

Smart homes outsmarted

Eerder kwam in Product de opkomst van slimme apparaten (smart devices) al aan bod. Apparaten vol sensoren worden tegenwoordig steeds vaker verbonden met internet. Omdat die apparaten zich weer met elkaar kunnen verbinden, kan er gecommuniceerd worden. Van daar: 'smart'. Dit web van smart devices wordt het 'Internet of Things' genoemd. Is het wel slim om alles zonder meer smart te willen maken, zonder goed over het (technisch) ontwerp, de beveiliging en eventuele consequenties van datalekken na te denken?

De smart device is de hoeksteen van de smart home: een huis dat is voorzien van huishoudelijke producten waarmee metingen kunnen worden gedaan, allerlei functies en diensten in en om het huis kunnen worden aangestuurd, of die zelfs functies helemaal automatisch uitvoeren. Voorbeelden zijn luidsprekers die terugpraten en opdrachten uitvoeren (Google Home), slimme meterkasten die de netbeheerder in staat stellen het energieverbruik op afstand uit te lezen, slimme verlichting en alarmsystemen die zo geavanceerd zijn dat ze zelf herkennen wanneer er zich in huis verdachte situaties voordoen.

Virtueel leger van hackers

Dit zijn natuurlijk gunstige ontwikkelingen voor de consument. Sommige fabrikanten en ontwerpers beseffen echter onvoldoende dat 'iets met internet verbinden' betekent dat er in potentie een virtueel leger van hackers op de loer ligt. Inzicht hebben in wat de smart device waarneemt of registreert kan waardevol zijn. Je kunt er bijvoorbeeld iemands leefritme uit afleiden. Een recent voorbeeld is het lek bij een energieleverancier waardoor gegevens over energieverbruik en adresgegevens van 2 miljoen klanten met een 'slimme meter' in onbevoegde handen kwamen (op 13 september jl.).

Cyberaanval

Een hack kan tot gevolg hebben dat een apparaat wordt 'overgenomen' met het doel er een DDos-aanval mee uit te voeren. Het Amerikaanse bedrijf Dyn werd op 21 oktober jl. slachtoffer van zo'n aanval. Het bedrijf is een spin in het wereldwijde web. Het zet domeinnamen (bijvoorbeeld www.productmagazine.nl) om in een IP-adres (het nummer van de netwerkkaart van een computer op internet). Bij de DDos-aanval werd heel veel internetverkeer op één server of groep servers gericht, waardoor deze overbelastte(n). Het gevolg: veel grote websites lagen urenlang plat. Wat bleek? In dit geval werd gebruikt gemaakt van het Mirai-botnet, bestaande uit veel verschillende (naar schatting zo'n 100.000) slecht beveiligde huishoudelijke smart devices. De apparaten worden gehackt en tot 'slaaf' gemaakt van de aanval. Zo helpen ze mee aan de cyberaanval. Journalist Marc Hijink duidde het incident treffend: "smart is vaak dommer dan je denkt."

Persoonsgegevens

De data die worden verwerkt met apparaten in huis worden vaak als 'persoonsgegevens' aangemerkt. Dit betekent dat de beveiliging van dat soort data moet voldoen aan de strenge privacywetgeving. Dit is belangrijk om cyberaanvallen en andere beveiligingsincidenten te voorkomen. Sinds 1 januari 2016 is dit extra belangrijk, omdat datalekken waarbij persoonsgegevens (waarschijnlijk) onbevoegd zijn ingezien of



gestolen, moeten worden gemeld aan de Autoriteit Persoonsgegevens en soms ook aan de 'eigenaren' van de data. Overtredingen kunnen tot boetes leiden.

Nieuwe eisen

En er komen nog meer regels aan. Producenten en ontwerpers van smart devices doen er goed aan zich alvast voor te bereiden op de eisen van de nieuwe Europese privacywet. Die wet eist namelijk dat bij het gebruik van nieuwe technologieën, eerst een *privacy impact assessment* wordt uitgevoerd – vooraf kijken dus naar de gevolgen voor de bescherming van persoonsgegevens, waar beveiliging een belangrijk onderdeel van is. Ook verplicht wordt het vooraf nadenken over het (technisch) ontwerp van een product vanuit het oogpunt van privacy, ook wel *privacy-by-design* genoemd. Producten smart maken is leuk, maar vraag jezelf van tevoren af of de beveiliging van data aan de almaar strenger wordende eisen kan voldoen!



Jurre Reus is advocaat
privacyrecht bij CMS
Derks Star Busmann N.V. te Utrecht.
E-mail: jurre.reus@cms-dsb.com