KNX Sicherheit Checkliste

Checkliste für die erhöhte Sicherheit in KNX Anlagen und Datenschutz

1 Wurden folgende Vorkehrungen bei der Montage berücksichtigt?

- [ ] Wurden Anwendungen und Geräte fest installiert? Ist sichergestellt, dass Geräte gegen einfache Demontage geschützt sind (Verwendung Diebstahlschutzeinrichtungen)?
- [ ] Wurde sichergestellt, dass Unterverteilungen mit KNX Geräten für unbefugte Personen schwer zugänglich sind (z. B. immer verschlossen oder in verschlossenen Räumlichkeiten)?
- [ ] Wurden Geräte im Außenbereich ausreichend schwer zugänglich (z. B. in ausreichender Höhe) installiert?
- [ ] Falls die KNX Anlage aus nicht-überwachten öffentlichen Bereichen von Gebäuden bedient werden kann, wurde die Verwendung von sicher verorteten (z. B. in der Unterverteilung) Binäreingängen oder Tasterschnittstellen in Erwägung gezogen?
- [ ] Sind KNX Touchpanels Passwort-gesichert (Benutzer, Gruppen- und Gastzugang)?

2 Wird Twisted Pair-Buskabel als Kommunikationsmedium verwendet?

- [ ] Ist die Busleitung innerhalb wie außerhalb des Hauses oder Gebäudes gegen unbefugten Zugang geschützt?
- [ ] Falls eine Busleitung im Außenbereich oder in besonders zu schützenden Bereichen genutzt wird, sind für die Koppler die unter Punkt 6 genannten Vorkehrungen angewandt worden?

3 Wird Powerline als Kommunikationsmedium verwendet?

- [ ] Wurden entsprechende Bandsperrfilter installiert?
- [ ] Falls im Außenbereich Powerline eingesetzt wird, sind für den Medienkoppler die unter Punkt 6 genannten Vorkehrungen angewandt worden?

4 Wird IP als Kommunikationsmedium verwendet?

- [ ] Wurden die Netzwerkeinstellungen dokumentiert und dem Hausbesitzer oder LAN Administrator übergeben?
- [ ] Sind Switches und Router so eingestellt, dass nur bekannte MAC Adressen Zugang zum Kommunikationsmedium haben?
- [ ] Wurde für die KNX Kommunikation ein separates IP-Netzwerk mit eigener Hardware aufgesetzt?
- [ ] Ist der Zugang zum (KNX-)IP-Netzwerk durch Nutzerkennungen und starke Passwörter auf einen berechtigten Personenkreis eingeschränkt?
- [ ] Für die Verwendung von KNX IP Multicast sollte eine andere als die voreingestellte IP-Adresse (voreingestellt: 224.0.23.12) verwendet werden. Wurde die IP Multicast Adresse abgeändert?
- [ ] Wurde die voreingestellte SSID vom drahtlosen Access Point geändert? Wurde die periodische Übermittlung der SSID nach der Installation unterbunden?
- [ ] Sind Ports von Routern Richtung Internet für KNX geschlossen und ist das Default-Gateway des verwendeten KNXnet/IP Routers auf 0 gesetzt? Wurde die (W)LAN Anlage durch eine entsprechende Firewall geschützt? Wenn ein Internet Zugang zu der Installation notwendig ist, überprüfen Sie die Möglichkeit folgendes zu implementieren:
  1. Aufbau einer VPN Verbindung mit dem Internet Router
  2. Einsatz herstellerspezifischer KNX Object Server

5 Wird Funk als Kommunikationsmedium verwendet?

- [ ] Sind für den Medienkoppler die unter Punkt 6 genannten Vorkehrungen angewandt worden?
- [ ] Wurde für jeden Funkbereich eine getrennte Domainadresse eingestellt?

6 Haben Sie Koppler in der Anlage im Einsatz?

- [ ] Wurden die physikalischen Adressen der Geräte entsprechend der Topologie eingestellt?
- [ ] Sind die entsprechenden Parameter bei den Kopplern so eingestellt, dass inkorrekte Quelladressen aus der Linie heraus nicht weitergeleitet werden?
- [ ] Ist Punkt-zu-Punkt und Broadcast Kommunikation über Koppler hinweg gesperrt?
- [ ] Sind die Filtertabellen korrekt geladen und sind die Einstellungen so, dass die Filtertabellen ausgewertet werden?
- [ ] Sind für die Koppler die Vorkehrungen aus Punkt 7 angewandt worden?

7 Sind die Geräte gegen Re-Konfiguration geschützt?

- [ ] Wenn nicht, geben Sie im ETS-Projekt einen BAU Schlüssel[1] ein.

8 Setzen Sie KNX Secure[2] Geräte ein?

- [ ] Verwenden Sie die vom Gerät vorgesehenen Authentifikations- und Verschlüsselungsmechanismen für die zu schützende Gruppenkommunikation?

9 Vermuten Sie, dass auf den Bus unautorisiert zugegriffen wird?

- [ ] Nehmen Sie den Telegrammverkehr auf und analysieren Sie ihn. Bei KNX Secure Geräten, lesen Sie die Failure Logs aus. Dokumentieren Sie Zeitpunkt und beobachtete Effekte (was passiert/passiert nicht, wo und wann)? Trennen Sie das KNX System (sofern betrieblich möglich) vom Internet und prüfen Sie, ob die Effekte weiterhin auftreten. Kontaktieren Sie die Herstellerhotline: Sind beim Hersteller vergleichbare Effekte/Sicherheitsprobleme bekannt, Updates verfügbar?
- [ ] Lesen Sie von Geräten den PID_Device_Control[3] aus und verifizieren Sie, ob andere Geräte mit der gleichen physikalischen Adresse senden.
- [ ] Lesen Sie von Geräten den PID_Download_Counter[3] aus und verifizieren Sie, ob das Gerät seit Ihrer Konfiguration neu geladen wurde.

1) nicht alle Geräte lassen sich dadurch gegen Re-Konfiguration schützen – setzten Sie sich mit dem jeweiligen Hersteller in Verbindung

2) Verfügbar ab ETS 5.5

3) Wird nicht in allen Geräten unterstützt

10 Kopplung KNX mit Sicherheitsanlagen

Wenn KNX mit Sicherheitsanlagen gekoppelt ist, wurde dies auf folgende Weise realisiert? ☐

1. Über VdS approbierte KNX Geräte oder Schnittstellen?
2. Über potentialfreie Kontakte (Binäreingänge, Tasterschnittstellen, ...)?
3. Über entsprechende Schnittstellen oder Gateways? Wurde dann sichergestellt, dass die KNX Kommunikation keine sicherheitsrelevanten Funktionen im Fremdsystem auslöst?

11 Allgemeine Sicherheitsmaßnahmen

Ist die ETS auf dem aktuellen Stand? ☐

1. Ist der Rechner, auf dem ETS installiert ist, sicher (aktueller Viren-Check, neuestes Betriebssystem-Update)? Es empfiehlt sich, ein dediziertes Gerät für KNX Planung und Inbetriebnahme einzusetzen.
2. Während der Installation soll vermieden werden, den Rechner mit anderen unbekannten Datenträgern (USB/Festplatte/…) zu koppeln.
3. ETS Plug-ins und Apps werden vorzugsweise vor der Installation geladen.
4. Sichern Sie nach der Installation die Projektdatei (idealerweise auf einen verschlüsselten USB Stick, der sicher aufbewahrt wird) und löschen Sie diese dann auf dem Notebook.

Ist die Firmware der Geräte aktuell? ☐

12 Weitere Maßnahmen zum Datenschutz (GDPR)

Installateur und Kunde sollten gemeinsam eine Datenschutzerklärung unterschreiben. ☐

Zur Erfüllung der GDPR-Richtlinie ist vom Installateur die ETS-Projektdatei dem Kunden zu übergeben. ☐