ICT CENTRAAL IN NEDERLAND

‘RESPONS TEAM MOET GEBREKKIGE IOT-BEVEILIGING AANPAKKEN’

Medio oktober publiceerden het Britse ministerie van Digitaal, Cultuur, Media en Sport (DCMS) en het Nationaal Cyber Security Centrum (NCSC) de zogenaamde Code of Practice. Dit zijn gedragsregels rondom de beveiliging van apparaten die zijn verbonden met het internet (IoT-apparaten). Engeland heeft daarmee de wereldwijde primeur om als eerste land ter wereld fabrikanten van IoT-apparaten op te roepen om apparaten zo goed mogelijk te beveiligen. Hoewel de code vrijwillig is, lijkt dit een goede eerste stap om de wildgroei in de strijd tegen onveilige situaties. De vraag is alleen of het opleggen van vrijwillige gedragsregels wel zin heeft?

Tekst Mary-Jo de Leeuw

De opmars van IoT-apparaten lijkt zijn weerga niet te kennen: van watersproeiers in de tuin tot aan barbecues, alles en iedereen met elkaar verbonden lijkt het credo anno 2018. En hoewel de apparaten steeds slimmer lijken te worden, gedraagt de gemiddelde gebruiker zich helaas nog steeds onnozel. Want zonder het nemen van de juiste stappen om IoT-apparaten veilig te kunnen gebruiken, vormen zowel de gebruiker als de data die vrij toegankelijk is, een groot risico.

Aankoopboycot

In navolging van de Britse gedragsregels, zijn er ook diverse initiatieven van Nederlandse bodem die – volgens de afzonderlijke initiatiefnemers – als doel hebben om ‘slimme’ apparaten beter te beveiligen. De Cyber Security Raad (CSR), die de overheid gevraagd en ongevraagd adviseert, liet bijvoorbeeld aan het begin van het jaar weten dat “veel IoT-producten nu nog onveilig zijn omdat er nauwelijks regelgeving voor bestaat”. Ik betwijfel of het ontbreken van wet- en regelgeving daadwerkelijk de oorzaak is van onveilige producten. Als consument kun je bijvoorbeeld ook een stevig stempel drukken door over te gaan op een aankoopboycot: daar heb je geen wet- of regelgeving voor nodig. De CSR gaf daarnaast aan dat “het kabinet zo snel mogelijk met Europese landen om de tafel moet om te komen tot maatregelen tegen veilige apparaten en deze van de Europese markt moet weren”.

Waarom zou je op voorhand al apparaten weren van de markt nog voordat je de problematiek hebt doorgrond? Uit eigen ervaring weet ik dat je vrij eenvoudig tot in het hart van een product dat is verbonden met het internet kunt komen, door bijvoorbeeld gebruik te maken van een onveilig netwerk. Het verbieden van een apparaat lost in dat geval dus niets op en dat geldt ook voor het verplicht stellen van keurmerken om de veiligheid van slimme apparatuur te kunnen waarborgen. Want wat heb je aan een keurmerk indien het netwerk de zwakste schakel is?

Maar er zijn meer oplossingen van Nederlandse makelij: Agentschap Telecom geeft aan dat “de veiligheid met een aantal simpele stappen moeten worden verbeterd. Zo zou het de fabrikanten verboden moeten worden hun apparaten met standaardwachtwoorden uit te rusten (denk: 0000 of 1234).”
Marie-José Bonthuis, IT-jurist bij IT’s Privacy, geeft aan dat deze oplossing iets genuanceerder ligt “omdat het qua beveiliging een risico-inschatting is die afhangt van aard en omvang van de gegevens (hoe gevoeliger, hoe meer maatregelen). De richtsnoeren ‘beveiligen van persoonsgegevens’ van de Autoriteit Persoonsgegevens (AP), geeft bijvoorbeeld aan dat een gebruikersnaam en wachtwoord vanaf risicoklasse 1 al wordt aanbevolen.“

Probleemeigenaar gezocht

De grote vraag is dus waar en door wie de minimumeisen moeten worden vastgelegd? Agentschap Telecom pleit “voor een samenwerking tussen industrieën en de overheid aangezien Europese cyberwetgeving nog jaren kan duren.” Dat klinkt allemaal plausibel en sympathiek maar de grote gemene deler blijft dat er vooralsnog geen enkele partij is, die als probleemeigenaar opstaat, ook Agentschap Telecom niet. En wat doen we in tussentijd?

D66 denkt het antwoord gevonden te hebben in een Nederlands keurmerk voor de beveiliging van IoT-apparaten. Dat keurmerk moet er zijn, blijkens het initiatiefvoorstel dat in november 2016 naar de Tweede Kamer werd gestuurd, totdat er op Europees niveau regels worden opgesteld. Uit de praktijk moet nog wel blijken wat uiteindelijk sneller is: het in het leven roepen van een keurmerk (inclusief normen- en toetsingskader) en bijhorend (privacy-proof) certificaat, dan wel het introduceren van nieuwe (Europese) regels. Bonthuis: “Het zou mooi zijn als er een privacy-proof-certificaat afgegeven kan worden, hetgeen natuurlijk nooit 100 procent garanties kan geven.”
D66 geeft daarnaast ook aan dat er duidelijke handleidingen moeten komen voor apparatuur. Mijn vraag aan u, lezer van dit stuk, of iemand in uw omgeving kunt opnoemen die handleidingen leest voor het in gebruik nemen van nieuwe apparatuur? Ik niet namelijk!

One stop shop

Kunnen we iets met de gedragsregels uit Engeland misschien? Geldt hier ook niet “beter goed gejat dan zelf slecht bedacht”? De Engelse richtlijnen, die overigens net zo vrijblijvend zijn als de aanbevelingen van de AP, geven handvatten hoe het voor gebruikers op een eenvoudige manier zou moeten lukken om persoonlijke data te verwijderen en geeft suggesties hoe software up-to-date kan blijven. Het is daarmee in ieder geval een goede eerste stap in de richting omdat het daadwerkelijk leidt tot actie. Want ondanks dat het vrijblijvend is, is er een aantal fabrikanten dat de gedragsregels omarmt en andere fabrikanten oproept hetzelfde te doen. Engeland toont daarmee aan dat ze de wildgroei aan slimme apparaten in ieder geval serieus nemen en geeft daarnaast een duidelijk signaal af: zij hebben een probleemeigenaar benoemd! Dus één organisatie die bereid is alle partijen bij elkaar te krijgen en te kijken naar gezamenlijke oplossingen om de wereld digitaal veiliger te krijgen. De spreekwoordelijke one stop shop waar alles en iedereen samenkomt om zo de mouwen op te stropen.

Mary-Jo de Leeuw is per 1 december aangesteld als Director Cybersecurity Advocacy: Europa, Midden Oosten en Afrika in Londen.

IoTCERT

Wat dat betreft zou ik pleiten voor een Nationaal Computer Emergency Respons Team (CERT), maar dan specifiek eentje die gespecialiseerd is in slimme apparaten. Dus een zogenaamde IoTCERT dat in geval van beveiligingsincidenten snel kan handelen en zo de schade kan beperken. Een one stop shop met een register voor onveilige apparaten, met handelingsperspectieven voor gebruikers, met een waarschuwingssysteem waarbij je als consument bijvoorbeeld een appje krijgt indien een volgend IoT-botnet op volle kracht bezig is. Een plek waar je als consument, fabrikant, toezichthouder of consumentenorganisatie terecht kunt met al je vragen of gewoon melding kan maken van een onveilige IoT-situatie. Want die bestaat nu simpelweg niet! Geloof me, ik heb bij een aantal organisaties meldingen willen doen van kwetsbaarheden, maar van de Agentschap Telecom tot aan de Consumentenbond en van de Voedsel en Warenautoriteit tot aan het ministerie van Economische Zaken en Klimaat, ze waren er allemaal “niet van”. Sterker nog: op de vraag “wie er wel van was” wezen ze allemaal naar elkaar. De hoogste dus tijd om de handen ineen te slaan, om een probleemeigenaar te benoemen die de Nederlandse IoT-kar gaat trekken en wat mij betreft dus ook de hoogste tijd voor een... IoTCERT! «