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

CHECKLIST KNX SECURE

CHECKLIST VOOR MEER VEILIGHEID EN PRIVACY BIJ KNX-INSTALLATIES

1. Werd er tijdens de installatie rekening gehouden met de volgende maatregelen?

Zijn de apparaten en applicaties vast gemonteerd? Wordt erop toegezien dat de apparaten naar behoren beschermd zijn tegen demontage? (Zijn er bijvoorbeeld maatregelen voor diefstalbeveiliging getroffen?)	☐
Wordt erop toegezien dat onbevoegden slechts beperkte toegang hebben tot verdeelborden waarop KNX-installaties gemonteerd zijn (bv. altijd vergrendeld of in een vergrendelde ruimte)?	☐
Is het moeilijk om toegang te krijgen tot apparaten in buitenruimten? (Zijn ze bijvoorbeeld hoog genoeg gemonteerd?)	☐
Als de KNX-installatie kan worden bediend vanaf een zone in het gebouw die openbaar en niet bewaakt is, hebt u dan het gebruik overwogen van (in verdeelborden gemonteerde) binaire ingangen of drukknopinterfaces?	☐
Zijn KNX-aanraakschermen met een wachtwoord beveiligd (gebruikers-, groeps- of gastmodus)?	☐

2. Wordt Twisted Pair gebruikt als communicatiemedium?

Is de kabel ergens binnen of buiten het huis of het gebouw beschermd tegen ongeoorloofde toegang?	☐
Indien de Twisted Pair-kabel wordt gebruikt in zones die extra beschermingsmaatregelen vereisen, hebt u dan de maatregelen getroffen die opgegeven worden in punt 6?	☐

3. Wordt Powerline gebruikt als communicatiemedium?

Zijn er bandsperfilters geïnstalleerd?	☐
Als ook buiten het gebouw Powerline wordt gebruikt, hebt u dan dezelfde maatregelen getroffen voor de mediakoppelaar die opgegeven worden in punt 6?	☐

4. Wordt IP gebruikt als communicatiemedium?

- [ ] Zijn de netwerkinstellingen gedocumenteerd en aan de huiseigenaar of netwerkbeheerder overhandigd?
- [ ] Zijn de schakelaars en routers ingesteld zodat alleen bekende MAC-adressen toegang kunnen krijgen tot het communicatiemedium?
- [ ] Wordt voor KNX-communicatie een apart LAN- of WLAN-netwerk met eigen hardware gebruikt?
- [ ] Is de toegang tot de (KNX) IP netwerken beperkt tot bevoegde personen met de juiste gebruikersnaam en een sterk wachtwoord?
- [ ] Voor KNX IP Multicast-communicatie moet een ander IP-adres worden gebruikt dan het standaardadres (normaal gezien 224.0.23.12). Werd dit IP multicast-adres gewijzigd?
- [ ] Is de standaard SSID van het draadloze toegangspunt gewijzigd? Werd de periodieke transmissie van de SSID na de installatie gedeactiveerd?
- [ ] Zijn de poorten van routers voor KNX gesloten voor het internet en werd de standaard gateway van de gebruikte KNXnet/IP-router ingesteld op 0? Werd de (W)LAN-installatie beveiligd door een passende firewall?
  Indien er internettoegang tot een KNX-installatie nodig is, controleer dan of het mogelijk is om:
  1. een VPN-verbinding met de internetrouter tot stand te brengen;
  2. KNX Object Servers te gebruiken die specifiek zijn voor de fabrikant.

5. Wordt Radio Frequency gebruikt als communicatiemedium?

- [ ] Hebt u voor de mediakoppelaar dezelfde maatregelen getroffen die opgegeven worden in punt 6?
- [ ] Heeft elk RF-domein een ander domeinadres?

6. Hebt u koppelaars gebruikt in de installatie?

- [ ] Werden de individuele adressen van apparaten toegewezen in overeenstemming met hun plaats in de topologie?
- [ ] Voorkomt u, door in de koppelaars de juiste parameters in te stellen, dat verkeerde bronadressen buiten de lijn worden doorgestuurd?
- [ ] Blokkeert u Point-to-Point en Broadcast communicatie over koppelaars?
- [ ] Zijn de filtertabellen correct ingeladen en maken de instellingen het voor de koppelaars mogelijk om rekening te houden met de filtertabellen?
- [ ] Hebt u rekening gehouden met de maatregelen die opgegeven worden in punt 7?

7. Zijn er apparaten vergrendeld nadat ze opnieuw werden geconfigureerd?

- [ ] Zo niet, voer dan een BCU-sleutel1 in het ETS-project in.

8. Gebruikt u KNX Secure[2]-apparaten?

Gebruik voor groepscommunicatie die beveiligd moet worden de voorziene mechanismen voor authenticatie en versleuteling van het apparaat. ☐

9. Vermoedt u dat er ongeoorloofd toegang werd verkregen tot de bus?

Neem het telegramverkeer op en analyseer het. Lees bij KNX Secure-apparaten de storingslogboeken. Documenteer het tijdstip en de waargenomen verschijnselen (wat er al dan niet gebeurt, waarom en wanneer).
Schakel de internetverbinding van het KNX-systeem uit en controleer of de verschijnselen al dan niet verdwijnen. ☐
Neem via de hotline contact op met de fabrikant: heeft de fabrikant weet van de verschijnselen of veiligheidsproblemen en zijn er updates beschikbaar?

Lees de PID_Device_Control3 van de apparaten af en controleer of de apparaten met behulp van hetzelfde individuele adres verzenden. ☐

Lees de PID_Download_Counter3 van de apparaten af en controleer of het apparaat opnieuw werd gedownload nadat u het had geconfigureerd. ☐

10. Zijn er apparaten vergrendeld nadat ze opnieuw werden geconfigureerd?

Werd een eventuele koppeling van KNX met beveiligingsinstallaties op een van de volgende manieren tot stand gebracht?

1. Via KNX-apparaten of gateways die gecertificeerd zijn door nationale schadeverzekeraars?
2. Via potentiaalvrije contacten (binaire ingangen, drukknopinterfaces ...)? ☐
3. Via passende interfaces (RS232 ...) of gateways: werd erop toegezien dat de KNX-communicatie geen functies kan triggeren die relevant zijn voor de veiligheid in het onderdeel van de installatie dat daarvoor instaat?

11. Algemene veiligheidsmaatregelen

Is ETS bijgewerkt?

1. Is de pc waarop ETS geïnstalleerd is beveiligd (bijgewerkte virusscanner, recentste update besturingssysteem)? Het is raadzaam een apparaat te gebruiken dat specifiek bedoeld is voor KNX-ontwerp en inbedrijfstelling.
2. Tijdens de installatie mogen geen andere, niet-vertrouwde apparaten voor dataopslag op de pc worden aangesloten (USB, externe harde schijf ...). ☐
3. Bij voorkeur moeten ETS-plug-ins en -apps vóór de installatie worden geïnstalleerd.
4. Maak na de installatie een back-up van het projectbestand (bij voorkeur op een beveiligde USB-stick die veilig wordt opgeborgen) en verwijder het project van de pc.

Is de firmware van de gebruikte apparaten bijgewerkt? ☐

12. Verdere privacymaatregelen (AVG)

De elektricien en de klant moeten een privacyverklaring ondertekenen. ☐

Om te voldoen aan de voorschriften van de AVG moet de elektricien een kopie van het ETS-projectbestand overhandigen aan de klant. ☐

[2] Beschikbaar vanaf ETS 5.5 / [3] Wordt niet op alle apparaten ondersteund