KNX SICHERHEIT IN GEBÄUDEN

KNX System Hardening Guide

Inhalt

1. Zweck des Dokuments **2**

2. KNX Secure: Eingebauter Schutz für Smart Homes und Gebäude **2**

3. Angriffsmethoden auf KNX-Systeme **2**

4. Ansätze zur Absicherung von KNX-Installationen **3**

a) Installation des Geräts 3
b) Twisted-Pair-Kommunikation (TP) 4
c) KNX Netzwerk Segmentierung 4
d) KNXnet/IP und IT-Netzwerke 4
1. OT-Netzwerk 5
2. IT-Sicherheit zum Schutz von Gebäudesteuerungen 6
3. MAC-Adressfilterung und IGMP 8

5. Sicherer Fernzugriff **8**

6. Projektübergabe **9**

a) ETS-Reports 9
b) Kundenaufklärung über den Zugang zu Projektdaten 9
c) Passwortverwaltung 9
d) Geräte-Zertifikate 10

1. Zweck des Dokuments

Dieses Dokument soll wesentliche Einblicke, in die für die Absicherung von KNX-Gebäudeautomationssystemen erforderlichen Cybersicherheitsmaßnahmen geben. Er zeigt typische Cyberattacken auf, die die Gebäudeautomation bedrohen können und bietet praktische Strategien zum Schutz von KNX-Installationen durch sichere Geräteinstallation und Netzwerkmanagement. Darüber hinaus werden in dem Dokument wichtige Überlegungen zur Projektübergabe angesprochen, um die Sicherheit und Widerstandsfähigkeit des Gebäudebetriebs zu gewährleisten.

2. KNX Secure: Eingebauter Schutz für Smart Homes und Gebäude

Die KNX Secure Technologie erfüllt sämtliche relevanten Sicherheitsvorschriften und gewährleistet einen robusten Schutz für moderne, vernetzte Infrastrukturen. KNX Secure ist nach EN 50090-3-4 genormt und begründet damit seine Wirksamkeit bei der Abwehr von Cyberangriffen auf die digitale Infrastruktur von intelligenten Gebäuden. Dadurch wird das Risiko eines unbefugten Zugriffs oder eines digitalen Einbruchs erheblich reduziert. KNX Secure hält sich an die höchsten Verschlüsselungsstandards, einschließlich ISO 18033-3, und verwendet AES 128 CCM-Verschlüsselung zum Schutz der Daten. Damit ist sichergestellt, dass die Kommunikation innerhalb des KNX-Systems vertraulich und manipulationssicher bleibt.

Cybersicherheit ist eine gemeinsame Verantwortung. Produkte spielen zwar eine entscheidende Rolle, insbesondere bei vernetzten intelligenten Haus- und Gebäudesteuerungssystemen, jedoch sind auch andere Faktoren wie die korrekte Installation, Konfiguration und Systemsegmentierung essenziell.

ABB unterstützt Systemintegratoren und Installateure bei der Sicherung ihrer Systeme. Die letztendliche Verantwortung für die Systemsicherheit liegt jedoch bei den Installateuren, Systemintegratoren, Planern, technischen Beratern und IT-Spezialisten, die an dem Projekt beteiligt sind.

3. Angriffsmethoden auf KNX-Systeme

Angriffe über das Internet
Potenzielle Angreifer können sich über das Internet Zugang zu einer Anlage verschaffen. Diese Angriffe können weitgehend anonym durchgeführt werden, da der Angreifer nicht vor Ort sein muss. Oft haben Angreifer bereits IT-Sicherheitsbarrieren umgangen, um Zugang zu KNX-Geräten oder dem System zu erhalten.

Angriff mit teilweisem Zugriff auf das KNX-System oder Komponenten
Beispiele sind ungeschützte Buskabel außerhalb des Gebäudes oder ein heimlich installierter Raspberry Pi. Diese Szenarien geben oft Anlass zu großer Besorgnis und sind zu Demonstrationszwecken nützlich. Sie sind jedoch relativ unrealistisch, da der Angreifer physisch anwesend sein muss.

Systematische und Vor-Ort-Angriffe in KNX-Installationen
Systematische oder Vor-Ort-Angriffe beinhalten die gezielte Ausnutzung von Schwachstellen in Geräten oder Kommunikationsprotokollen. Diese Szenarien erfordern in der Regel tiefgreifende Kenntnisse des KNX-Systems und ein umfassendes Verständnis der spezifischen Installation. Als solche sind sie im Allgemeinen nur in großen oder sicherheitskritischen Umgebungen relevant und hängen oft von Insiderwissen ab.

4. Ansätze zur Absicherung von KNX-Installationen

Ein Grundprinzip jedes robusten Sicherheitskonzepts ist die strikte Isolierung des Systems vor unbefugtem Zugriff. Im Zusammenhang mit KNX-Systemen sollte der physische Zugang ausschließlich auf autorisierte Personen wie Installateure, Hausmeister oder bestimmte Benutzer beschränkt werden. Diese Isolierung kann durch eine Kombination von nativen KNX-Technologien, wie KNX Secure, und IT-Sicherheitsstrategien, einschließlich der Segmentierung von Systemen in verschiedene Sicherheitszonen, erreicht werden.

Während der Planungs- und Installationsphase müssen alle kritischen Punkte, die mit jedem KNX-Medium verbunden sind, sorgfältig abgesichert werden. Die folgenden Grundsätze sollten bei jeder KNX-basierten Gebäudeleittechnik beachtet werden:

- Nutzen Sie, wo immer möglich und sinnvoll, KNX Secure Kommunikation, um einen verschlüsselten und authentifizierten Datenaustausch zu gewährleisten.
- Implementieren Sie zusätzliche Sicherheitsmaßnahmen über KNX Secure hinaus, um den Schutz zu erhöhen. Diese Maßnahmen gelten sowohl für KNX Secure als auch für KNX Plain Installationen.
- Diese Maßnahmen sollten nicht als Ersatz für KNX Secure angesehen werden. Stattdessen sollten sie sich zu einem mehrschichtigen Sicherheitsansatz ergänzen.
- In KNX Plain oder gemischten Umgebungen sind diese zusätzlichen Sicherheitspraktiken besonders kritisch, da sie eine entscheidende Rolle bei der physischen Isolierung des Systems und der Abschwächung potenzieller Schwachstellen spielen.

a) Installation des Geräts

Produkte der Gebäudesteuerung müssen sicher installiert werden, um eine einfache Entfernung zu verhindern, die einen unbefugten Zugriff auf den KNX-Bus ermöglichen könnte. Wenn ein Diebstahl- oder Demontageschutz vorhanden ist, sollte dieser genutzt werden.

Gehäuse und Verteilerkästen, die KNX-Geräte enthalten, müssen in geeigneter Weise verschlossen oder in Räumen installiert werden, die nur für befugtes Personal zugänglich sind.

In öffentlichen Bereichen, die nicht ausreichend überwacht werden, empfiehlt es sich, konventionelle Installationsprodukte in Kombination mit Binäreingängen oder Tasterschnittstellen zu verwenden. Dies kann den Zugang zum Gebäudeleitsystem erschweren.

Die folgenden Punkte sollten bewertet werden: Wurden die folgenden Maßnahmen bei der Installation berücksichtigt?

- **Gerät montieren:** Sind die Geräte sicher montiert? Wurde ein angemessener Diebstahlschutz implementiert, um ein unbefugtes Entfernen zu verhindern? Die Geräte sollten in sicheren Schalttafeln montiert oder gegen Diebstahl geschützt werden.
- **Zugangskontrolle:** Ist der Zugang zu Verteilern, die KNX-Installationen enthalten, nur für autorisiertes Personal möglich (z.B. indem sie immer verschlossen sind oder sich in gesicherten Räumen befinden)?
- **Externe Zugänglichkeit:** Sind die im Außenbereich installierten Geräte so angebracht, dass ein unbefugter Zugriff erschwert wird (z. B. in ausreichender Höhe montiert)?
- **Betrieb im öffentlichen Bereich:** Wenn die KNX-Installation von öffentlich zugänglichen und unbeaufsichtigten Bereichen innerhalb eines Gebäudes aus bedient werden kann, wurde die Verwendung von Binäreingängen (installiert in Verteilern) oder Tasterschnittstellen in Betracht gezogen?

- **Touch Panel Sicherheit:** Sind KNX Touchpanels durch Passwörter geschützt (z.B. Benutzer-, Gruppen- oder Gastmodus)?

b) Twisted-Pair-Kommunikation (TP)

Die folgenden Punkte sollten bewertet werden:

- **Ist die Verkabelung - ob innerhalb oder außerhalb des Gebäudes - ausreichend gegen unbefugten Zugriff oder Manipulationen geschützt?**

  Die KNX-Verkabelung sollte in öffentlichen Bereichen oder von der Außenseite des Gebäudes nicht zugänglich sein. Sollten an solchen Stellen Sensoren erforderlich sein (z. B. Wettersensoren oder Drucktasten), ist es empfehlenswert, Nicht-KNX-Geräte zu verwenden und diese an KNX-Eingangsmodule anzuschließen, die sich in sicheren, nicht zugänglichen Bereichen befinden. Dadurch entfällt die Notwendigkeit, die KNX-Busleitung durch ungesicherte Bereiche zu führen, was die Systemsicherheit erhöht.

- **Wenn Twisted-Pair-Verkabelung in Bereichen verwendet wird, die einen erhöhten Schutz erfordern, wurden die erforderlichen Sicherheitsmaßnahmen ergriffen?**

  Diese Maßnahmen können die Gestaltung der Netztopologie umfassen, indem spezielle KNX-Linien oder KNX-Liniensegmente für solche Bereiche bereitgestellt werden. Darüber hinaus sollten geeignete Filtereinstellungen angewendet werden, um diese Bereiche zu schützen und zu isolieren. KNX-Repeater bieten zwar durch die galvanische Trennung einen gewissen Schutz, unterstützen jedoch keine Filterung des KNX-Busverkehrs. Für eine verbesserte Kontrolle und Sicherheit sollte die Topologie daher stattdessen mit KNX-Segmentkopplern oder Linienkopplern (z. B. ABBs LK/S4.3) aufgebaut werden.

c) KNX Netzwerk Segmentierung

Erhöhte Sicherheit kann durch die Aktivierung von Filtertabellen und die Konfiguration der entsprechenden Filtereinstellungen erreicht werden. KNX-Linienkoppler und KNX-IP-Router unterstützen das Weiterleiten, Filtern oder Sperren folgender Telegrammtypen:

- Broadcast-Telegramme (z. B. Bus-Scans)
- Individuell adressierte Telegramme (für die Konfiguration und Parametrierung von KNX-Geräten)
- Gruppenadressierte Telegramme

In der Standard-KNX-Laufzeitkommunikation werden ausschließlich gruppenadressierte Telegramme verwendet. Durch die Sperrung oder Filterung aller anderen Telegrammtypen wird die Gesamtsicherheit der KNX-Installation deutlich erhöht.

Im Allgemeinen sollte die ungefilterte Kommunikation temporären Test- und Debugging-Zwecken vorbehalten sein. In Installationen mit einem Visualisierungssystem, bei denen die meisten gruppenadressierten Telegramme an eine zentrale Schnittstelle geleitet werden, wird die Aktivierung der Filterung dringend empfohlen. Dies erhöht nicht nur die Systemleistung, sondern verbessert auch die Nachrichtenkontrolle und die Zuverlässigkeit.

d) KNXnet/IP und IT-Netzwerke

IP-basierte Gebäudesteuerungsgeräte werden häufig in dedizierten Netzen eingesetzt. In der Vergangenheit wurden diese technischen Netze nicht verwaltet und waren lediglich für die Bereitstellung grundlegender IP-Konnektivität für die Gerätekommunikation konzipiert. Sicherheitsaspekte wurden dabei kaum oder gar nicht berücksichtigt.

Die Sicherung von IP-basierten Gebäudesteuerungsgeräten (wie HLK-, Beleuchtungs-, Zugangskontroll- und Überwachungssysteme) ist in modernen intelligenten Gebäuden von entscheidender Bedeutung.

1. OT-Netzwerk

Ein OT-Netzwerk (Operational Technology) ist eine spezialisierte Infrastruktur für den Betrieb und die Steuerung von IP-Geräten außerhalb der IT. Diese Systeme umfassen Systeme der Gebäudesteuerung HLK (Heizung, Lüftung und Klimatisierung), Beleuchtung, Aufzüge, Feuermelder und Sprinkler, Zugangskontrolle und -überwachung sowie Energiemanagementsysteme. Der Aufbau eines OT-Netzwerks erfordert in der Regel die Zusammenarbeit zwischen zwei Gewerken: dem Gebäudesteuerungshandwerk und dem IT-Handwerk. Eine frühzeitige Planung und Kommunikation sind dafür unerlässlich.

Wodurch unterscheiden sich OT-Netze von IT-Netzen?

Merkmal	OT-Netzwerk	IT-Netzwerk
Zweck	Steuerung und Automatisierung von physikalischen Systemen	Datenverarbeitung und Kommunikation
Geräte	Sensoren, Steuerungen, Aktoren, PLCs	PCs, Server, Drucker
Protokolle	BACnet, Modbus, KNX, …	TCP/IP, HTTP, SMTP
Prioritäten	Verfügbarkeit, Sicherheit, Echtzeitkontrolle	Vertraulichkeit, Integrität
Häufigkeit der Aktualisierung	Unregelmäßige Aktualisierungen aufgrund von Betriebszeitanforderungen	Regelmäßige Patches und Updates

Netzwerktrennung / OT-Netz
IT-Sicherheit kann durch die Integration herkömmlicher Cybersicherheitsgrundsätze wirksam auf Gebäudeleitsysteme angewendet werden. Ein erster Schritt ist die Einführung der Netzwerksegmentierung und die Platzierung von IP-Geräten zur Gebäudesteuerung in einem speziellen OT-Netzwerk. Das OT-Netz kann ein dediziertes physisches Netz sein; in vielen Fällen, insbesondere in größeren Installationen, wird es jedoch ein VLAN (Virtual Local Area Network) sein.

VLAN (Virtuelles lokales Netzwerk)
Ein VLAN bietet mehrere wesentliche Sicherheitsvorteile in einer Netzwerkumgebung. Mit einem VLAN können Sie Geräte nach Funktion, Abteilung oder Anwendung gruppieren, nicht nur nach dem physischen Standort. Selbst wenn Geräte an denselben Switch angeschlossen sind, können sie mithilfe von VLANs voneinander isoliert werden. Normalerweise können alle an einen Switch angeschlossenen Geräte miteinander kommunizieren. Bei VLANs wird der Switch so konfiguriert, dass er Ports verschiedenen Virtual Local Area Networks (VLANs) zuweist. Geräte in VLAN 10 können nicht mit Geräten in VLAN 20 kommunizieren, es sei denn, ein Router oder Layer-3-Switch verbindet sie miteinander.

Wichtigste Vorteile:

- Isolierung von Nicht-IT-Infrastrukturen: Gebäudesysteme (wie HLK, Aufzüge, Beleuchtung und Zugangskontrolle) verfügen häufig nicht über die Sicherheitsmerkmale von IT-Geräten und können anfälliger für Cyberangriffe sein.
- Geringeres Risiko einer seitlichen Bewegung: Cyber-Angreifer bewegen sich oft seitlich innerhalb eines Netzwerks, nachdem sie einen ersten Zugang erhalten haben. Die Netzwerktrennung verhindert eine seitliche Bewegung von Bürosystemen (z. B. E-Mail, Dateiserver) zu operativen Systemen, die die physische Infrastruktur kontrollieren.

- Schutz von Notsystemen: Systeme wie Feuermelder, Notbeleuchtung und Zugangskontrollen sind unternehmenskritisch. Durch ihre Isolierung wird sichergestellt, dass ein Eindringen in das OT- oder IT-Netz keine Systeme beeinträchtigt, die die Sicherheit von Menschen schützen.
- Maßgeschneiderte Sicherheitsrichtlinien: Gebäudeleitsysteme verwenden oft spezielle Protokolle (z. B. BACnet, Modbus), die in IT-Umgebungen nicht verwendet werden. Ein separates Netzwerk ermöglicht maßgeschneiderte Firewalls und Zugangskontrollen, die auf diese Protokolle zugeschnitten sind.
- Verbesserte Überwachung und Reaktion auf Zwischenfälle: Mit einem dedizierten Netzwerk ist es einfacher, den Datenverkehr zu überwachen, Anomalien zu erkennen und auf Vorfälle zu reagieren, ohne dass es zu Störungen des IT-Datenverkehr kommt.
- Sichere Wartung und Prüfung: Aktualisierungen oder Änderungen an Gebäudesystemen können isoliert getestet werden, wodurch das Risiko einer Unterbrechung des Geschäftsbetriebs oder der Offenlegung sensibler Daten verringert wird.
- Einhaltung von Vorschriften: Viele Normen (z. B. IEC 62443, NIST, ISO/IEC 27001) empfehlen oder fordern eine Netzsegmentierung für kritische Infrastrukturen. Mit einem separaten Netz lassen sich diese Anforderungen leichter erfüllen.

2. IT-Sicherheit zum Schutz von Gebäudesteuerungen

Sobald sich die Geräte zur Gebäudesteuerung in einem getrennten IT-Netz befinden, können gezielte IT-Sicherheitsmaßnahmen den Schutz der Gebäudesteuerung verbessern:

Firewalls und Zugangskontrolllisten

- Zweck: Steuern Sie, welche Geräte oder Benutzer mit den Gebäudesystemen kommunizieren können.
- Nutzen: Verhindert unbefugten Zugang und seitliche Bewegungen.
- Beispiel: Erlauben Sie nur bestimmten Verwaltungsstationen den Zugriff auf das Gebäudemanagementsystem.

Netzwerkzugangskontrolle

- Zweck: Wenn technisch möglich authentifizieren und autorisieren Sie Geräte, bevor sie sich mit dem Netzwerk verbinden.
- Nutzen: Blockiert nicht autorisierte Geräte.
- Beispiel: MAC-Adressfilterung oder 802.1X-Authentifizierung verwenden

Überwachung und Protokollierung

- Zweck: Verfolgen Sie Netzwerkaktivitäten und erkennen Sie Anomalien.
- Nutzen: Frühzeitige Erkennung von Einbrüchen oder Fehlkonfigurationen.

Schwachstellen-Management

- Durchführung regelmäßiger Schwachstellen-Scans der Gebäudekontrollnetze und -geräte zur Ermittlung potenzieller Sicherheitsrisiken.
- Priorisierung und Beseitigung der ermittelten Risiken nach ihrem Schweregrad.

Sichere Protokolle und Verschlüsselung

- Ersetzen Sie unverschlüsselte IP-Protokolle durch sichere Alternativen (z. B. KNX IP Secure anstelle von KNXnet/IP und BACnet/SC anstelle von BACnet/IP).

Sicherheitsbewusstsein und Schulung

- Schulung von Gebäudemanagern und Gebäudetechnikern in Sachen **Cyberhygiene** und **Reaktion auf Vorfälle**.

- Fördern Sie die Zusammenarbeit zwischen IT- und OT-Teams.
- Viele IP-basierte Gebäudesteuerungsprotokolle unterstützen von Haus aus keine Netzwerkauthentifizierung, Datenverschlüsselung oder Zugangskontrolle. In diesem Fall besteht die beste Methode zur Sicherung des Systems darin, den Zugang zum IP-Netz so weit wie möglich zu kontrollieren und einzuschränken, und zwar mit Hilfe der üblichen IT-Methoden.

MAC-Adressen-Filterung

- Die MAC-Adressfilterung ist eine Netzwerksicherheitsfunktion, die in Geräten wie Routern, Switches und Access Points verwendet wird, um zu kontrollieren, welche Geräte eine Verbindung zum Netzwerk herstellen dürfen. Jedes netzwerkfähige Gerät (z. B. Computer, Smartphone oder Drucker) verfügt über eine eindeutige Kennung, die als MAC-Adresse (Media Access Control-Adresse) bezeichnet wird und in der Regel als 12-stellige Hexadezimalzahl formatiert ist (z. B. 00:1A:2B:3C:4D:5E).
- Netzwerkadministratoren können die MAC-Adressfilterung auf zwei Arten konfigurieren:
    - **Whitelist (Liste zulassen):** Nur Geräte, deren MAC-Adressen in dieser Liste aufgeführt sind, können eine Verbindung herstellen.
    - **Schwarze Liste (Ablehnungsliste):** Geräte mit MAC-Adressen auf dieser Liste werden ausdrücklich für die Verbindung gesperrt.
- Vorteile:
    - Bietet eine zusätzliche Ebene der Zugangskontrolle.
    - Besonders effektiv in kleinen oder statischen Netzen, in denen die Geräte bekannt sind und sich selten ändern.
- Beschränkungen:
    - **Nicht narrensicher:** MAC-Adressen können von Angreifern gefälscht werden.
    - **Manuelle Instandhaltung:** Das Hinzufügen oder Entfernen von Geräten erfordert manuelle Aktualisierungen.
    - **Begrenzte Skalierbarkeit:** Wird in großen oder sich häufig ändernden Umgebungen unpraktisch.
- Im Zusammenhang mit Gebäudeautomationssystemen wie KNXnet/IP, das wie viele IP-Standards für die Gebäudesteuerung keine native Authentifizierung auf IT-Ebene unterstützt, muss die Cybersicherheit durch mehrschichtige Schutzmaßnahmen verstärkt werden. Die MAC-Adressfilterung allein kann zwar keine Sicherheit garantieren, trägt aber zu einer "Defense-in-Depth"-Strategie bei, indem sie den Aufwand für einen unbefugten Zugriff erhöht.

Was ist IGMP?

IGMP (Internet Group Management Protocol) ist ein Netzwerkprotokoll, das zur Verwaltung von Multicast-Gruppen in einem IP-Netzwerk verwendet wird. Sie ermöglicht es Hosts, Multicast-Gruppen beizutreten und zu verlassen, um Daten effizient an mehrere Empfänger gleichzeitig zu übermitteln. IGMP ist Teil der IP-Protokollsuite und arbeitet auf der Netzwerkschicht. Sie ermöglicht es Geräten (wie Computern, IP-Kameras oder Smart-TVs), einem Router mitzuteilen, dass sie bestimmten Multicast-Verkehr empfangen möchten, z. B. einen Live-Video-Stream oder ein KNXnet/IP-Signal.

Multicast ist eine Methode, bei der ein Datenstrom an mehrere Empfänger gleichzeitig gesendet wird, ohne dass an jedes Gerät eine eigene Kopie gesendet wird. Es ist effizienter als Unicast (one-to-one) oder Broadcast (one-to-all). KNXnet/IP Routing verwendet Multicast-Kommunikation auf der IANA-registrierten Multicast-IPv4-Adresse 224.0.23.12 (Standard).

3. MAC-Adressfilterung und IGMP

Sowohl IGMP Snooping als auch MAC Address Filtering können zur Filterung und Kontrolle der Multicast-IP-Kommunikation verwendet werden. Der primäre Anwendungsbereich der beiden Technologien ist unterschiedlich. Während das Hauptziel des IGMP-Protokolls darin besteht, eine effektive Multicast-Kommunikation zu gewährleisten, liegt der Schwerpunkt der MAC-Adressfilterung auf der Netzzugangskontrolle. Beide Technologien erfordern eine enge Zusammenarbeit mit den IT-Abteilungen, die das VLAN verwalten. Die Umsetzung hängt stark von der Netzgestaltung und der Art der verwendeten Netzausrüstung ab.

Merkmal	MAC-Adressen-Filterung	IGMP
Primärer Zweck	Zugangskontrolle	Verwaltung von Multicast-Gruppen
Nutzer Rollen	Ja	Nein (außer in Kombination mit IGMP Snooping)
Benutzerfreundlichkeit	Einfach	Komplexer
Anwendungsfall	Kleine Netzwerke, Wi-Fi	IPTV, Streaming, Multicast
Verkehrskontrolle	Nein	Ja (für Multicast)

5. Sicherer Fernzugriff

Der sichere Fernzugriff ermöglicht die Fernüberwachung, -verwaltung und -wartung von Gebäudemanagementsystemen und trägt somit zur Senkung der Wartungskosten bei. Um eine sichere Konnektivität zu gewährleisten, sollten die folgenden bewährten Verfahren implementiert werden:

- Verwendung von verschlüsselten Kommunikationskanälen: Verwenden Sie sichere Protokolle wie KNX Secure (KNX IP Secure) und VPN-Tunnel, um Daten während der Übertragung zu schützen.
- Authentifizierung und Zugangskontrolle: Implementieren Sie starke Authentifizierungsmechanismen und rollenbasierten Zugang, um den Systemzugang auf autorisiertes Personal zu beschränken.
- Firewall und Netzwerksegmentierung: Isolieren Sie das KNX-Netzwerk von externen Netzwerken mit Firewalls und segmentieren Sie es, um die Ausbreitung potenzieller Bedrohungen zu begrenzen.
- Regelmäßige Updates und Patches: Halten Sie alle Geräte, Router und Software mit den neuesten Sicherheits-Patches auf dem neuesten Stand, um optimale Sicherheit zu gewährleisten.
- Überwachung und Protokollierung: Kontinuierliche Überwachung von Fernzugriffssitzungen und Führung von Protokollen für Audits und die Reaktion auf Zwischenfälle.

Für die Nutzung mit Remote-Zugriff sollten KNX IP Secure Geräte eingesetzt werden, wie beispielsweise der KNX IP Router (IPR/S3.5.1) und die IP-Schnittstelle (IPS/S3.5.1). In Kombination mit einem VPN-Gateway wird so ein sicheres und effizientes Systemmanagement von überall aus ermöglicht.

6. Projektübergabe

Der EU Cyber Resilience Act (CRA) führt verbindliche Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen ein, einschließlich KNX-Produkte. Ein zentrales Prinzip des CRA ist, dass Kunden davon ausgehen können müssen, dass ein Produkt standardmäßig sicher ist. Jegliche Einschränkungen dieser Sicherheit sind dem Kunden mitzuteilen.

Bei der Übergabe eines KNX-Projekts ist es wichtig, dass:

- Übertragen Sie alle sicherheitsrelevanten Daten, zusammen mit den allgemeinen Projektdaten.
- Erklären Sie dem Kunden die Sicherheitsmerkmale des Systems, einschließlich aller bekannten oder unvermeidbaren Risiken.
- Dokumentieren Sie diese Informationen und nehmen Sie sie in das technische Übergabepaket auf, um künftige Haftungen zu vermeiden.

a) ETS-Reports

Die ETS erstellt zwei Reports, die wichtige Sicherheitsinformationen enthalten:

- Projekt-Sicherheitsreport
- Projektzertifikatsreport

Diese Berichte sind zu erstellen, mit dem Kunden abzustimmen und in die Projektübergabeunterlagen aufzunehmen.

b) Kundenaufklärung über den Zugang zu Projektdaten

Die Kunden - insbesondere diejenigen ohne ETS-Zugang - müssen über folgendes informiert werden:

- Die zentrale Rolle des ETS-Projekts bei der Wartung von KNX Secure Systemen.
- Die Notwendigkeit einer Zusammenarbeit mit dem Systemintegrator, um die Sicherheit des Projekts aufrechtzuerhalten und zu gewährleisten, dass es auf dem neuesten Stand bleibt.

c) Passwortverwaltung

Das ETS-Projekt ist durch ein Passwort geschützt, das für die Planung und Wartung erforderlich ist. Wenn der Kunde eine ETS-Lizenz hat, kann er ein neues lokales Kennwort vergeben, aber:

- Diese Änderung betrifft nur ihre lokale Kopie.
- ToolKeys, MAC Keys und Group-Keys sind davon nicht betroffen.
- Wenn der Systemintegrator eine Kopie des Projekts behält, kann er weiterhin auf das System zugreifen und es ändern.

Es wird empfohlen:

- Einigen Sie sich auf eine klare Richtlinie für die Verwaltung von ETS-Projektkopien und Passwörtern.
- Führen Sie eine Liste der Personen, die Zugang zum ETS-Projekt haben.

d) Geräte-Zertifikate

Für die Wiederverwendung von KNX Secure Geräten nach einem Master-Reset oder in einem neuen Projekt wird das Gerätezertifikat benötigt. Die Art der Distribution und des Abrufs von Zertifikaten variiert je nach Hersteller und Produkt. Es ist von entscheidender Bedeutung, ein Verfahren zur Erfassung, Verwaltung und Übertragung dieser Zertifikate zwischen dem Systemintegrator und dem Kunden einzurichten.