P E R S B E R I C H T

*Maximale privacybescherming voor slimme gebouwen*

**Internationaal gestandaardiseerde KNX Secure zorgt voor allerhoogste veiligheidsniveau**

Brussel, 30 oktober 2017 – KNX is het eerste en tot op heden enige protocol voor slimme woningen en gebouwen dat overal ter wereld voldoet aan de hoogste veiligheidseisen op het gebied van cyber security. Dat is officieel bevestigd door internationale standaardiseringscomités. KNX Secure, de veiligheidsarchitectuur van het protocol, heeft per direct de EN 50090-4-3 certificering gekregen.

Via KNX Secure beschermt KNX de digitale infrastructuur van slimme gebouwen tegen hackersaanvallen en garandeert het een maximale privacybescherming. Digitale inbraken op een KNX-systeem zijn als de juiste KNX Secure componenten worden gebruikt, verleden tijd.

**Zwakke punten in netwerken**

Al langer waarschuwen IT-experts dat hackers zich in toenemende mate richten op de infrastructuur van slimme woningen en gebouwen. Steeds vaker zijn er nieuwe gevallen bekend waarbij hackers voor hun digitale rooftochten gebruik hebben gemaakt van de zwakke punten van producten, interfaces of draadloze netwerken. “Tot nu toe kwamen inbrekers binnen via deuren en ramen. Nu is dat via draadloze en bedrade communicatienetwerken. Met de digitale aansluiting van gebouwen zijn ook de gevaren veranderd. Hiervoor heeft tot op heden alleen KNX het passende antwoord", legt Franz Kammerl, president van de KNX Association, uit.

**De hoogste coderingsnormen**

De ontwikkelaars van KNX hebben al vroeg op de nieuwe bedreigingen gereageerd en uitgekiende beschermingsconcepten voor slimme gebouwen geïmplementeerd in het internationaal gestandaardiseerde protocol. Daarmee is de veiligheidsarchitectuur KNX Secure ontstaan, die onder andere gebaseerd is op de internationaal, conform ISO 18033-3 genormeerde veiligheidsalgoritmen zoals de AES 128 CCM-codering. Via die algoritmen kan men aanvallen op de digitale infrastructuur van gebouwen effectief verhinderen en maximale privacybescherming realiseren.

**Dubbele veiligheid**

Dankzij een dubbel beschermingsconcept biedt KNX Secure dubbele veiligheid. Dit bestaat in feite uit twee mechanismen:

1. KNX IP Secure beveiligt de IP-communicatie tussen de KNX-installaties. Hiervoor breidt KNX IP Secure het IP-protocol zo uit, dat alle overgedragen telegrammen en gegevens volledig gecodeerd worden.
2. KNX Data Secure beveiligt door middel van codering en authenticatie de gebruiksgegevens – ook wanneer ze met de verschillende bedieningsdevices worden uitgewisseld – tegen onbevoegde toegang en manipulatie. Beide mechanismen kunnen met elkaar gecombineerd en parallel worden gebruikt, om voor maximale veiligheid te zorgen.

"Bedieningsdevices, interfaces, draadloze netwerken en communicatieprotocollen: zwakke punten kunnen overal zijn. Daarom moeten slimme woningen en gebouwen met de meest uitgebreide en op dit gebied wereldwijd unieke, erkende veiligheidsnorm worden beveiligd. Gebruik dus KNX Secure", aldus Franz Kammerl.

Voor meer informatie zie de speciale website: <http://KNXSecure.knx.org>

**Noot voor de redactie:**

Voor meer informatie: Rob van Mil, woordvoerder KNX Nederland, 06-54681144, rob@stijlmeesters.nl