KOMMENTAR DIGITALISIERUNG INNOVATION

Smart Home: Kein Zutritt für Hacker

06.11.2023 / Österreich / Karin Bornett

Damit Gebäude smart werden, müssen sie Daten sammeln. Welche das sind. Was damit passiert. Und wie sie nicht in falsche Hände geraten. Ein Überblick.

Moderne Gebäude sind intelligent. Dank vernetzter, digitaler Sensoren und Überwachungssystemen können sie die Heizung, die Kühlung, die Beschattung und die Beleuchtung bis hin zur Gartenbewässerung selbst steuern. Das spart menschliche Ressourcen im Betrieb und bei der Wartung. Außerdem arbeiten automatisierte Gebäudesysteme energieeffizienter. Und sie erkennen und melden Schwachstellen oder technische Gebrechen frühzeitig.

Die Daten

Smarte Gebäude können je nach Ausführung eine Vielzahl verschiedener Daten erfassen und verarbeiten: Temperatur, Luftfeuchtigkeit, Lichtintensität, CO2-Gehalt der Luft. Anzahl der Personen in einem Raum, Energieverbrauch, Betriebsdaten von Geräten wie die Betriebsdauer der Heizung oder die Kapazität der PV-Anlage, Einsatzstatus der Fahrstühle oder Daten von Zutritts- und anderen Sicherheitssystemen. Ohne diese Daten bleiben Gebäude aufwendig in der Wartung, träge bei der Behebung von Mängeln und schwerer kalkulierbar – beispielsweise in Sachen Energieversorgung oder Betriebskosten. Insgesamt sind Smart Buildings effizienter als konventionelle Gebäude. Laut **Deloitte Smart Building Studie 2023** waren die Betriebskosten von zwanzig analysierten Smart Buildings sogar bis zu 26 % niedriger als jene von konventionellen Gebäuden. Der Energieverbrauch war durchschnittlich um 34 % geringer. Gleichzeitig wurde der Komfort in den untersuchten Smart Buildings als sehr hoch wahrgenommen. Um die Klimaziele zu erreichen und im Angesicht steigender Bau- und Energiekosten werden Gebäude in Zukunft nicht ohne smarte Systeme auskommen.

Die Gefahren

(c) generiert mit bing

Die andere Seite der Medaille zeigt im Extremfall sehr beunruhigende Szenen: Kameras werden zum Ausspionieren von Bewohner*innen genutzt, die Stromversorgung manipuliert oder das Zutrittssystem von Fremden deaktiviert. Unsichere Systeme öffnen Hacker*innen Tür und Tor. Buchstäblich. Mögliche Motive: Datenklau für den Schwarzmarkt, Erpressung der Betreiber*innen oder Übernahme der Kontrolle für Einbruch und Diebstahl vor Ort. Im April 2022 sind zum Beispiel Hacker*innen in das Steuerungssystem des Wiener Stephansdoms eingedrungen und haben dessen Glocken um 02:00 Uhr morgens für gut zwanzig Minuten läuten lassen. Außer der kurzen Irritation der Bevölkerung ist zum Glück kein Schaden entstanden. Das Motiv dieser Tat? Unklar. Aber selbst wenn der Fall unter Jugendstreich abgetan werden könnte, machen Vorfälle wie dieser klar, wie wichtig die Cybersecurity von Gebäuden ist – nicht nur im Neubau.

Die Maßnahmen

Zum Schutz gegen Angriffe von außen und zur Gewährleistung eines reibungslosen Betriebs muss jedes intelligent vernetzte Haus ein umfassendes Sicherheitskonzept haben – sowohl für die Betriebs- als auch die Informationstechnik. Die datenbasierten Lösungen und Services von Smart Buildings nutzen Cloud-Plattformen und Internet of Things-Infrastrukturen. Um Daten und Systeme vor Angriffen zu schützen, sind alle Verbindungen verschlüsselt und mit sicheren Passwörtern und Zugangscodes versehen. Die Verantwortung für die Cybersicherheit von ganzen Gebäuden liegt bei den Eigentümer*innen beziehungsweise den Betreiber*innen. Wichtig ist, dass das Sicherheitskonzept laufend evaluiert und angepasst wird. Und wer zu Hause Smart Home Systeme nutzt, sollte unbedingt auch selbst folgende Maßnahmen zur Gewährleistung der Cybersecurity treffen:

- Kaufen Sie nur Smart Home Geräte, welche die DIN VDE V 0826-1 erfüllen.
- Achten Sie auf verschlüsselte Verbindungen nach aktuellen Standards.
- Nutzen Sie eine Firewall und ein Virenschutzprogramm.
- Achten Sie darauf, sichere Passwörter einzurichten.

In Deutschland warnt das Bundesamt für Verfassungsschutz Ende August 2023 vor Cyberangriffen chinesischer Hackergruppen auf Privatpersonen. Diese würden sich häufen und vor allem über Smart Home Systeme passieren.

Das Fazit

Intelligent vernetzte, gut geschützte Gebäude sparen Ressourcen, während sie hohen Komfort bieten. Sie sind ein wichtiger Baustein zur Erreichung der Klimaziele. Cyberattacken sind zwar eine Gefahr, ausgefeilte Sicherheitskonzepte und -technologien breiten aber einen umfassenden, virtuellen Schutzschirm über die Systeme. Das Bewusstsein bei Eigentümer*innen und Unternehmen ist groß und wird weiter wachsen. Im Jahr 2022 sollen in Deutschland laut Statista insgesamt rund EUR 7,8 Mrd. für IT-Sicherheit ausgegeben worden sein; weltweit rund USD 71 Mrd. Im Jahr 2025 rechnet man mit Ausgaben von rund EUR 10,3 Mrd. Euro in Deutschland.