Gebäudeautomationssysteme zur Bereitstellung von Security in bestehenden KNX Projekten: Organisationale Maßnahmen und Geräteüberwachung

Teil 1: Aktueller Stand der Security in der Gebäudeautomation

Security in der Haus- und Gebäudeautomation ist eines der zentralen Schlagworte unserer Zeit. Aber warum ist Security in der Gebäudeautomation eigentlich so wichtig? Warum sollte es mich stören, wenn eine fremde Person beispielsweise meine Raumtemperatur wissen möchte?

Die Antwort ist gerade in der Automation von Zweckbauten relativ simpel. Es geht um die Vermeidung von massiven, wirtschaftlichen Bedrohungen, wie z.B.:

- Der kompletten Abschaltung des Gebäudeautomationssystems in einem Hotel
- Umgehen des Sicherheitssystems wie z.B. Abschalten des Alarmsystems
- Massenpanik in öffentlichen Bereichen durch den Ausfall des Beleuchtungssystems
- Schwerwiegende Beeinträchtigung der Arbeit in Krankenhäusern durch Ausfall des Beleuchtungssystems in der Notaufnahme
- Manipulation von Verbrauchswerten von intelligenten Energiezählern uvm.

Das Gebäudeautomationssystem kann auch als Eintrittspunkt für andere Systeme wie etwas das Hotelmanagementsystem dienen.

Dabei handelt es sich insbesondere um zwei sicherheitskritische Faktoren - Zugangskontrollen und Einbruchalarm.

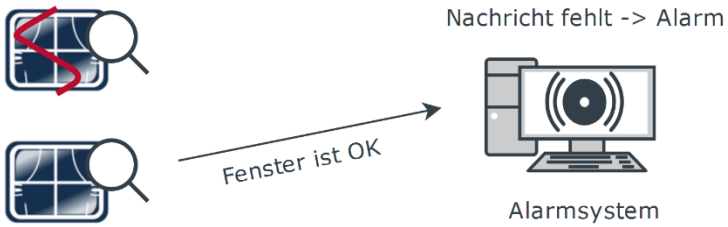
In der Vergangenheit waren alle gängigen Protokolle mehr oder weniger anfällig für Angriffe. Aufgrund der erkannten Bedrohungen, aber auch der Aktualität des Themas, verbessert sich die Lage zusehends. Insbesondere für KNX sind neue Standarderweiterungen verfügbar (KNX Data Security, KNX IP Security). Dabei kommen modernste kryptografische Technologien zum Einsatz, wie sie bereits in anderen Bereichen (TLS/SSL, e-banking, …) verwendet werden.

Für neue Projekte ist damit eine geschützte Kommunikation innerhalb des Gebäudeautomationssystems gewährleistet. Was passiert jedoch mit bereits bestehenden KNX Projekten, in denen noch keine sicheren KNX Geräte verwendet wurden? In manchen Fällen ist auch die Verwendung von Verschlüsselung nicht ausreichend. Warum, zeigen wir Ihnen im nachfolgenden Beispiel:

Denial-of-Service-Angriff im Alarmsystem

Im Falle eines Einbruchs sendet der Glasbruchsensor eine Nachricht, wenn die Fensterscheibe bricht. Der Gebäudebetreiber wird dadurch über den Einbruch informiert. Ein Jamming-Angriff kann jedoch das gesamte Alarmsystem lahmlegen und verhindern, dass das Alarmsystem die Nachricht des Glasbruchsensors empfängt. Auch eine Verschlüsselung löst dieses Problem nicht. Eine sichere Lösung für dieses Problem ist es,

den Sensor so einzustellen, dass er in regelmäßigen Abständen „OK" Nachrichten an das Alarmsystem schickt. Fehlt diese „OK" Nachricht, wird umgehend ein Alarm ausgelöst.



Was sie unternehmen können um Sicherheitslücken in Ihren bestehenden und zukünftigen Projekte zu vermeiden, erfahren Sie in den nachfolgenden Teilen.

Teil 2: Bestehende Projekte sicher gestalten

Teil 3: Sichere Gebäudeautomatisierung durch Managementlösung (NETx BMS Server)