KNX Association cvba
De Kleetlaan 5 bus 11
B-1831 Brussels-Diegem
Belgium

Tel.: +32 (0) 2 775 85 90
Fax: +32 (0) 2 675 50 28

info@knx.org
www.knx.org

Pressemitteilung

KNX Secure – Sichere KNX Kommunikation

KNX IP Secure und KNX Data Secure machen KNX Installationen zugriffsicher.

BRÜSSEL, 24. August 2016: Es gibt sie, die Hacker, die in die Gebäudetechnik eindringen. Witzbolde schalten dann Licht beim Nachbarn und brüsten sich damit. Mit krimineller Energie und entsprechendem Fachwissen kann aber auch großer Schaden angerichtet werden. Deshalb ist das Thema KNX Secure brandaktuell. KNX ist bisher schon den Sicherheitsansprüchen gerecht, wenn Installateure der Gebäudesystemtechnik die empfohlenen Schutzmaßnahmen gegen Manipulation beachten. Doch mit neuen Medien wie LAN und WLAN, mit Internetzugang, drahtlosen Bedienkonzepten und Anwendungen in sensiblen Bereichen erhöht sich das Schadensrisiko durch unerwünschte Eindringlinge. Diesen und anderen Anforderungen entsprechend hat KNX neue Sicherheitskonzepte entwickelt: KNX Data Secure und KNX IP Secure. Beide basieren auf weltweit etablierten Sicherheitsprotokollen und können auch in die bestehenden KNX Anlagen nahtlos integriert werden.

Mit den Möglichkeiten der Fernanbindung von KNX Installationen über das Internet oder/und dem Drahtlosnetzwerk WLAN werden zusätzliche technische Sicherungsmaßnahmen notwendig. Durch Zugriff auf Geräte und Medien besteht die Gefahr der Manipulation des Datenverkehrs. Es ist also notwendig, die übertragenen Informationen auf jedem Medium (KNX TP, PL, RF, IP) gegen Änderungen oder gegen Aufzeichnung eines Telegramms und dessen manipulierende Wiederholung durch Eindringlinge zu schützen. Der Fernzugriff über das Internet auf ein KNX Bussystem sollte so abgesichert werden können, dass die Bedienung und Konfiguration von Busgeräten nur durch nachweislich Berechtigte erfolgen kann. Ein wirksamer Schutzmechanismus gegen Manipulationen ist, wenn nur Busteilnehmer miteinander kommunizieren können, die sich gegenseitig als Teils des Bussystems erkennen. Diesen und anderen Anforderungen entsprechend hat KNX neue Sicherheitskonzepte entwickelt: KNX Data Secure und KNX IP Secure. Beide verwenden Mechanismen, wie sie zum Beispiel zur sicheren Übertragung von Daten zwischen Elektrozählern und Energieversorgern (EVU) Verwendung finden.

Verschlüsselte Telegramme

Werden Daten über das Internet gesendet, lässt sich die Verbindung zwischen dem Sender- und Empfängernetzwerk durch eine VPN-Verbindung schützen. Damit ist aber nicht sicher, ob der Sender

autorisiert ist, das Bussystem zu konfigurieren oder Daten mit ihm auszutauschen. Hier bietet KNX IP Secure zusätzliche Sicherheit, indem das KNX IP Protokoll so erweitert wird, dass die übertragenen Daten vollständig verschlüsselt sind. Diese lässt sich mit kleinem Zusatzaufwand besonders auch in bestehenden Anlagen umsetzen.

Wenn Daten nur lokal über KNX gesendet werden, genügt es, entsprechend Anwendungsdaten zusätzlich durch eine Erweiterung des Busprotokolls zu schützen. Der spezifizierte Schutzmechanismus KNX Data Secure bewirkt, dass unabhängig vom Medium ausgewählte KNX Telegramme authentifiziert und/oder verschlüsselt werden. Die Schlüssel werden über die ETS den Geräten bzw. Objekten zugeordnet. Da in einem und demselben KNX System gesicherte und ungesicherte Anwendungen möglich sind, müssen nicht alle Geräte gesichert sein. Auch vorhandene Systemkomponenten kann man belassen. Somit hält sich der Aufwand in Grenzen und wird die Investition in die KNX Bustechnik gewahrt.

Sicherheitsprotokoll weltweit etabliert

Mit den neuen spezifizierten Schutzmechanismen KNX Data Secure und KNX IP Secure lassen sich künftige gesicherte Kommunikationskanäle zwischen den KNX Teilnehmern aufbauen. So wird verhindert, dass ein Angreifer durch Einspeisen manipulierter Meldungen Kontrolle über die Anlage bekommt. Dazu ist jede Meldung mit einem Authentifizierungscode versehen. Der Versuch, Meldungen aufzuzeichnen und diese später zum Zweck einer Sabotage zu senden, wird durch automatische Vergabe von Sequenznummern bzw. einer Sequenzidentifikation verhindert. Schließlich macht die Verschlüsselung des Netzwerkverkehrs KNX Installation nahezu unangreifbar. Das Verfahren basiert auf weltweit etablierten Sicherheitsprotokollen.

Einführung mit ETS 5.5

Nicht zuletzt liegt es an den Planern, Installateuren und Systemintegratoren, dass Hacker keine Chance bekommen. Sie müssen die Schutzmaßnahmen kennenlernen und umsetzen. Bei der Übergabe der Anlage und durch regelmäßige Überprüfung im Betrieb lassen sich die Anlagenfunktionen und das angestrebte Sicherheitsniveau sicherstellen. Die neuen Sicherheitsfunktionen, insbesondere für den Zugriff über das Internet, können in bestehende Anlagen durch Verwendung von Schnittstellen mit den neuen KNX Sicherheitsmechanismen eingeführt werden. KNX IP Secure und KNX Data Secure werden ab der neuen ETS 5.5 auch in der Planungs- und Inbetriebnahmesoftware unterstützt.

Weitere Informationen:

Weitere Informationen zum Thema KNX Secure, wie u.a. eine KNX Secure Checklist, das KNX Secure Positionspapier, eine Einladung zum KNX Secure Webinar, etc., stehen Ihnen auf der KNX Secure Webseite zur Verfügung: http://knxsecure.knx.org

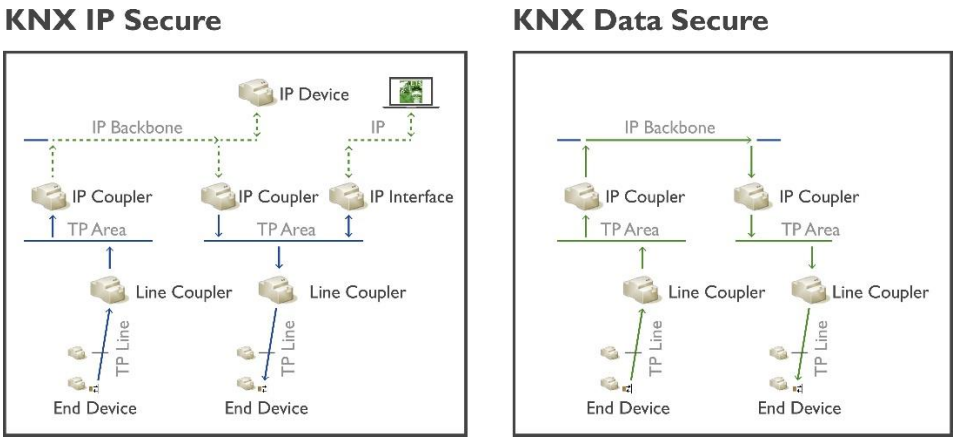

Bild 1: KNX IP Secure für sichere KNX Übertragung zwischen Gebäuden

KNX Data Secure für sichere KNX Übertragung im Gebäude

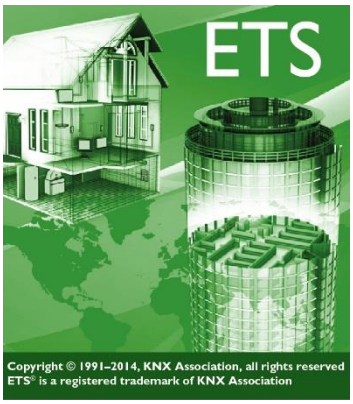

Bild 2: KNX IP Secure und KNX Data Secure sind ab der neuen ETS 5.5 verfügbar.

Über KNX
KNX Association ist der Begründer und Eigentümer der **KNX** Technologie – des weltweiten STANDARDS für alle Anwendungen im Bereich Haus- und Gebäudesystemtechnik, von der Beleuchtungs- und Rollladensteuerung bis hin zu Sicherheitssystemen, Heizung, Lüftung, Kühlung, Überwachung, Alarm, Wasserregelung, Energiemanagement und Zähler wie auch Haushaltsgeräten, Audio/Video und mehr. **KNX** ist weltweiter Standard für Haus- und Gebäudesystemtechnik mit einem einzigen hersteller- und produktunabhängigen Inbetriebnahme Tool (ETS), mit einem kompletten Satz von Übertragungsmedien (TP, PL, RF und IP) wie auch einem kompletten Satz von Konfigurationsmodi (Systemmodus und Einfacher Modus). **KNX** ist als

Europäischer Standard (CENELEC EN 50090 und CEN EN 13321-1) und als internationaler Standard (ISO/IEC 14543-3) anerkannt. Dieser Standard basiert auf 26 Jahren Erfahrung. Über 400 Mitgliedsunternehmen weltweit bieten fast 7.000 **KNX** zertifizierte Produktgruppen in ihren Katalogen an. Die **KNX** Association hat mit nahezu 53.000 Installationsfirmen in 143 Ländern Partnerschaftsverträge.

www.knx.org

Für mehr Information/Material, bitte wenden Sie sich an:
heinz.lux@knx.org

Bilder können auf folgender Webseite heruntergeladen werden:
www.knx.org/knx-de/presseraum/