Sichere Kommunikation als Grundlage moderner Gebäudeautomation

IT-Sicherheit in der vernetzten Gebäudetechnik

Der Security-by-Design-Ansatz sorgt für mehr IT-Sicherheit bei Anwendungen in der Gebäudetechnik. Hier erfahren Sie mehr darüber.

© tci GmbH

Die Digitalisierung von Gebäuden schreitet rasant voran: Steuerungen für Heizung, Lüftung, Klima (HLK), Beleuchtung, Jalousien, Zutritt, Videoüberwachung und Energiemanagement sind heute durchgehend vernetzt. Bei den ganzen Vorteilen in Sachen Effizienz und Funktionalität sollte man jedoch die IT-Sicherheit nicht aus den Augen verlieren. Neben der allgemeinen Betrachtung der verschiedenen Facetten der IT-Sicherheit in der Gebäudetechnik wird gezeigt, wie Gerätehersteller durch den Security-by-Design-Ansatz für eine Grundsicherheit auf Komponentenebene sorgen können.

Autor:
Gerhard Bäurle
freier Technikjournalist, für tci - Gesellschaft für technische Informatik mbH
www.tci.de

IP-basierte Kommunikation

Als Ergänzung zu proprietären Schnittstellen und Protokollen wird in der Gebäudetechnik zunehmend auf eine IP-basierte Kommunikation gesetzt. Spätestens mit der Integration von WLAN-Komponenten, Cloud-Diensten und App-basierten Steuerungen verschwimmen die Grenzen zwischen klassischer Gebäudesystemtechnik und Informationstechnik. Das erlaubt auch Remote-Zugriffe über Visualisierungspanels, Browser-Interfaces oder mobile Endgeräte über Gebäudegrenzen hinweg. Damit gewinnen Themen wie Authentifizierung, Verschlüsselung, Netzwerksegmentierung und Patch-Management an Bedeutung – auch und gerade im Elektrohandwerk.

Schnittstellen, Protokolle und Angriffsflächen

Wo früher potenzialfreie Kontakte oder serielle Schnittstellen dominierten, kommen heute zunehmend IP-basierte Protokolle wie BACnet/IP, KNXnet/IP, Modbus TCP oder MQTT zum Einsatz. Diese Standards ermöglichen herstellerübergreifende Kommunikation und eine flexible Systemintegration. Allerdings verfügen viele dieser Protokolle in ihren ursprünglichen Spezifikationen nicht über integrierte Sicherheitsmechanismen wie Verschlüsselung oder Authentifizierung – oder sie werden in der Praxis ohne deren Aktivierung betrieben. Das macht sie anfällig für Manipulation und unautorisierten Zugriff, sofern nicht zusätzliche Sicherheitsmaßnahmen getroffen werden.
Viele Komponenten – vom Raumcontroller bis zum Touchpanel – verfügen über integrierte Webinterfaces. Ohne zusätzliche Maßnahmen wie HTTPS-Verschlüsselung oder Zugangskontrolle können diese Schnittstellen potenziell von jedem erreicht werden, der sich im gleichen Netzwerk befindet.
Hinzu kommt: In vielen Projekten fehlt eine klare Trennung der Netzwerke. Gebäudetechnik, Büro-IT und Gäste-WLAN hängen nicht selten am selben Switch – ein konzeptioneller Fehler, der die Sicherheit der gesamten Anlage gefährdet. Für mögliche Angreifer bieten sich dadurch zahlreiche Einfallstore: sei es über ungesicherte Telnet-Ports, Fernwartungszugänge mit Standardpasswörtern oder veraltete Firmware-Versionen ohne aktuelle Sicherheits-Patches.

Sichere Kommunikation beginnt mit Planung

IT-Sicherheit lässt sich nicht nachrüsten – sie muss von Anfang an eingeplant werden. Dazu gehört in erster Linie eine saubere Netzwerkarchitektur: Die Trennung der Systeme über VLANs, Subnetze oder dedizierte physische Infrastruktur ist essenziell.
Kommunikationsverbindungen zwischen Komponenten – insbesondere bei Fernzugriffen – sollten grundsätzlich verschlüsselt sein. Ob HTTPS, SSH, TLS oder VPN: Eine unverschlüsselte Kommunikation in der Gebäudetechnik ist praktisch eine Einladung an potentielle Angreifer.
Auch im WLAN-Bereich ist Sorgfalt gefragt: WPA3 sollte der Standard sein, idealerweise ergänzt durch Client-Isolation, deaktiviertes WPS und ein separates Gäste-Netzwerk. Steuerungsgeräte wie Touchpanels oder Gateways sollten vorzugsweise per LAN angebunden sein, um Störungen und potenzielle Angriffe über Funkverbindungen zu vermeiden.
Ein weiterer wichtiger Punkt ist die Zugriffssicherheit. Systeme mit Benutzerverwaltung sollten nicht nur über starke Passwörter geschützt werden, sondern – wenn möglich – die Zwei-Faktor-Authentifizierung (2FA) unterstützen. So lässt sich verhindern, dass ein kompromittiertes Passwort allein zum Zugriff ausreicht.

Security by Design – was moderne Geräte leisten müssen

Sichere Kommunikation endet nicht an der Netzwerkkante. Auch die eingesetzten Geräte müssen heutigen Anforderungen genügen. Eine wachsende Zahl professioneller Hersteller, darunter tci, verfolgt deshalb bei den Touchpanels für die Gebäudeautomation das Prinzip „Security by Design".
Ein zentrales Element ist dabei der Einsatz von Secure Boot: Nur signierte Firmware und Betriebssystem-Komponenten werden beim Startvorgang der Touchpanels geladen – eine effektive Maßnahme gegen das Einschleusen von Rootkits oder manipulierten Images.
Ergänzt wird dieses Konzept durch den Einsatz eines Trusted Platform Modules (TPM). Dieser Sicherheitschip ist in der Lage, kryptografische Schlüssel und Zertifikate sicher zu speichern – unabhängig vom Betriebssystem. Das macht Angriffe auf die Vertrauensbasis der Geräte erheblich schwerer.
Ein weiterer Aspekt ist die Integrität des Dateisystems: Moderne Linux-basierte Panels setzen auf schreibgeschützte Root-Partitionen, um Manipulationen zuverlässig auszuschließen. Systemupdates werden über sichere, signierte Prozesse eingespielt – entweder manuell oder automatisiert über eine cloudbasierte Plattform mit End-to-End-Verschlüsselung.

Langfristige Sicherheit durch Update-Strategien

Ein weitverbreitetes Sicherheitsproblem in der Gebäudetechnik ist die Vernachlässigung von Firmware- und Software-Updates. Viele Systeme laufen über Jahre oder gar Jahrzehnte – häufig ohne je ein Update erhalten zu haben.
Das mag im Sinne von „never change a running system" nachvollziehbar erscheinen, ist jedoch riskant. Sicherheitslücken werden mit der Zeit bekannt und lassen sich von Angreifern gezielt ausnutzen. Daher sollte bereits bei der Geräteauswahl darauf geachtet werden, dass die Systeme regelmäßig gewartet und aktualisiert werden.
Zeitgemäße Panels und Steuergeräte sollten daher über eine dokumentierte Update-Strategie verfügen. Idealerweise lassen sich Updates zentral verwalten, im Vorfeld testen und in geplanten Wartungsfenstern einspielen. Panels mit abgesicherten Remote-Update-Funktionen – etwa über eine verschlüsselte Cloud-Anbindung – bieten hier einen echten Mehrwert.

Fazit: Elektrotechnik und IT-Sicherheit wachsen zusammen

Die Anforderungen an Fachbetriebe im Bereich Elektro- und Gebäudetechnik verändern sich. Netzwerktechnik, IT-Sicherheit und Kommunikationsprotokolle sind heute ebenso Teil der Planung wie Stromlaufpläne oder Schaltschranklayouts.

Verschlüsselung, sichere Updates, Secure Boot, TPM (Trusted Platform Module) und Long-Term Support ermöglich sichere Systeme in der Gebäudetechnik

Wer ein modernes Gebäude zuverlässig betreiben will – sei es im Wohnbau, Gewerbe oder in der Industrie – muss IT-Sicherheit als Teil des Gesamtkonzepts verstehen und anwenden. Natürlich sind sie darauf hingewiesen, dass auch die Komponentenhersteller ihre Hausaufgaben machen. Statt der Nutzung vorgegebener Standard-Passwörter, die oft jahrelang unverändert bleiben – sollten die Gerätehersteller neben langzeitverfügbarer Hardware auch Sicherheitsmechanismen einbauen, wie die zwangsweise Vergabe eines sicheren Passwortes bei Inbetriebnahme des Geräts.
Für Planer, Integratoren und Betreiber bedeutet das: Wer bei Kommunikation und Sicherheit mitdenkt, schafft die Grundlage für einen störungsfreien und zukunftssicheren Betrieb – und schützt gleichzeitig die Investitionen seiner Kunden.

Sicherheit durch signierte Updates am Praxisbeispiel eines Touchpanels

Als Basis für ein sicheres Gebäudetechnik-Touchpanel bietet sich ein gehärtetes Yocto-Linux mit Secure Boot und TPM an. Die Software läuft auf einem schreibgeschützten Root-Dateisystem und akzeptiert nur signierte System-Images. Updates erfolgen über eine verschlüsselte, cloudbasierte Plattform – automatisch, sicher und nachvollziehbar dokumentiert. Solche Lösungen eignen sich für Anwendungen in sicherheitskritischer Infrastruktur, öffentlichen Gebäuden und in Zweckbauten wie Büro- oder Hotelkomplexen. ◄

Glossar

- **TPM (Trusted Platform Module)**
  Sicherheitschip zur sicheren Speicherung von kryptografischen Schlüsseln, Zertifikaten und Passwörtern.
- **Secure Boot**
  Startmechanismus, bei dem nur signierte Systemkomponenten geladen werden. Er verhindert Manipulationen und das Einschleusen von Schad-Software.
- **2FA (Zwei-Faktor-Authentifizierung)**
  Kombination zweier unabhängiger Authentifizierungsmerkmale – z.B. Passwort + Einmalcode.
- **VLAN (Virtual Local Area Network)**
  Virtuelle Trennung von Netzwerksegmenten zur Steigerung der Sicherheit und Strukturierung von Netzwerken.
- **TLS (Transport Layer Security)**
  Verschlüsselungsprotokoll zur Absicherung der Kommunikation in IP-Netzen