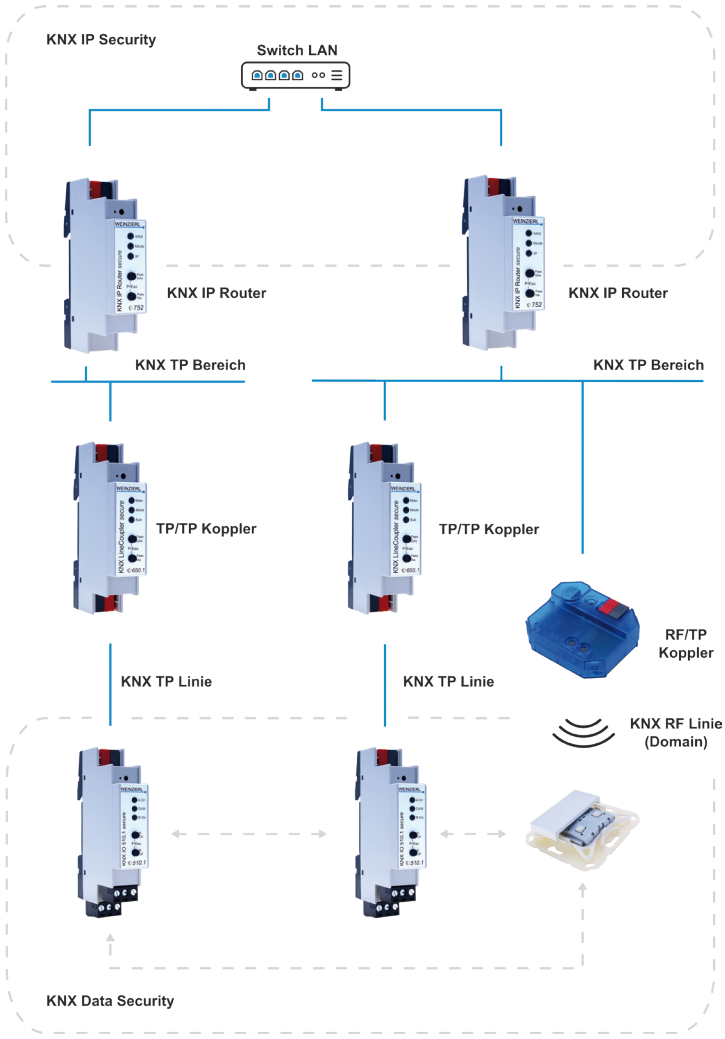
Installationen von innen und außen schützen



Fehlermeldung des Webbrowsers über mangelnde Sicherheit

Kommunikation und Datenverarbeitung sind heute ohne Berücksichtigung von Sicherheitsaspekten kaum noch denkbar. In der Tat werden unsichere Kommunikationssysteme schnell inakzeptabel. Das Internet hat es vorgemacht: Das bekannte http-Protokoll aus dem Jahr 1991 wurde weitgehend durch die verschlüsselte Variante https ersetzt. Ein Jahr früher als http wurde übrigens das KNX-System unter dem Namen EIB eingeführt.

Bedarf an sicherer Kommunikation

Auch in Gebäuden ist der Bedarf an sicherer Kommunikation nicht mehr zu übersehen. Derzeit gibt es zwar, trotz der Berichte über Manipulationen, kaum konkrete Hinweise auf tatsächliche Schäden durch Hacker, aber ihre Bemühungen werden wahrscheinlich zunehmen, sodass es notwendig ist, potenziellen Gefahren für die technische Infrastruktur zu begegnen. Die abgebildete Fehlermeldung des Webbrowsers über mangelnde Sicherheit sollte auch als Warnung für die Gebäudetechnik dienen.

Entstehung von KNX Security

Als Herstellerverband hat sich die KNX Association schon früh unter dem Titel „KNX Security“ mit dem Thema Sicherheit beschäftigt. Die Spezifikation und Umsetzung dauerte mehrere Jahre, was nicht zuletzt an der Komplexität des KNX Protokolls liegt, bei dem die für das gesamte KNX-System essentielle Gruppenadressierung eine große Herausforderung für eine sichere Verschlüsselung darstellt.
Anfang 2019 galten sowohl das System als auch die Testspezifikationen als stabil und wurden vom Technischen Ausschuss (KNX Technical Board) der KNX Association genehmigt. Darüber hinaus investierte die KNX Association viel Aufwand in die Umsetzung des Sicherheitsthemas in der ETS – der zentralen Installationssoftware für KNX. Auch die Testwerkzeuge für die Entwicklung von KNX Secure Geräten wurden entsprechend erweitert und zertifizierte KNX Secure Produkte sind verfügbar.
KNX Security wird in zwei Varianten unterschieden: KNX Data Security und KNX IP Security.

KNX Data Security

KNX Data Security zielt auf eine sichere Kommunikation auf Telegrammebene ab. Es kann unabhängig vom KNX Medium sowohl für die Inbetriebnahme als auch für die Laufzeitkommunikation genutzt werden KNX Data Security bietet den Schutz innerhalb der KNX Installation.

KNX IP Security

KNX IP Security verfolgt einen alternativen Ansatz, basiert aber auf den gleichen Verschlüsselungsmethoden wie KNX Data Security. KNX IP Security ist ein pragmatischer Ansatz, der auf der Annahme beruht, dass es einen Angriffspunkt auf der IP-Ebene gibt. Während man davon ausgeht, dass KNX Twisted Pair als rein lokales Medium in der Wand relativ sicher ist, ist die IP Kommunikation oft mit dem Internet verbunden und kann daher aus der Ferne angegriffen werden. KNX IP Security schützt die KNX-IP-Kommunikation, während Twisted Pair unverschlüsselt bleibt. KNX IP Security schützt vor dem Eindringen Unbefugter in die KNX Installation.

KNX IP Routing & Tunneling

KNX IP enthält das KNX-IP-Routing-Protokoll, das für IP-Backbones verwendet wird, aber auch das KNX-IP-Medium darstellt. Auf der anderen Seite wird das Tunneling-Protokoll verwendet, um einem Client (z.B. ETS) den Zugang zu einer TP-Linie über IP zu ermöglichen. Während KNX-IP-Router in der Regel beide Protokolle implementieren, unterstützen KNX IP Schnittstellen nur die Tunnelfunktion.

Gemischte Installationen mit und ohne Security

Da nicht zu erwarten ist, dass alle benötigten Geräte kurzfristig in der secure Variante zur Verfügung stehen, ist es wichtig, dass secure und unsecure Kommunikation in einer Installation gemischt werden können. Die sichere Eigenschaft wird auf Gruppenebene definiert. Wenn zwei Gruppenobjekte, die beide Security unterstützen, miteinander verbunden sind, schlägt die ETS eine sichere Verbindung vor. Wenn jedoch nur ein Objekt in einer Gruppe ohne Security ist, muss die gesamte Gruppe unsecure kommunizieren. ◄

Weinzierl Engineering GmbH
info@weinzierl.de
www.weinzierl.de