INTERNET OF THINGS IS VAAK LEK

Een gehackt seksspeeltje, televisies die afluisterapparaten worden en een aanval via onbeveiligde security-camera's. Allemaal recente voorbeelden van het slecht beveiligde Internet of Things. Wat maakt het zo kwetsbaar? En wat doen we daaraan?

tekst **Marc Seijlhouwer MSc**

De We-Vibe, een trillend seksspeeltje, bleek vorig jaar eenvoudig te hacken. Onverlaten konden op afstand de trilintensiteit instellen en gebruiksgegevens achterhalen. Begin maart trof de maker een schikking met de gedupeerden voor in totaal 3,75 miljoen dollar. Daarmee is voor hen de kous voorlopig af, maar het legt een fundamenteel probleem bloot: dit soort 'slimme' apparaten hebben zelden of nooit adequate beveiliging. 'Deze devices worden vaak laconiek op de markt gebracht', vertelt dr. Mariëlle Stoelinga. Haar onderzoeksgroep bij de Universiteit Twente kreeg begin dit jaar een beurs om het Internet of Things (IoT) veiliger te maken.

Rampscenario

Jaya Baloo, Chief Information Security Officer bij KPN, herkent de lakse houding van bedrijven. 'Je kunt niet zomaar een dom apparaat aan het internet koppelen en het smart noemen. Toch gebeurt dat nu vaak. Dingen worden in elkaar geknutseld met onduidelijk geschreven software. Bedrijven denken daarbij nauwelijks over de toekomst van hun product, bijvoorbeeld als het gaat over het updaten van de software. Dat moet vaak gebeuren, maar niemand wil elke keer dat er een update nodig is een nieuwe koelkast of wasmachine kopen.'
Verder blijken veel van deze apparaten te hacken, of het nu gaat om beveiligingscamera's, thermostaten of glijbanen in waterparken. En één kwetsbaar apparaat lijkt misschien geen groot probleem, maar zo'n lek kan grote gevolgen hebben. 'Als je eenmaal een device overneemt, kun je een heel netwerk infiltreren', zegt Stoelinga. Via een thermostaat met een slechte beveiliging (bijvoorbeeld een standaardinlognaam en -wachtwoord) krijgen kwaadwillenden toegang tot andere apparaten die met hetzelfde wifinetwerk zijn verbonden, zoals computers en tv's. 'Aan de informatie op de thermostaat hebben hackers misschien niet zoveel, maar het geeft ze ook veel andere mogelijkheden.'
Intussen doemt in de zorg een mogelijk rampscenario op. Daar kan IoT veel betekenen voor patiënten, die langer thuis kunnen wonen door via *wearables* hun gezondheid te monitoren. Ook artsen zijn ermee geholpen: die kunnen snel en makkelijk patiëntgegevens uitlezen. 'Maar ziekenhuizen zijn notoir slecht beveiligd', aldus Stoelinga. 'Bovendien moeten gegevens vaak met spoed worden verkregen. Als een arts dan een lang wachtwoord moet invoeren, kan dat kostbare seconden vertraging veroorzaken.'

Keurmerk

De oplossing voor al die problemen hoeft niet ingewikkeld te zijn, denkt Baloo. 'Er zijn concrete, technisch eenvoudige stappen te zetten om de beveiliging enorm te verbeteren. Maar fabrikanten doen dat vaak niet, omdat ze snel en goedkoop een apparaat met internetverbinding uit willen brengen.' Stoelinga ziet het iets anders: 'Het veilig maken van een IoT-apparaat kan enorm complex zijn. Je moet bij elke stap nadenken: is dit absoluut veilig? Als dat bij één onderdeel niet het geval is, loopt het hele systeem risico.'
Eind vorig jaar stelde D66 een mogelijke oplossing voor: een keurmerk voor IoT-beveiliging. Experts vonden het een aardig initiatief, maar lastig uitvoerbaar; het lijkt bijvoorbeeld moeilijk om producten uit China aan die wetgeving te laten voldoen.
De consument moet in elk geval niet alleen verantwoordelijk zijn voor zijn eigen veiligheid. 'Mensen moeten zich daar geen zorgen over hoeven maken; het moet automatisch zijn geregeld door de leverancier', aldus Baloo. Stoelinga: 'Internetveiligheid is een onzichtbaar iets, dus mensen weten vaak niet of ze kwetsbaar zijn. Daarom moeten bedrijven verantwoordelijkheid nemen.'
Gezien de risico's die nu nog aan het Internet of Things kleven, is het de vraag of de consument er überhaupt aan moet beginnen. Stoelinga heeft haar bedenkingen: 'Ik zou wel twee keer nadenken voordat ik iets koop.' Baloo is positiever: 'De opkomst van IoT is een feit. We moeten die technologie ook gewoon benutten; hij kan veel opleveren. Maar privacy en veiligheid moeten fundamentele onderdelen worden van een smart apparaat, anders gaat het nooit werken.'

Hackers wisten de trilinstellingen van het seksspeeltje We-Vibe op afstand te veranderen en gebruikersgegevens te achterhalen.

foto **We-Vibe**