Smart, sicher und vernetzt

Connected Security in Gebäuden

Angesichts stetig steigender Risiken durch digitale Angriffe härtet die moderne Gebäudeautomation ihre Systeme kontinuierlich gegen unautorisierte Zugriffe ab.

Connected Security in Gebäuden erfordert ein konsequent abgestimmtes Zusammenspiel aus technischen, organisatorischen und benutzungsspezifischen Maßnahmen.

IT-Security ist mittlerweile auch in der Gebäudeautomation ein nicht mehr zu vernachlässigendes Thema. BACnet/SC, ein zusätzlicher Netzwerk-Layer zum weltweit verbreiteten BACnet-Standard, bietet eine Lösung für einen effektiven Schutz gegen Cyber-Kriminelle.

SAUTER Deutschland
www.sauter-cumulus.de

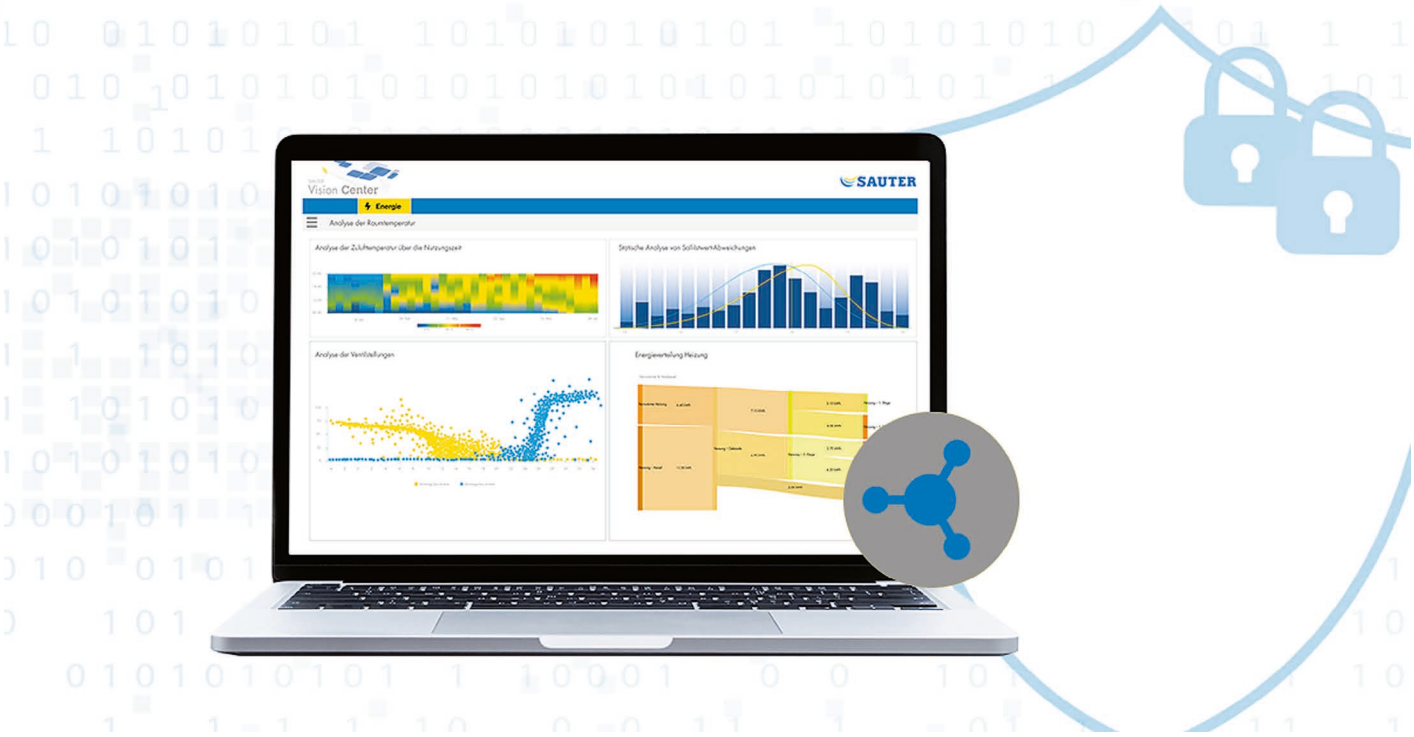
Die Awareness gegenüber der digitalen Bedrohung steigt

So schätzten im Jahr 2025 bereits rund 69% der deutschen Unternehmen das Risiko, Opfer eines Cyberangriffs zu werden, als hoch ein. Zehn Jahre zuvor lag der Anteil noch bei 34%.
Heutige Gebäudeautomationssysteme setzen fundamental auf aktuellen IT-Technologien und IT-Infrastrukturen auf. Dies bedeutet jedoch, dass eine moderne Gebäudeautomation – vergleichbar wie eine IT-Infrastruktur – betrachtet und abgesichert werden muss. Im Zeitalter herstellübergreifender Gebäudeautomation mit umfassender Vernetzung, Cloud-Dienstleistungen, Remote-Verbindungen und Digital Services sind Connected Security Strategien in der Immobilienwirtschaft zum zentralen Thema geworden.
Durch die Manipulation von Heizungs-, Lüftungs- und Klimaanlagen können digitale Angriffe die Nutzung von Büros stark beeinträchtigen oder Rechenzentren sogar komplett lahmlegen.

Eine Gebäudeautomation kann bei gemeinsam genutzten Infrastrukturen und nicht ausreichenden Sicherheitskonzepten als Einfallstor in andere IT-Bereiche ausgenutzt werden. Daher ist es heutzutage erforderlich die IT-Sicherheit der Gebäudeautomation bei jeder Planung im Rahmen einer Risikoanalyse zu bewerten. Das schreiben die Normen VDI 3814 und das VDMA-Einheitsblatt (EB) 24774 ausdrücklich vor. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät bei Gebäuden mit erhöhtem IT-Sicherheitsbedarf zu einer möglichst verschlüsselten Kommunikation wie beispielsweise BACnet/SC.

BACnet: offener Standard für die effiziente Gebäudeautomation

Gemäß der europäischen EPBD und des deutschen GEG ist für größere Nichtwohngebäude (>290 kW) eine Gebäudeautomation verpflichtend vorgeschrieben. Die hierdurch zu realisierenden



Die Gebäudemanagement- und Integrationsplattform SAUTER Vision Center macht Immobilien intelligenter, sicherer und effizienter.

Energieeinsparungen sprechen wie die gleichzeitigen Komfortsteigerungen für eine bedarfsgerechte Gebäudeautomatisierung.
Neben klassischen Raumparametern wie Temperatur oder Luftfeuchtigkeit können zum Beispiel Informationen über geplante und gemessene Raumbelegung oder Wetterdaten in das hochkomplexe Regelsystem mit einbezogen werden. So können Raumkonditionen komfortabel auch über eine Smartphone-App an individuelle Bedürfnisse angepasst werden.
Eine moderne Gebäudeautomation bietet zudem Fernwartungsmöglichkeiten für Digital Services Angebote sowie Analysen zur Auswertung aller aufgezeichneten Gebäudedaten oder digitale Gebäudemodelle zur vorausschauenden, energie- und komfortoptimierten Steuerung und Regelung.

BACnet/SC: Cyber-Security-Layer

Durch diese zunehmende Vernetzung von Gebäuden steigen die Risiken für Cyberangriffe. Dies kann ungeschützt zu Datenmanipulation, Datenverlust oder zum Ausfall der Gebäudeautomation führen, mit Auswirkungen auf den Geschäftsbetrieb oder gar Folgen wie Personenschäden. Um eine Gebäudeautomation vor solchen Angriffen zu schützen, wurden bewährte Kommunikations- und Sicherheitsstandards wie TCP/IP und TLS 1.3 in die BACnet Kommunikation der Gebäudeautomation integriert. Das Ergebnis ist der zusätzliche, neue BACnet/SC (BACnet Secure Connect) Transport-Layer.
Die BACnet-spezifischen Kommunikationsstrukturen und die BACnet Semantik ist vollständig kompatibel erhalten geblieben. Änderungen an einer Gebäudeautomationsprogrammierung der HLK-Funktionalität sind nicht erforderlich, denn alle BACnet-Dienste, -Objekte und -Properties bleiben gleich. BACnet/SC basiert außerdem auf den üblichen CAT5e- und CAT6-Verkabelungen oder Lichtwellenleitern; auch hier muss im Vergleich zum bisher üblichen BACnet/IP nichts umgerüstet werden. Hinzugefügt wird lediglich eine zentrale Komponente: der BACnet/SC-Hub. Er kann ebenso redundant ausgelegt werden, damit kein Single Point of Failure entsteht.
Für die sichere Datenübermittlung im BACnet/SC-Netz sind TLS-Zertifikate erforderlich, die regelmäßig aktualisiert werden müssen. Dabei kommt die schon bei HTTPS-Verbindungen bewährte Kombination aus öffentlichen und privaten Schlüsseln zum Einsatz. Hiermit lassen sich BACnet/SC-fähige Geräte und Systeme aus der Gebäudeautomation zugriffssicher in moderne IT-Infrastrukturen integrieren. Wer die Zertifikate manuell wechselt, sollte dies bei der jährlichen GA-Wartung oder spätestens nach 18 Monaten tun. BACnet/SC verfügt zusätzlich über eine eigene Geräteauthentifizierung.

BACnet/SC als KRITIS-Standard

In besonders gefährdeten Bereichen und insbesondere bei kritischen Infrastrukturen (KRITIS) führt angesichts der dramatisch verschärften Bedrohungslage an BACnet/SC kaum ein Weg mehr vorbei. Der BACnet/SC Transport Layer ist bei der Neuplanung wie auch in Bestandssysteme integrierbar. Vorhandene BACnet/IP-Segmente können bei Bestandsprojekten ebenfalls über BACnet/IP-zu-BACnet/SC-Router in eine neue BACnet/SC-Kommunikation integriert werden. BACnet/SC empfiehlt sich zudem immer, wenn Daten aus der Gebäudeautomation einen separierten, vertrauenswürdigen Bereich verlassen. Dies ist beispielsweise bei der Anbindung weiter entfernter Gebäudeteile und Liegenschaften der Fall oder bei den heutzutage sehr verbreiteten Cloud-Anwendungen. BACnet/SC steht hier für maximale Sicherheit, auch ohne zusätzliches VPN.
In der Praxis zeigt sich allerdings häufig, dass eine sorglose Anwendung selbst bei ausgereiften Hardware-Schutzkonzepten zum Risiko werden kann. Daher erfordert ein Sicherheitskonzept für die Gebäudeautomation neben der technischen Ausstattung auch die umfassende Schulung und Sensibilisierung aller Beteiligten im Hinblick auf potenzielle Angriffsvektoren.

Die Bedrohungslage hat sich dramatisch verschärft

Nicht zuletzt aufgrund der weltweiten Tendenz zur Konfrontation auf allen Ebenen. Das gilt auch für die Gebäudetechnik und ist durchaus ein Grund zu erhöhter Vorsicht, doch kein Grund zur Angst oder gar Panik. Es gibt heute ausgereifte Technologien, die Gebäudeautomationssysteme nahezu unerreichbar für Cyberkriminalität oder Sabotage machen. Wer sich auf zeitgemäße Hardware und einen kompetenten Lifecycle Partner verlässt, kann sich auf seine Gebäudetechnik verlassen.

Wer schreibt:

SAUTER Deutschland ist mit 100 Jahren Expertise spezialisiert auf die Bereiche Gebäudeautomation, Systemintegration, Facility Management sowie HLK Anlagenbau. ◄