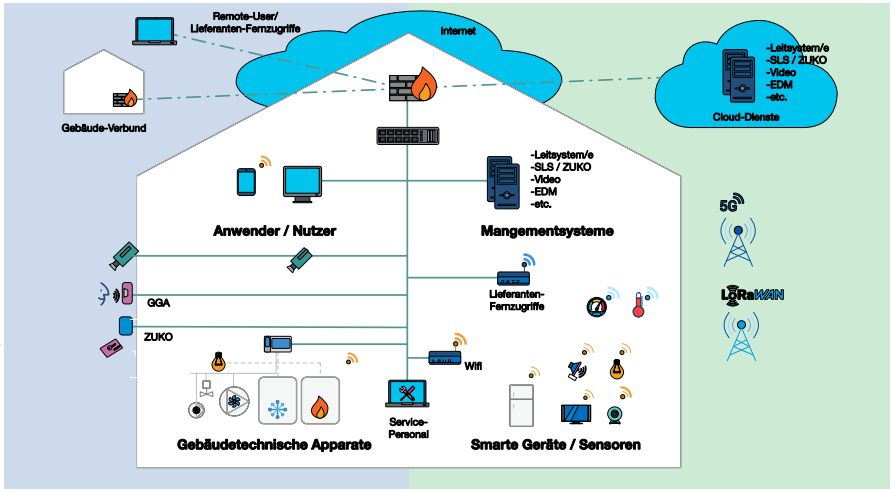
Cybersecurity im Gebäude

Gebäude werden immer digitaler und vernetzter. Dies bietet neue Möglichkeiten für Arbeitsplatzmanagement, Elektromobilität oder Energiemanagement. Gleichzeitig steigen aber auch die Risiken, wie ein Gebäude böswillig manipuliert oder die Gebäudetechnik genutzt werden kann, um in die Systeme der im Gebäude ansässigen Firma oder der Bewohner einzudringen.



Angriffspunkte in Gebäuden

Von **Tania Messerli**

Neben den bestehenden Haftungsfragen ergibt sich damit für den Immobilieneigentümer ein weiteres Thema, das er strategisch angehen muss. Bereits bei der Projektentwicklung muss über die Digitalisierung eines Objekts nachgedacht werden. Dies ist bisher eine grosse Herausforderung, da sich die Anforderungen je nach Nutzung ändern und auch in keinem SIA-Prozess abgebildet sind. Cybersecurity, Gebäudeautomation und planungs- und baubegleitendes Facility Management sind Querschnittsaufgaben, die den Betrieb finanziell erheblich entlasten, wenn sie von Anfang an sauber geplant werden.

AUTOR

Tania Messerli

Geschäftsführerin Gebäude Netzwerk Initiative

> *g-n-i.ch*

Bereits Kleinigkeiten können zu unerwünschten Effekten führen. Während des Baus werden 5G-Router zur einfachen und effizienten Ferninbetriebnahme bei verschiedenen Gewerken platziert. Diese verbleiben nach Fertigstellung oft mit funktionierendem Sender im Objekt oder sind ggf. sogar mit der Haustechnik verbunden und stellen somit ein potenzielles Einfallstor dar.

Der Bauherr und Eigentümer hat die Aufgabe, bei der Ausschreibung von Neu- und Umbauten einen geeigneten Weg zu finden, dass diese Einstiegspunkte in das Gebäudenetz bzw. in das Netz des Nutzers reduziert werden. Für ihn stellen sich zwei grundsätzliche Fragen

1. Wie viel Technik soll verbaut werden? Wie kann das Objekt nach physikalischen Prinzipien nachhaltig bzw. kreislauffähig gestaltet werden, sodass bestimmte Anlagen gar nicht notwendig sind und das Gebäude dadurch in verschiedener Hinsicht robuster wird?
2. Wie soll die Steuerung der haustechnischen Anlagen und Raumkomponenten gelöst werden? Welche Aufgaben werden kabelgebunden durch die klassische Gebäudeautomation und welche durch IoT-Geräte und Sensoren bzw. mit WLAN etc. ausgestattete Anlagen und Geräte erledigt? Diese Entscheidung beeinflusst das Baubudget, aber auch die Betriebskosten und die Cybersecurity bzw. den Umgang mit Mieterausbauten und Geräten der Mieter und deren Serviceprovider.

Akuter Handlungsbedarf im Facility Management

Das Facility Management steht vor einer gewaltigen Aufgabe, die sich in der Digitalisierung der Gebäude manifestiert. Vielfach verlief dieser Prozess bisher schleichend und im Hintergrund, sodass kaum finanzielle und personelle Ressourcen dafür bereitgestellt wurden.

Grosse Unternehmen sind hier bereits gut aufgestellt, da sie von ihrer IT-Abteilung viele Vorgaben erhalten und aktiv in die Diskussionen eingebunden werden bzw. gebäudetechnische Umbauten eine Vielzahl von Prüfpunkten durchlaufen müssen, um überhaupt realisiert zu werden. Eine gut geführte Unternehmens-IT gewährleistet somit in bestimmten Bereichen auch eine höhere Sicherheit für die OT (Haustechnikanlagen).

Was ist aber mit der Mehrheit des Gebäudebestands von kleineren Eigentümern sowie den Anlageobjekten, wo sich niemand darum kümmert? Die sind genauso vernetzt mit all ihren ungesicherten Geräten. Solange die Geräte nicht sprechende Namen haben, ist dies ein bedingter Schutz bzw. das Interesse für

Hacker weniger gross, wenn sie nicht wissen, ob sich hinter der Steuerung ein Serverraum oder ein einfacher Abstellraum befindet. Meistens steht aber eine offen zugängliche Visualisierung zur Verfügung und somit ist die Gefahr sehr hoch.

In der Abbildung sind die verschiedenen Angriffspunkte aufgezeigt. Dadurch wird klar, wie vielfältig diese sein können und was für eine Mammutaufgabe auf das Facility Management zukommt, wenn nur alle Felder minimal gesichert werden sollen.

Strategische Herangehensweise

Eine so vielfältige Aufgabe kann auf verschiedene Weise angegangen werden. Wichtig ist aber zu wissen, dass es sich hierbei um einen Prozess handelt. Dieser ist beim Eigentümer, Verwalter wie Facility Manager sowie dem Mieter zu etablieren und laufend zu pflegen. Regelmässige Schulung der Mitarbeitenden und eine gezielte Abwägung zwischen Kosten und Nutzen einzelner Massnahmen sind die Basis. Wichtig ist eine Vorgehens-Methodik zu finden, welche für die Objekte und das Budget passt und umsetzbar ist.

Zentrale Aspekte sind der Passwortschutz, Prüfung der Vorgaben an Service-Unternehmen, aber auch regelmässige Updates aller Haustechniksysteme, die am Netz hängen und Überlegungen, welche Daten wo in einer Cloud gespeichert sind. Durch Zonierung der verschiedenen IT-Systeme, einer redundanten Datenhaltung sowie mit einem Notfallplan auf Papier, der regelmässig aktualisiert und durchgespielt wird, kann der Schaden in Grenzen gehalten werden. Denn die Angreifer gehen über alle Geräte und Möglichkeiten und daher ist es leider oft nur eine Frage der Zeit, bis die eigenen Gebäude und Anlagen bzw. die Firmen in den schlecht gesicherten Gebäuden betroffen sind. Das Thema Cybersicherheit im Gebäude ist daher von allen Beteiligten ein ernst zu nehmender laufender Prozess.

Weiterbildung

GNI bietet in Zusammenarbeit mit asut einen Kurs zur Sensibilisierung an und zeigt Hilfsmittel wie die Cybersecurity im Gebäude erhöht werden kann. Dabei werden die technischen und prozessualen Aspekte laufend durch juristische Aspekte ergänzt. Innert zwei Halbtagen erhalten Teilnehmende einen Überblick und können dann mit diesem Wissen die Handlungsfelder analysieren, bzw. die Sicherheit im Gebäudebestand erhöhen.
Programm und Anmeldung via **>** *g-n-i.ch*