# Cyberdijk en het Internet of Things

**aanleiding**

De overheid wil consumenten voorlichten zodat zij zich beter kunnen weren tegen misbruik van Internet-of-Things (IoT) apparaten. Een voorlichting is een eerste goede stap maar er zijn verstrekkende maatregelen nodig om ons land te beschermen tegen een IoT-Cyber-Tsunami.

Apparaten, auto's speelgoed en andere 'gadgets' zijn steeds vaker verbonden met het internet. De overheid wil consumenten nu helpen om zich beter te weren tegen misbruik van dit soort Internet-of-Things (IoT) apparaten. Een goed initiatief, maar in plaats van consumentenvoorlichting als puntoplossing, pleit ik als IoT-specialist voor een multidisciplinaire aanpak om grip te krijgen op dit groeiende potentiele probleem.

De consument 'moet willen', de leverancier 'zal moeten' en van overheden wordt vooral duidelijkheid verwacht hoe zo'n Cyber-Delta-plan eruit zou moeten zien.

**de consument**

Zonder concrete aanleiding zal een fris postbus 51 spotje geen effect hebben, of hebben u en uw vrienden thuis wel een noodpakket op zolder liggen met een zaklantaarn, warme deken, watervoorraad en een radio met volle batterijen? Van intrinsiek gemotiveerde consumenten kunnen we niet meer verwachten dan het ophangen van een gifwijzer en neerzetten van jodiumtabletten in de meterkast.
We kunnen het er lang of kort over hebben; de consument bepaalt zelf of hij een slim-product wil kopen. De trend van acceptatie van slimme producten zet snel door; deze beweging is niet tegen te houden.
De consument is geïnteresseerd in slimme ‘gadgets’; een lage prijs en een goed merk met een hoge ‘bling en show factor’. Een gemiddelde(!) consument heeft primair intrinsiek geen interesse in cyberbeveiliging en andere productkwaliteitsmerken zoals CE-markering, kies-bewust logo’s, verstandige fair-trade en CO2-neutrale diensten. Dit zijn pas zaken waarin hoogstens in tweede instantie over wordt nagedacht. Er moet zich wel een erg grote ramp voordoen voordat de gemiddelde consument in Nederland dit primaire risico op het netvlies heeft staan en in beweging komt.

**de leveranciers en importeurs**

Deze partijen hebben maar interesse in twee zaken: zo goedkoop mogelijk produceren en zo snel mogelijk aan dezelfde klant weer een nieuwe verbeterde productvariant te verkopen. Instanties als de consumentenbond pleiten al langer voor de verantwoordelijkheid die leveranciers/importeurs moeten nemen.
De wetgever moet duidelijkheid geven en ervoor zorgen dat deze partijen verplicht zijn gedurende de ‘redelijk te verwachtte gebruiksduur’ van een product te voorkomen dat het product schade kan veroorzaken.
Dit omvat dus niet alleen gebruiksschade gedurende de 2-jaars gararantie-termijn, maar ook gevolgschade door bijvoorbeeld misbruik en de mogelijkheid als cyberaanval stepping stone te fungeren.
Hierin moet vanuit mijn oogpunt veel harder op gestuurd worden. Geen ronde tafels, maar duidelijke systeemsoftware-update-zorgplicht en verplichte terugroepacties als noodmiddel

**operators en internet Service providers**

Apparaten zijn niet uit zichtzelf aan internet gekoppeld. Internet service providers en operators bieden aanvullende diensten zoals spam-detectie en optionele content filtering. In tegenstelling tot mensen die wel honderden websites dagelijks bezoeken, bouwen slimme apparaten niet zo maar verbindingen op naar allerlei systemen en servers.
Of het nu om slimme luidsprekers, tandenborstels, deuropeners of zonnepaneel-omvormers gaat; deze IoT-apparaten communiceren aan de 'internet-zijde' maar met één of twee beheerplatformen en enkele standaard internetdiensten zoals domein-naam en tijd-servers.
Koppelingen van verschillende IoT-appraten gaan op gecontroleerde gestandaardiseerde methoden via server-koppelingen bij leveranciers.

Afgezien van bovengemiddelde gebruikers die een losse router en firewall heeft; gebruikt de gemiddelde consument een internet router van een internet serviceprovider. Waarom kunnen daarin niet standaard open source tools verwerkt worden zoals de (bij specialisten bekende) nmap-tool om afwijkend gedrag van IoT-devices te detecteren en signaleren? Zijn internet service providers bereid om dit gezamenlijke probleem onder controle te krijgen? Indien niet, waarom dan wel implementatie van centrale mitigerende algoritmes om de eigen mail-servers te beschemen tegen spam, maar waarom niet IoT-stepping stone detectie vanuit de internetmodems bij klanten?

**wat nu?**

De vraag is wat wij als samenleving willen doen: wachten op een frisse publiekscampagne of daadwerkelijk de eerste spade in de grond zetten om een IoT-Cyber-Deltaplan te bouwen .

Bouwt u multidisciplinair mee?

Robert Heerekop

Robert Heerekop is zelfstandig IoT-specialist en heeft de afgelopen 15 jaar, in verschillende landen, talloze organisaties geholpen met het vormen van de juiste Internet of Things(IoT) strategie en vervolgens realiseren van grootschalige B2B/B2C IoT-projecten. Met zijn gespecialiseerde technische kennis en praktische ervaring ondersteunt hij zowel het MKB, multinationals, overheden en investeerders. Daarnaast publiceert hij regelmatig over IoT en geeft hij hands-on kennisdeel-workshops voor kids&managers op basis van het slimste zelfbouw IoT-vogelhuisje van Nederland.