IoT zorgt voor groeispurt in wereld van smarthome

In maart 2020 bleek uit de Smart Home Monitor dat de Nederlandse consumenten inmiddels al 2,5 miljard euro aan smarthome-apparaten in huis heeft. Dit betekent dat de markt in één jaar, van 2018 naar 2019, met 800 miljoen euro (47 procent) groeide. Ook een pan-Europese enquête van BSRIA constateert deze forse groei van op internet gebaseerde technieken. BSRIA concludeert ook dat KNX het populairste protocol is voor woning- en gebouwautomatisering in de meeste Europese markten.

Over een paar jaar zijn minimaal 20 miljard apparaten verbonden via het Internet of Things (IoT). Deze enorme golf van internettechnologie zal de bediening en bewaking van woningen en gebouwen sterk beïnvloeden. De internationale KNX Association, met wereldwijd meer dan 450 fabrikanten als lid, is ervan overtuigd dat juist de combinatie van haar KNX-protocol met die van IP de basis vormt voor een toekomstvast automatiseringsconcept. De standaard draagt bij aan de technische standaardisatie in de industrie. BSRIA schat dat het aandeel KNX-gebaseerde oplossingen gemiddeld 50 procent bedraagt.

IoT wordt groot in gebouwen

Gebouwen zijn de grootste gebruikers van het IoT. Slimme huizen komen op de tweede plaats, met wereldwijd ongeveer 1 miljard verbonden apparaten in 2018. Uit onderzoek van Gartner blijkt dat commercieel vastgoed sterk profiteert van IoT-implementaties die leiden tot nieuwe diensten als het verzamelen van gegevens en inzichten uit sensoren. Vooral in industriële zones, kantoorgebieden, winkelcentra en lucht- en zeehavens kan IoT bijdragen aan het verminderen van de kosten van energie, ruimtelijk beheer en onderhoud van gebouwen.

Gebruiksgemak

De groep consumenten die verwacht binnen twee jaar een volledige smarthome te hebben, is verdubbeld ten opzichte van vorig jaar. De belangrijkste reden voor bezitters en niet-bezitters van slimme apparaten om géén smarthome-producten aan te schaffen, is de prijs van deze producten (37 procent). De meest genoemde beweegredenen om wél slimme apparaten in huis te halen is gebruiksgemak, energiebesparing en plezier.

KNX is in feite IoT

Inmiddels is in de praktijk al duidelijk dat IoT geen bedreiging is voor het automatiseringsprotocol KNX, maar juist een zakelijke kans. Volgens Joost Demarest, chief technology officer van de internationale KNX Association in Brussel, zijn er vele KNX-innovaties die nu op de markt komen en die de IoT-integratie faciliteren. "IoT gaat KNX niet wegvegen. Sterker nog, als je naar de definitie van IoT kijkt, dan zijn wij in feite het IoT. De hele configuratie en samenstelling van een KNX-netwerk, heeft één op één alle kenmerken van een IoT-configuratie."

Volstrekt interoperabel

"Met onze nieuwe producten en toepassingen zijn wij volstrekt interoperabel en kunnen we nog beter gebruik maken van de mogelijkheden die het IoT biedt", aldus Demarest. "Omdat onze bestaande IP-routers en IP-gateways, die KNX-fabrikanten op de markt brengen, nog niet IT-friendly genoeg zijn, hebben we KNX Web Services geïntroduceerd. Hiermee bieden we een nieuwe, verbeterde manier om KNX-systemen te integreren in het internet en ze via het internet te besturen en te visualiseren. Via de gateway van KNX Web Services, die onze leden op de markt brengen, maken we het voor IT-specialisten eenvoudiger om door de data van onze installaties te browsen. KNX legt zo, bij wijze van spreken, de rode loper voor hen uit."

Beveiligings-issues

Een opvallende trend binnen de markt van smarthome-producten is de toename van het gebruik van slimme luidsprekers. Van de consumenten die bekend zijn met het fenomeen smarthome, heeft inmiddels bijna een vijfde van hen een slimme speaker in huis. Via deze slimme speakers is het mogelijk om met behulp van een virtuele assistent van bijvoorbeeld Google, Apple of Amazon slimme apparaten en systemen in het huis met stemcommando's aan te sturen. Om een slimme luidspreker te gebruiken, moet deze via het internet (wifi) met de woningautomatisering worden verbonden. Vaak brengt die verbinding met het internet ook het gemak met zich mee doordat de gebruiker (en vaak ook de installateur) de installatie ook op afstand, op een andere locatie, kan bedienen.

Open verbinding

Maar die verbinding brengt een risico met zich mee, wanneer deze niet goed wordt beveiligd. Zet je zomaar een poort op de router open, of ga je onzorgvuldig om met segmentering van het netwerk, dan kunnen hackers in het systeem inbreken en de bediening overnemen. Bezitters en niet-bezitters van smarthome-producten zijn onvoldoende van die risico's op de hoogte. En dat geldt helaas ook voor de installateur en system integrator. Bewustwording is daarom erg belangrijk. En de mensen die zich wel van deze risico's bewust zijn, noemen de gevaren vaak als reden om smarthome-producten niet aan te schaffen. Met name privacy-issues en de angst voor hacking zien velen als dé blokkade om een woning of gebouw te automatiseren.

Dubbele veiligheid

Om die angst uit de weg te ruimen, ontwikkelde KNX het beveiligingsconcept KNX Secure. KNX Secure omvat twee verschillende mechanismen, waardoor het concept in feite uit twee veiligheidslagen bestaat. De eerste: KNX IP Secure beveiligt de IP-communicatie tussen KNX-installaties en het internet. Speciale KNX IP Secure componenten tussen het KNX-systeem en het internet maken dat het doorgeven van informatie volledig veilig kan verlopen. De tweede: KNX Data Secure beveiligt door middel van codering en authenticatie van de data op de KNX-bus – ook wanneer ze met de verschillende bedienings-devices worden uitgewisseld – tegen onbevoegde toegang en manipulatie. KNX IP Secure en KNX Data Secure kunnen met elkaar worden gecombineerd en parallel worden gebruikt, om voor maximale veiligheid te zorgen. Meer informatie - onder meer een gratis 'KNX Handboek voor adviseurs' - is te vinden op de community www.smartinside.nl.

Internationale norm voor KNX Secure

KNX is het eerste en tot op heden enige protocol voor slimme woningen en gebouwen dat overal ter wereld aan de hoogste veiligheidseisen kan voldoen. Dit is officieel bevestigd met de toekenning van de internationale veiligheidsstandaard EN ISO 22510 aan de techniek van KNX IP Secure. In 2015 is KNX Secure ontwikkeld op basis van internationale beveiligingsalgoritmen die in overeenstemming met ISO 18033-3 zijn gestandaardiseerd. De systematiek maakt gebruik van erkende codering in overeenstemming met AES 128 CCM. Demarest: "We hebben een laag in onze standaard toegevoegd die het fabrikanten mogelijk maakt om berichten in ons protocol te versleutelen en te authenticeren. De IP-backbone valt zo niet af te luisteren zonder de geheimtaal te kennen."

Door: Rob van Mil