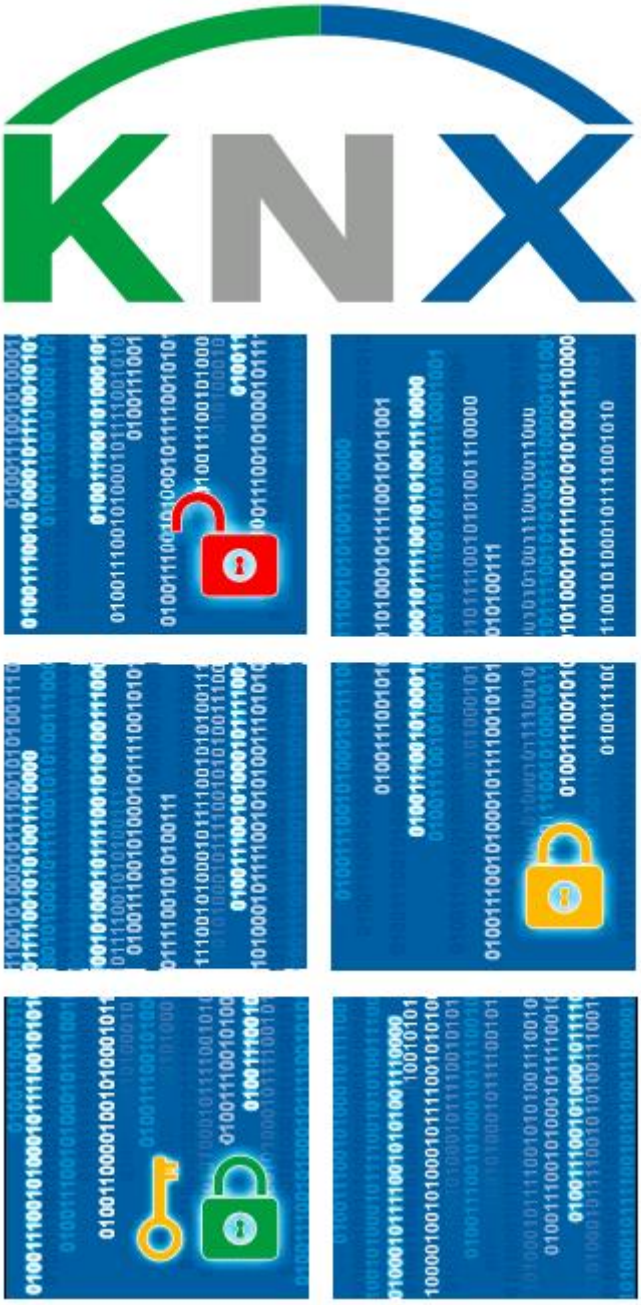

KNX zabezpečení
Kontrolní seznam

Kontrolní seznam pro zajištění bezpečnosti KNX instalace

1 Byla následující opatření využita během montáže instalace?

- [ ] Jsou přístroje a aplikace pevně připojeny? Je zaručeno, že přístroje jsou řádně chráněny proti demontáži (např. použití opatření na ochranu proti krádeži)?
- [ ] Je zaručeno, že neoprávněné osoby mají omezený přístup k rozvaděčům s namontovanými instalačními prvky KNX (např. vždy uzamčeny nebo jsou v uzamčených místnostech)?
- [ ] Jsou přístroje ve venkovních místech obtížně přístupné (např. namontované v dostatečné výšce)?
- [ ] V případě, že instalace KNX může být ovládána z veřejně přístupných oblastí v budovách, která nejsou hlídaná, jsou použity binární vstupy (namontované v rozvaděčích), nebo tlačítková rozhraní?

2 Je kroucený pár použit jako komunikační médium?

- [ ] Je kabel kdekoliv uvnitř nebo mimo byt nebo budovu chráněn proti neoprávněnému přístupu?
- [ ] V případě, že kabel s krouceným párem je použit v oblastech, které vyžadují zvláštní ochranná opatření, byla přijata opatření podle bodu 6?

3 Je Powerline použit jako komunikační médium?

- [ ] Byly již nainstalovány pásmové nádrže?
- [ ] Pokud se Powerline používá také vně budovy, byla přijata stejná opatření k provázání médií, jak je uvedeno v bodě 6?

4 Je IP použito jako komunikační médium?

- [ ] Byla již zdokumentována síťová nastavení a byla předána majiteli objektu nebo správci sítě LAN?
- [ ] Byly již spínače a routery nastaveny takovým způsobem, že pouze známými MAC adresami lze získat přístup ke komunikačnímu médiu?
- [ ] Je oddělená LAN nebo WLAN síť s vlastním hardwarem použita pro komunikaci KNX?
- [ ] Je přístup ke (KNX) IP sítím omezen na oprávněné osoby prostřednictvím vhodných uživatelských jmen a silných hesel?
- [ ] Pro KNX IP Multicast komunikaci byla použita jiná IP adresa jako výchozí adresa (obvykle 224.0.23.12). Byla tato IP Multicast adresa změněna?
- [ ] Byla změněna výchozí SSID bezdrátového přístupového bodu? Bylo periodické vysílání SSID deaktivováno?
- [ ] Byly porty routerů pro KNX uzavřeny pro internet a bylo výchozí rozhraní použité jako KNXnet / IP router nastaveno na 0? Byla instalace (W) LAN chráněna vhodným firewallem? Je-li nutný přístup instalace KNX k internetu, zkontrolujte možnost implementovat:
  1. Navázání spojení VPN k síti Internet Router
  2. Použití KNX objekt serveru konkrétních výrobců

5 Je bezdrátový přenos RF použit jako komunikační médium?

- [ ] Jsou přijata stejná opatření k mediálním spojkám, jak je uvedeno v bodě 6?
- [ ] Má každá RF doména jinou adresu domény?

6 Jsou v instalaci použity spojky?

- [ ] Byly individuální adresy přístrojů přiřazeny podle jejich umístění v topologii?
- [ ] Je zabráněno pomocí nastavení příslušných parametrů spojek, aby nesprávné zdrojové adresy byly předávány mimo linii?
- [ ] Je blokována komunikace bod po bodu a Broadcastingový přenos přes spojky?
- [ ] Byly správně nahrány filtrační tabulky a bylo nastavení uskutečněno takovým způsobem, že spojky berou do úvahy filtrační tabulky?
- [ ] Uvažovali jste o opatření pro spojky, jak je uvedeno v bodě 7?

7 Jsou přístroje zabezpečeny proti jinému nastavení?

- [ ] Pokud tomu tak není, zadejte v projektu ETS sběrnicovým spojkám klíč[1].

8 Jsou použity přístroje KNX Secure[2]?

- [ ] Aby byla zajištěna zabezpečená skupinová komunikace, musí být využity předpokládané autentizační a šifrovací mechanismy přístroje.

9 Máte podezření, že došlo neoprávněnému přístupu ke sběrnici?

- [ ] Záznam telegramového provozu a jeho analýza.
- [ ] Přečtěte PID_Device_Control[3] z přístroje a zkontrolujte, zda přístroj odesílá shodnou individuální adresu.
- [ ] Přečtěte PID_Download_Counter[3] z přístroje a zkontrolujte, zda přístroj byl znovu nahrán po jeho konfiguraci.

10 Propojení KNX do zabezpečovacích systémů?

- [ ] Je-li KNX systém propojen se zabezpečovacími instalacemi, projeví se to v některé z následujících možností?
  1. Přes KNX přístroje nebo rozhraní certifikované národními pojišťovnami?
  2. Prostřednictvím bezpotenciálových kontaktů (binární vstup, tlačítková rozhraní, ...)?
  3. Prostřednictvím vhodných rozhraní (RS232, ...) či bran: bylo tak zajištěno, že KNX komunikací je možné spustit příslušné zabezpečovací funkce v zabezpečovací části instalace?

1) Ne všechny přístroje mohou být chráněny proti neoprávněnému překonfigurování - obraťte se na příslušného výrobce

2) K dispozici od ETS 5.5 a vyšší

3) Není podporováno všemi přístroji

KNX zabezpečení – kontrolní seznam

www.knx.org
www.knxcz.cz