Gehackte IoT-apparaten en aansprakelijkheid

Door de ogen van een advocaat: wie heeft schuld?

Gaaf he, dat Internet of Things (IoT)? Met je mobieltje alvast de verwarming thuis aanzetten en meer van dat soort handige dingen. Er zijn echter ook gevaren. Zo werd bij een casino via het aquarium in de lobby de hele database (10 GB) aan klanteninformatie geupload naar hackers: het 'internet connected aquarium' was uitgerust met sensoren die verbonden waren met een pc die temperatuur, voedsel en waterhygiëne regelde.

Stel nou dat dat aquarium in de lobby van een kerncentrale had gestaan ... hmm. Een van de reactoren beleeft een meltdown. Stralingsslachtoffers melden zich bij de kerncentrale. Hypothetische situatie: de kerncentrale is geen eigendom van de overheid met onmetelijk diepe zakken en de verzekering dekt dit niet. De kerncentrale zou failliet gaan als ze dit allemaal moet ophoesten, maar heeft inmiddels de oorzaak achterhaald. De kerncentrale wijst naar de aquariumproducent. We gaan even uit van een wereldwijd leverende fabrikant met veel geld en niet van de aquariummaker op de hoek. Is die aansprakelijk op grond van productaansprakelijkheid?

Fictieve rechtszaak IoT-fabrikant

Over rechtszaken rondom gehackte IoT-apparaten is mij niets bekend. Stel dat zo'n rechtszaak rondom het gehackte aquarium in Nederland plaats zou vinden, hoe zou de rechter dan oordelen? Een stralingsslachtoffer eist een schadevergoeding. Laten we er vanuit gaan dat de basis voor de rechtszaak zou zijn: productaansprakelijkheid wegens een gebrekkig product. De wet zegt – kort samengevat – dat een product gebrekkig is: *"indien het niet de veiligheid biedt die men daarvan mag verwachten, vanuit het redelijkerwijs te verwachten gebruik."*

Internet connected aquarium gebrekkig product?

Je mag er vanuit gaan dat een percentage mensen dom of digibeet of roekeloos of alles tegelijk is en het aquarium aan zijn netwerk hangt zonder dit af te scheiden (hetgeen redelijk eenvoudig is voor de gemiddelde lezer van dit blad maar ik zie het de meeste mensen nog niet doen). En af en toe staat zo'n aquarium dus niet in de woonkamer maar in een kerncentrale. Waar het aquarium wordt geïnstalleerd door de secretaresse met passie voor

tropische vissen en niet door de netwerkbeheerder (die weet van niets). Het besturingssysteem is een gemodde Android 5 in plaats van de laatste kale Androidversie, zodat de visliefhebber is overgeleverd aan de fabrikant en die brengt geen patches uit. Je zou kunnen zeggen: gebrekkig product, je moet er als fabrikant maar voor zorgen dat toch in ieder geval de laatste kale Androidversie met auto-update er op staat of dat je patches van je eigen gemodde versie uitbrengt zolang het apparaat dat trekt. Zijn we er dan? Nee, er bestaat zoiets als 'eigen schuld': *"De aansprakelijkheid van de producent wordt verminderd of opgeheven rekening houdende met alle omstandigheden, indien de schade is veroorzaakt zowel door een gebrek in het product als door schuld van de benadeelde of een persoon voor wie de benadeelde aansprakelijk is"*. Daar is echter in dit geval geen sprake van: de stralingsslachtoffers hebben het aquarium niet aangesloten. Je kunt natuurlijk roepen: ja maar de hackers hebben het toch gedaan? Het wetsartikel over productaansprakelijkheid zegt echter dat de aansprakelijkheid van de producent niet minder wordt, als de schade niet alleen is veroorzaakt door een gebrek in het product maar ook door een gedraging van een derde (de hackers en de visminnende secretaresse).

> "als u onderstaande lap tekst niet uitvoert, wordt u mogelijk gehackt"

Gevaarzetting?

Naast de productaansprakelijkheid is er nog dit: als je een gevaarlijke situatie veroorzaakt, kan er sprake zijn van een 'onrechtmatige daad' wegens 'gevaarzetting'. In 1961 liet een Coca-Colabezorger bij café De Munt in Amsterdam het kelderluik open staan, waarna een nietsvermoedende bezoeker naar beneden tuimelde. De hoogste rechter van Nederland kwam toen met de zogenoemde 'Kelderluikcriteria', die nog steeds worden gebruikt:

- Hoe waarschijnlijk is de niet-inachtneming van de vereiste oplettendheid en voorzichtigheid?
- Hoe groot is de kans dat daaruit ongevallen ontstaan?
- Hoe ernstig kunnen de gevolgen zijn?
- Hoe bezwaarlijk (kosten/werk) zijn de veiligheidsmaatregelen?

Passen we dit toe op onze aquariumcasus, dan krijgen we de volgende beantwoording. De kans van niet-inachtneming van de vereiste oplettendheid en voorzichtigheid is redelijk groot: wie zo'n aquarium bestelt (in onze casus de visminnende secretaresse) is niet per definitie een wizzkid maar in de eerste plaats een aquariumliefhebber, dus ga er maar van uit dat de meerderheid niet weet hoe je het aquarium scheidt van de rest van het netwerk. Zelfs niet met een gebruiksaanwijzing uit een consumentencomputerblad. Waarschuwen (een sticker met "als u onderstaande lap tekst niet uitvoert, wordt u mogelijk gehackt") is niet steeds voldoende.

Dodelijke jetblast

Een latere "kelderluikzaak" ging over een vliegtuigspotter die na een jetblast met haar hoofd de stoep raakte en daardoor overleed (zie YouTube voor video's met deze idioten ...). Ging vliegveld Sint-Maarten vrijuit, omdat het een waarschuwingsbord had geplaatst: *"Pas op! Niet te dichtbij komen, dodelijke jetblast!"*. Nee, dat was niet voldoende. Bekend was dat elke dag thrillseekers (zo kun je ze ook noemen ...) zich aan het hek vasthielden als er een vliegtuig overkwam, wachtend op die jetblast. Kernvraag was volgens de Hoge Raad *"of te verwachten valt dat deze waarschuwing zal leiden tot een handelen of nalaten waardoor dit gevaar wordt vermeden"*. Nou, nee dus.

Terug naar het aquarium en het door de secretaresse ondanks waarschuwing niet nachtenlang puzzelen op het scheiden van het netwerk (of bellen van de netwerkbeheerder). De kans dat uit die houding een ongeval ontstaat is, als het aquarium in een organisatie staat met gevaarlijke apparatuur, redelijk groot.

Voorzorgsmaatregelen mogelijk?

Maar, zijn er dan voorzorgsmaatregelen *mogelijk*? Ik pas hierop dan de 'Kelderluikcriteria' toe. Ik hou het voor mogelijk dat een rechter bij een Android 5-aquarium de kans op een hack en dus een ongeval substantieel acht als dat aquarium zich op een risicolocatie als een kerncentrale bevindt. De gevolgen kunnen fors zijn: ernstig letsel of overlijden. Extra maatregelen bij de productie om te voorkomen dat het aquarium niet wordt gehackt terwijl er op de installatielocatie niets aan het netwerk verandert, wordt een lastige. Wie het weet, mag het zeggen. Volgens computerworld is het uit gebrek aan hardwareresources en uit economisch oogpunt niet te doen om IoT-endpoints to the max te beveiligen, en moet je dat op netwerkniveau regelen. Als de oplossing echter voor de desbetreffende IoT-fabrikant voor de hand ligt en de kosten in verhouding zijn, zou de aquariumproducent ook volgens de Kelderluikcriteria niet geheel vrijuit gaan.

Eigen schuld?

Ook hier geldt echter weer de verdeling op grond van "eigen schuld": de kerncentrale die wordt aangesproken door een slachtoffer en op haar beurt de aquariumfabrikant aanspreekt, zal een deel van de schade zelf moeten dragen als er een waarschuwing op de doos zat en een handleiding om het netwerk te scheiden. Tot dusver ontbreekt echter een dergelijke waarschuwing en handleiding bij de meeste IoT-apparaten.

Hub Dohmen, advocaat

Dohmen advocaten is onder één dak gevestigd met octrooi-/modellen-/merkenbureau Griebling.
Meer opiniestukken van Mr. Dohmen staan op www.engineersonline.nl.

e: info@dohmenadvocaten.nl
i: www.dohmenadvocaten.nl