WWW.MINDYOURSTEP.INFO

Hacken via Internet of Things

van het hacken van je slimme thermostaat tot erger

De vraag

Ontzettend handig, een seintje krijgen wanneer je oma de hele dag nog geen thee heeft gezet, maar het brengt ook gevaren met zich mee. Het Internet of Things biedt ons zogenoemde 'slimme' apparaten. Met slimme apparaten wordt bedoeld dat het om apparaten gaat die, vaak via een app, verbonden zijn met het internet. En daardoor zelfs met elkaar kunnen communiceren.
We horen steeds vaker over grote aanvallen op computers.
Maar het hacken van al onze andere slimme apparaten in huis is misschien nog wel gemakkelijker en zeker niet minder schadelijk. Apps om je televisie aan te sturen, je wasmachine aan te zetten, je verlichting te bedienen en beveiligingscamera's te checken... er is steeds meer mogelijk. Deze apps werken samen met meer en meer apparaten in het huishouden. Maar wat als door een hack je internet uitvalt en daarmee je kluis op slot blijft, of je de verwarming niet meer aankrijgt? Of erger, dat een virus alles overneemt? Om het al helemaal maar niet te hebben over maatschappelijke uitdagingen door het hacken via slimme apparaten, zoals het op afstand laten crashen van vliegtuigen, het overnemen van auto's, het saboteren van medische apparaten en het laten uitvallen van verkeerslichten. Via internetsites kun je tegenwoordig erg gemakkelijk zoeken naar de onbeveiligde beelden van beveiligingscamera's bij mensen thuis, en hackers dus ook. Erger nog, zonder dat je daar expliciet toestemming voor geeft, kunnen hackers bij je thuis meekijken. Terwijl die camera's aanvankelijk voor beveiliging bedoeld waren... Hoe maak je eigenlijk veilig gebruik van deze nieuwe, slimme, online apparaten?

De uitdaging

Internet of Things betekent dat verschillende apparaten met elkaar zijn verbonden via het internet. De toegenomen risico's die met het Internet of Things zijn ontstaan zijn onder te verdelen in drie categorieën; softwarebesturing, tussenverbindingen en autonomie. Zoals je weet besturen we steeds meer met software. Het gevolg daarvan is dat er ook steeds meer te hacken valt. Zeker apparaten als onderdeel van het Internet of Things behoren bij een kwetsbare categorie, omdat je nu eenmaal niet regelmatig je koelkast of thermostaat een beveiligingsupdate geeft. Juist deze apparaten, die ook nog eens verbonden zijn met je volledige netwerk thuis, maken hackaanvallen gemakkelijker. Via het ene slimme apparaat kan een ander slim apparaat eenvoudig worden aangevallen.
Computersystemen worden daarnaast ook steeds meer autonoom. Zoals bijvoorbeeld de matrixborden boven de snelweg die een aangepast snelheidslimiet tonen wanneer camera's zelf detecteren dat er file staat. Hoe meer apparaten menselijk handelen gaan overnemen, des te groter de schade bij de inbreuk op een systeem.

De oplossing

De enige échte oplossing is simpelweg het niet gebruiken van slimme apparaten binnen je netwerk. Kies je hier toch voor dan kunnen de volgende tips je helpen zo veilig mogelijk gebruik te maken van het Internet of Things:

- Denk nog één keer na of je echt een 'videobeltelefoon' voor je hond nodig hebt, om vanuit je werk 'Spike' in de woonkamer te kunnen zien liggen, voordat je deze met internet verbindt. Géén verbinding is namelijk het meest veilig.
- Als gebruiker van slimme apparaten op je online netwerk kun je er niet blindelings op vertrouwen dat de producent van het apparaat zich druk heeft gemaakt over de bescherming van je gegevens. Het is goed om erover na te denken of het verstandig is bepaalde functies via een apparaat uit te voeren dat verbonden is aan het internet.
- Sluit slimme apparaten aan op een apart WiFi-netwerk zodat zij met elkaar kunnen communiceren, zonder dat mogelijke hackers via deze apparaten in je thuisnetwerk kunnen komen.
- Sta toegang tot je slimme apparaten alleen toe door voldoende complexe wachtwoorden, het liefst via een dubbele authenticatie waarbij je zowel een wachtwoord gebruikt dat je kent, als een code die je hebt, bijvoorbeeld ontvangen via een sms.
- Houd, net zoals je computer en je netwerk, ook je slimme apparaten up-to-date door op updates te blijven controleren en deze te installeren.
- Controleer of je slimme apparaat automatisch verbinding maakt met andere apparaten of internetdiensten. Dit is niet aan te raden.
- Gebruik een Internet of Things-scanner om te detecteren of er slimme apparaten op je thuisnetwerk zijn verbonden die gehackt of slecht beveiligd zijn. Zo ja, wijzig dan direct je inlognamen en wachtwoorden.
- Maak een 'whitelist' van de slimme apparaten die je toegang wilt verlenen tot je thuisnetwerk. Alleen apparaten die op deze lijst staan kunnen verbinding maken met je thuisnetwerk. Dit voorkomt dat vreemde systemen toegang krijgen tot je slimme apparaten. Dit kun je doen door zogenoemde 'Machine Access Code'-adressen van je slimme apparaten in je router of accespoint in te voeren.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak. Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.