21 februari 2019

Onderzoek: Duizenden huizen en kantoren kwetsbaar voor hackers door onbeveiligde domotica

Duizenden gebouwbeheersystemen van ‘slimme’ woningen en kantoren wereldwijd zijn eenvoudig toegankelijk voor hackers. Dit constateert een ethisch hacker van Computest op basis van een security-onderzoek naar de KNX-standaard voor woning- en gebouwautomatisering. Uit het onderzoek blijkt dat de systemen die zijn gebaseerd op deze standaard, veelvoudig aan het internet gekoppeld worden. Doordat deze systemen echter geen enkele vorm van authenticatie bevatten, kunnen kwaadwillenden hiermee op afstand onder meer de beveiliging, verlichting, airconditioning en verwarming van huizen en kantoren bedienen. In totaal zijn er 17.444 gebouwen met systemen die zijn gebaseerd op de KNX-standaard waarvan er zich 1.322 in Nederland bevinden. Hiermee is Nederland na Spanje en Duitsland, het land met de meeste locaties die kwetsbaar zijn voor hackers.

Security-scan laat 17.444 kwetsbare locaties zien
Zowel bedrijven als particulieren verbinden steeds meer systemen met het internet. Het onderling koppelen van deze IoT-toepassingen zorgt voor extra gemak, maar brengt ook serieuze risico’s met zich mee. Het onderzoek van ethisch hacker Daan Keuper richtte zich op verschillende domotica-toepassingen die zijn gebaseerd op de KNX-standaard. Hij ontdekte dat er wereldwijd 17.444 gebouwen en woningen zijn waarvan de systemen vrij eenvoudig door een hacker kunnen worden overgenomen. Spanje en Duitsland voeren de lijst aan met respectievelijk 1.985 en 1.768 locaties. Nederland volgt met 1.322. Amsterdam is in ons land de stad met de meeste gebouwen met een KNX-systeem. De security-scan van Keuper liet verder zien dat ook in China, Amerika en Rusland gebouwbeheersystemen gebaseerd op de KNX-standaard te vinden zijn.

Computest vermoedt dat KNX-systemen doorgaans door installateurs aan het internet gekoppeld worden om netwerken op afstand te kunnen configureren. Daarnaast wordt het protocol door sommige mobiele apps gebruikt om op afstand domotica-oplossingen te bedienen.

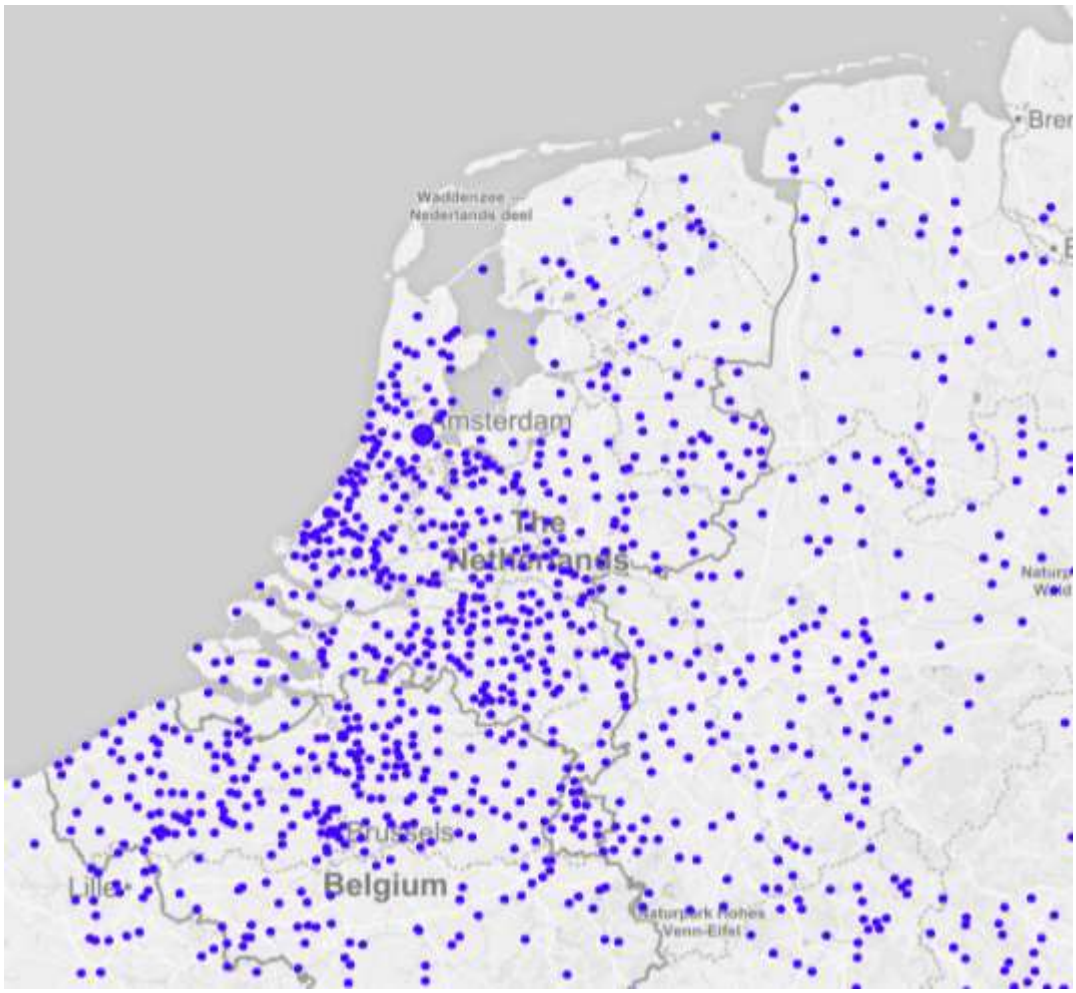
Verantwoordelijkheid security
“Als er gebruikgemaakt wordt van een standaard, gaat men er doorgaans vanuit dat het met de security ook wel goed zit”, zegt Keuper. “Het ontbreken van authenticatie in de KNX-systemen laat zien dat dit een gevaarlijke aanname is.” De verantwoordelijkheid voor een goede beveiliging van de systemen ligt volgens Computest zowel bij de leverancier, de installateur als bij de consument. De

consument moet de installateur kunnen aanspreken op de security van hetgeen wordt geïnstalleerd. Het idee is dat deze installateur hetzelfde doet richting de leverancier en/ of andere partijen in de keten. Daarmee worden de leverancier en de installateur zelf ook kritischer in welke producten zij selecteren en zijn ze eerder in de positie om eisen te stellen en te kiezen voor partijen voor wie die de beveiliging van hun toepassingen een prioriteit is.

“Er is nog veel werk te verrichten in het bewust maken van de installatiebranche van de risico’s die deze slimme systemen met zich meebrengen”, vindt Petra Oldengarm, Directeur van Cyberveilig Nederland. “Daarnaast is het belangrijk dat men weet hoe deze risico’s moeten worden geminimaliseerd. Daarom zijn we in gesprek met vertegenwoordigers van de installatiebranche om initiatieven te ontplooien die bijdragen aan het ontwikkelen van het bewustzijn en het kennisniveau, zodat gebruikers kunnen vertrouwen op KNX-producten die in hun kantoor of huis worden geïnstalleerd.”

Zelf controleren of KNX-installatie veilig is

Om gebouwbeheerders en consumenten in staat te stellen te controleren of hun KNX-installatie veilig is, heeft Computest de site www.knxscan.com in het leven geroepen. Om de installatiebranche niet alleen bewust maken van dit probleem, maar ook te helpen het op te lossen, organiseert Computest bovendien op 19 maart een gratis training. Hiermee krijgen installateurs inzicht in de security-risico’s en hoe zij deze kunnen minimaliseren.



Klik hier voor de interactieve kaart van de wereldwijde locaties met KNX-systemen.

Over Computest

Computest is opgericht in 2005 en is de enige specialist in Nederland die het complete portfolio aanbiedt op het gebied van performance, security en geautomatiseerd functioneel testen. Het bedrijf helpt met een geïntegreerde benadering organisaties en instellingen in onder meer de financiële sector, de e-commerce- en mediabranche en bij de overheid, de prestaties en beveiliging van hun applicaties en digitale netwerken te optimaliseren. Computest telt circa 100 medewerkers en is gevestigd in Zoetermeer. Meer informatie: http://www.computest.nl/.

Meer informatie:

ItsaRep
Chantal Schepers
computest@itsarep.nl
06 235 099 23