

IM FOKUS: DIGITALISIERUNG

Cyberrisiken in der Gebäudeautomation

» Vernetzte Haustechnik bringt Effizienz und Komfort, macht Gebäude aber auch anfällig für Cyberangriffe. Facility Managerinnen und Hauswarte stehen damit vor Aufgaben, die weit über den klassischen Unterhalt hinausgehen.

Autorin: Sabine Born

Im Versuchslabor für Cybersicherheit der Hochschule Luzern werden reale Gebäudeautomationsanlagen nachgebildet, um Sicherheitsversuche und Schulungen durchzuführen.

Auch wenn das Ausmass schwer zu beziffern ist, müssen Betreiber damit rechnen, dass technische Anlagen oder Gebäudeleitsysteme ins Visier von Hackern geraten können. «Bei klassischer Haustechnik wie Heizungs- und Lüftungsanlagen stellt vor allem der Fernzugriff ein Einfallstor dar», erklärt Olivier Steiger, Professor an der Hochschule Luzern und Vizepräsident der Gebäude Netzwerk Initiative (GNI). «Gehackte Anlagen können ausgeschaltet oder beschädigt werden, zum Beispiel indem manipulierte Wärmepumpen permanent ein- und ausgeschaltet werden oder eine Lüftung gegen geschlossene Klappen betrieben wird.»

Doch nicht nur sicherheitsrelevante Anlagen stehen im Fokus. Auch Reinigungs- und Mähroboter sind für Hacker interessant, da sie sensible Betriebsdaten wie Grundrisse erfassen, während Videoüberwachungssysteme und Sensoren mit Sprachsteuerungen Bewegungsprofile oder Audioaufnahmen liefern. «Eine neue und bislang wenig beachtete Gefahr ist, dass solche Daten für das Training von KI genutzt werden könnten. Stimmen und Videodaten eignen sich zudem für die Erstellung täuschend echter Fake-Videos», warnt Olivier Steiger.

Und auch wenn der Ausfall einer gehackten Lüftung nicht gravierend wirkt, sorgt eine lahmgelegte Heizung bereits für mehr Unbehagen und blockierte Türen oder stillstehende Lifte bergen bereits klare Sicherheitsrisiken. Hinzu kommen mögliche finanzielle Schäden, zum Beispiel, wenn es zu Produktionsstillständen kommt oder Rechenzentren mangels Kühlung heruntergefahren werden müssen. Zudem sind Erpressungsversuche über abgeflossene Daten denkbar, ebenso wie der Missbrauch von Präsenzinformationen: Wenn bekannt ist, wann Wohnungen oder Büros leer stehen, steigt das Einbruchrisiko erheblich.

VERANTWORTUNG UND ZUSTÄNDIGKEITEN

Wer aber trägt die Verantwortung für die Sicherheit vernetzter Geräte in einem Gebäude? «Im Grundsatz



Bild: +vg

die Geschäftsleitung, die in Grossunternehmen durch IT-Fachleute ergänzt wird», betont der Experte. «Bei KMU gibt es gelegentlich einen IT-Sicherheitsbeauftragten oder man zieht externe Fachleute bei. In kleinen Organisationen hat man im besten Fall jemanden, der IT-affin ist, häufig aber auch gar niemanden.»

Damit rückt auf der operativen Ebene eine weitere Gruppe in den Fokus: Facility Managerinnen und Hauswarte. Sie sind in der Regel keine IT-Experten, nehmen aber dennoch eine Schlüsselrolle ein, da sie täglich an den Anlagen arbeiten. «Sie sind gewissermassen das Frühwarnsystem: Sie sind täglich im Gebäude, erkennen Störungen oder ungewöhnliches Verhalten. Wenn sich Systeme plötzlich anders verhalten, ohne dass klar ist warum, sollten sie sich fragen, ob es mit Cybersicherheit zu tun haben könnte», sagt Olivier Steiger.

Zugleich fungieren Hauswarte als Gatekeeper: Sie kontrollieren nicht nur den Zutritt externer Dienstleister, sondern stellen auch sicher, dass die Arbeiten beaufsichtigt werden. «Vor Ort kann ein Handwerker mehr anrichten als über Fernzugriff», warnt Olivier Steiger. Verändert ein Externer also Einstellungen an Anlagen, müssen Facility Manager dies erkennen, verstehen und die ursprüngliche Konfiguration bei Bedarf wiederherstellen können. Ebenso zentral ist die Dokumentation: Alle Vorfälle und Interventionen an Anlagen müssen festgehalten werden.»

NEUE KOMPETENZEN IM DIGITALEN ALLTAG

Für Hauswarte und Facility Manager rücken damit neue Kompetenzen ins Zentrum. Sie benötigen beispielsweise ein Grundverständnis für Passwortsicherheit, Sicherheitszertifikate oder für das Software-Update- und Patchmanagement. Zur Erklärung: Ein Sicherheitspatch ist vergleichbar mit einem Pflaster, also eine kleine Korrektur, die eine Sicherheitslücke schliesst. Ein Update hingegen ist ein grösseres Paket, das mehrere Fehler gleichzeitig behebt und neue Funktionen aufspielt.

«Kommt also ein Patch oder ein Update, muss es jemand einspielen. Schwierig ist das nicht, aber oft wird es nicht gemacht, weil Anlagen für Updates teilweise abgeschaltet werden müssten», weiss Olivier Steiger. «Ein erster Schritt ist also die Definition einer Person, die für Updates zuständig ist. Ist es nicht der Hauswart, weil die nötige Affinität fehlt, kommen externe Partner wie Systemintegratoren, Hersteller oder spezialisierte OT-Fachleute in Frage.»

Ein weiteres Problem betrifft Haustechnikanlagen, die gar nicht erst mit dem Internet verbunden sind und deshalb oft gar keine Updates erhalten. Diese müssten manuell via USB-Stick eingespielt werden, was jedoch häufig unterbleibt, weil kein Serviceabo



Bild: zvg

Olivier Steiger ist Professor am Institut für Gebäudetechnik und Energie IGE an der Hochschule Luzern und Vizepräsident der Gebäude Netzwerk Initiative (GNI).

besteht. Solange solche Anlagen offline bleiben, ist das Risiko überschaubar. Kritisch wird es dort, wo Systeme einen Fernzugriff erlauben: Unsichere Komponenten können dann zum Eintrittstor werden. Selbst wenn Anlagen nur ins LAN eingebunden sind, bestehen in der Regel Schnittstellen zum Gebäude-WLAN und schon ein einziges unsicheres Gerät kann Angreifern den Zugang öffnen.

«Mein Hauptfokus ist deshalb, das Bewusstsein für diese Thematik zu schärfen», sagt der GNI-Vizepräsident. «Viele sehen Cyberangriffe in der Gebäudeautomation nicht als grosses Problem. Doch mit der zunehmenden Vernetzung wächst die Angriffsfläche und ein Angriff kann weitreichende Folgen haben.» Facility Managerinnen und Hauswarte sollten sich deshalb absichern und die Geschäftsleitung in die Pflicht nehmen, die Organisation so aufzusetzen, dass sie entweder entsprechend geschult werden oder bei Bedarf Unterstützung durch Experten erhalten.»



Sabine Born
Redaktorin
Unterhaltplus.
Ersterscheinung
des Artikels:
Unterhaltplus
04-2025

