



Smart home and building solutions.  
Global. Secure. Connected.

# KNX SECURE CHECKLISTE



# CHECKLISTE FÜR MEHR SICHERHEIT UND DATENSCHUTZ IN KNX ANLAGEN

## 1. Wurden die folgenden Maßnahmen bei der Installation berücksichtigt?

Sind die Geräte und Anwendungen fest montiert? Ist sichergestellt, dass die Geräte ordnungsgemäß gegen Demontage gesichert sind (z. B. Einsatz von Diebstahlsicherungsmaßnahmen)?

Ist sichergestellt, dass Unbefugte nur begrenzten Zugang zu Verteilern mit montierten KNX Anlagen haben (z. B. immer verschlossen oder in abgeschlossenen Räumen)?

Ist der Zugang zu Geräten im Außenbereich erschwert (z. B. Montage in ausreichender Höhe)?

Falls die KNX Anlage von öffentlich zugänglichen und nicht überwachten Bereichen in Gebäuden bedient werden kann: Haben Sie die Verwendung von Binäreingängen (in Verteilern montiert) oder Tasterschnittstellen in Erwägung gezogen?

Sind die KNX Touchpanels passwortgeschützt (Benutzer-, Gruppen- oder Gastmodus)?

## 2. Wird Twisted Pair als Kommunikationsmedium verwendet?

Ist das Kabel überall innerhalb oder außerhalb der Wohnung oder des Gebäudes vor unbefugtem Zugriff geschützt?

Falls das Twisted-Pair-Kabel in Bereichen verwendet wird, die besondere Schutzmaßnahmen erfordern: Haben Sie die unter Punkt 6 genannten Maßnahmen ergriffen?

## 3. Wird Powerline als Kommunikationsmedium verwendet?

Wurden Bandsperrefilter installiert?

Wenn Powerline auch außerhalb des Gebäudes verwendet wird: Haben Sie die gleichen Maßnahmen für den Medienkoppler getroffen, wie in Punkt 6 beschrieben?

## 4. Wird IP als Kommunikationsmedium verwendet?

- 
- Wurden die Netzwerkeinstellungen dokumentiert und dem Hauseigentümer oder dem LAN-Administrator übergeben?
- 
- Wurden Switches und Router so eingestellt, dass nur bekannte MAC-Adressen auf das Kommunikationsmedium zugreifen können?
- 
- Wird für die KNX Kommunikation ein separates LAN- oder WLAN-Netzwerk mit eigener Hardware verwendet?
- 
- Ist der Zugang zu den (KNX-) IP-Netzwerken auf autorisierte Personen über entsprechende Benutzernamen und sichere Passwörter beschränkt?
- 
- Für die KNX-IP-Multicast-Kommunikation sollte eine andere IP-Adresse als die Standardadresse verwendet werden (normalerweise 224.0.23.12). Wurde diese IP-Multicast-Adresse geändert?
- 
- Wurde die Standard-SSID des drahtlosen Zugangspunktes geändert? Wurde die periodische Übertragung der SSID nach der Installation deaktiviert?
- 
- Wurden die Ports der Router für KNX zum Internet hin geschlossen und das Standard-Gateway des verwendeten KNXnet/IP-Routers auf 0 gesetzt? Wurde die (W)LAN-Installation durch eine geeignete Firewall geschützt?
- Wenn ein Internetzugang zu einer KNX Anlage benötigt wird, prüfen Sie die Möglichkeit der Implementierung von:
1. Aufbau einer VPN-Verbindung zum Internet-Router
  2. Verwendung von herstellerspezifischen KNX-Objekt-Servern
- 

## 5. Wird Funkfrequenz als Kommunikationsmedium verwendet?

- 
- Haben Sie für den Medienkoppler die gleichen Maßnahmen ergriffen wie unter Punkt 6 angegeben?
- 
- Hat jede RF-Domäne eine andere Domänenadresse?
- 

## 6. Haben Sie Koppler in der Anlage verwendet?

- 
- Wurden die physikalischen Adressen der Geräte entsprechend ihrer Position in der Topologie zugewiesen?
- 
- Verhindern Sie durch die Einstellung entsprechender Parameter in den Kopplern, dass falsche Quelladressen nicht außerhalb der Linie weitergeleitet werden?
- 
- Sperrern Sie Punkt-zu-Punkt- und Broadcast-Kommunikation über Koppler?
- 
- Wurden die Filtertabellen korrekt geladen und die Einstellungen so vorgenommen, dass die Filtertabellen von den Kopplern berücksichtigt werden?
- 
- Haben Sie die unter Punkt 7 genannten Maßnahmen für die Koppler berücksichtigt?
- 

## 7. Wurden die Geräte gegen Umkonfiguration gesperrt?

- 
- Wenn nicht, geben Sie einen BCU-key1 in das ETS-Projekt ein.
-

## 8. Verwenden Sie KNX Secure<sup>2</sup>-Geräte?

Verwenden Sie für die Gruppenkommunikation, die gesichert werden muss, die vorgesehenen Authentifizierungs- und Verschlüsselungsmechanismen des Geräts.

## 9. Vermuten Sie unbefugten Zugriff auf den Bus?

Zeichnen Sie den Telegrammverkehr auf und analysieren Sie ihn. Bei KNX-Secure-Geräten lesen Sie die Fehlerprotokolle.

Dokumentieren Sie den Zeitpunkt und die beobachteten Auswirkungen (was passiert, was passiert nicht, warum und wann?).

Deaktivieren Sie die Internetverbindung des KNX Systems und prüfen Sie, ob die Auswirkungen verschwinden oder nicht.

Wenden Sie sich an die Hotline des Herstellers: Sind die Auswirkungen oder Sicherheitsprobleme beim Hersteller bekannt, sind Updates verfügbar?

Lesen Sie die PID\_Device\_Control<sup>3</sup> von Geräten aus und prüfen Sie, ob Geräte mit der gleichen physikalischen Adresse senden.

Lesen Sie den PID\_Download\_Counter<sup>3</sup> von Geräten aus und prüfen Sie, ob das Gerät nach Ihrer Konfiguration erneut heruntergeladen wurde.

## 10. Wurden die Geräte gegen Umkonfiguration gesperrt?

Wenn KNX mit Sicherheitsanlagen gekoppelt ist, wurde dies auf eine der folgenden Arten realisiert?

- über KNX Geräte oder Gateways, die von nationalen Schadenversicherern zertifiziert sind?
- über potentialfreie Kontakte (Binäreingänge, Tasterschnittstellen usw.)?
- über entsprechende Schnittstellen (RS232 usw.) oder Gateways: Wurde sichergestellt, dass die KNX Kommunikation keine sicherheitsrelevanten Funktionen im Sicherheitsbereich der Anlage auslösen kann?

## 11. Allgemeine Sicherheitsmaßnahmen

Ist die ETS auf dem neuesten Stand?

- Ist der PC, auf dem die ETS installiert ist, sicher (aktueller Virenschutz, neuestes Betriebssystem)?

Es wird empfohlen, ein dediziertes Gerät für KNX Design und Inbetriebnahme zu verwenden.

- Während der Installation ist es zu vermeiden, andere nicht vertrauenswürdige Datenspeicher an den PC anzuschließen (USB, externe Festplatte, usw.).

- Die ETS-Plug-ins und Apps sollten vorzugsweise vor der Installation installiert werden.

- Sichern Sie die Projektdatei nach der Installation (idealerweise auf einem gesicherten USB-Stick, der sicher aufbewahrt wird) und löschen Sie das Projekt vom PC.

Ist die Firmware der verwendeten Geräte auf dem neuesten Stand?

## 12. Weitere Datenschutzmaßnahmen (DSGVO)

Installateur und Kunde müssen eine Datenschutzerklärung unterzeichnen.

Um die DSGVO-Vorschriften zu erfüllen, muss der Installateur eine Kopie der ETS-Projektdatei an den Kunden aushändigen.

<sup>2</sup> Verfügbar ab ETS 5.5, <sup>3</sup> Wird nicht von allen Geräten unterstützt