Internet en de dingen die vreselijk kunnen misgaan

De thermostaat, de koelkast, een pacemaker - dankzij het web kunnen we op afstand veel dingen regelen zonder het apparaat in handen te hebben. Alleen is het met de beveiliging van die toestellen vaak beroerd gesteld.

DOOR PETER VAN AMMELROOY
ILLUSTRATIE STUDIO VONQ

Gemak dient de mens. Dankzij internet kunnen we onze digitale videorecorder thuis programmeren terwijl we op kantoor zitten. We kunnen zo ook de thermostaat een paar graden hoger draaien en de hond te eten geven met een brokjesdispenser. Er zijn al meer dan vijf miljard van dit soort apparaten. Wekelijks komen er 5,5 miljoen bij. Dit internet of things (IoT, of internet der dingen) groeit als een gek.

Gemak dient ook de hacker.

Canadese en Israëlische onderzoekers lieten dat vorige week zien met een technologie die al vijftien jaar wordt gebruikt om apparaten draadloos met het internet te laten 'praten'. ZigBee is een radioprotocol dat draadloos een brug slaat tussen digitale sloten, schakelaars, lampen, rookmelders en het wereldwijde computernetwerk.

ZigBee-zendertjes hebben een bereik van zo'n tien meter. Grotere afstanden worden overbrugd doordat de toestellen de gegevens via elkaar doorgeven naar een kastje dat ons toegang verleent tot het internet.

Internetcriminelen kunnen die eigenschap misbruiken om een heel netwerk te besmetten met een computervirus. Het onderzoeksteam demonstreerde dat met Hue, een lichtregelsysteem van Philips met lampen die elke gewenste kleur kunnen aannemen en die zich laten dimmen met een smartphone-app.

De onderzoekers vlogen een drone met zender langs een kantoor waarin ze Hue-lampen hadden aangebracht. Hoe dichter de drone het gebouw naderde, hoe meer lampen er begonnen te flikkeren. Ze raakten van slag door een virus dat van lamp naar lamp was gehopt.

Knipperende verlichting lijkt geen levensbedreigend probleem, al zijn lampen zo te ontregelen dat ze epileptische toevallen veroorzaken. Maar onlangs toonden onbekenden aan dat IoT-apparaten wel degelijk schade kunnen veroorzaken.

Duizenden videorecorders en webcamera's werden 21 oktober gebruikt om een ongekend zware aanval uit te voeren op een Californisch internetbedrijf. De hackers hadden die IoT-toestellen eerder met een computervirus in gijzeling genomen. Zo ontstond een leger van 'zombie-apparaten' dat massa's onzinnige data zond naar de servers van het bedrijf. Die bezweken onder die digitale tsunami. Daardoor waren sites als Twitter, Amazon, Paypal, Spotify en Reddit uren onbereikbaar.

Liever cool dan veilig

Slecht beveiligde IoT-apparaten zijn eerder regel dan uitzondering, zegt Paul Ducklin van de Britse computerbeveiliger Sophos. 'Er zijn veel toestellen op de markt gekomen die niet waren bedoeld om aan het internet te hangen. Zoals bewakingscamera's. Die waren ooit groot en zwaar en zaten met dikke kabels vast aan een enkele computer.'

'Nu koop je kekke beveiligingscamera's voor 30 euro, plak je ze tegen het plafond en sturen ze draadloos hun beeld naar je smartphone.' Er is evenwel een probleem, zegt Ducklin: 'Alle aandacht van de fabrikant gaat naar coole functies. Een hoop camera's zijn zo slecht beveiligd dat een hacker kan zien dat jij in de bioscoop zit.'

Maar hoe groot is de kans dat hackers tussen die miljarden andere apparaten op internet nou net ons IoT-broodrooster vinden?

Groot. Hackers hoeven niet handmatig het net af te speuren. Daar zetten ze bots voor in, zelfstandige opererende programmaatje die gegevens over IoT-apparaten verzamelen. Uitzoeken welke apparaten digitaal kwetsbaar zijn, is een koud kunstje.

Een journalist van het Amerikaanse tijdschrift The Atlantic nam recent de proef op de som. Hij verbond een broodrooster met internet en keek hoe snel hackers zouden proberen het apparaat te kapen. 'Ik had met experts gesproken en ging ervan uit dat het mogelijk een week zou duren en misschien wel nooit zou gebeuren', zei Andrew McGill in een interview. 'Maar het gebeurde veel sneller. Binnen 41 minuten. De tweede poging kwam 10 à 15 minuten daarna.' Gemak dient de mens - tegen een prijs.

Tien markante IoT-toepassingen

1. Toilet

Verwarmt de bril voor

2. Eierbergdoos

Telt resterende aantal eieren en meldt welke de oudste zijn

3. Sproei-installatie

Geef je tuin op afstand water

4. Luier

Geeft seintje als baby heeft gepoept

5. Prullenmand

Zet foto's van je afval op Facebook om aan te zetten tot minder weggooien

6. Luxaflex

Op afstand bedienbare raambekleding

7. Machinegeweer

Met internet verbonden app helpt je beter richten

8. Snoepdispenser

Voor honden, inclusief camera

9. Pacemaker

Stuurt je hartslag naar je dokter

10. Deurslot

App om leveranciers toe te laten tot je huis

Veiliheidstips IoT-toestellen

Wijzig altijd de standaardgebruiksnaam en wachtwoord van een apparaat als je dat installeert. Er gaan lijsten rond op internet met welke gebruiksnamen fabrikanten gebruiken (admin is populair).

Maak de SSID-naam van je modem/router onzichtbaar zodat die niet in lijst van beschikbare netwerken komt van smartphones, tablets, computers.

Check geregeld of er updates zijn van firmware, de software in een apparaat. Apparaten geven veel prijs over zichzelf op internet. Hackers kunnen zo checken of bekende kwetsbaarheden zijn verholpen.