ELEKTOR ETHICS

Een grote uitdaging

veilige producten in het IoT-tijdperk

Tessel Renzenbrink (Nederland)

Veiligheidsgordels, airbags, kreukelzones, maximumsnelheid en beperking van alcohol in het verkeer. Decennia van technologische innovatie en regelgeving hebben auto's steeds veiliger gemaakt. Hetzelfde geldt voor andere consumentenproducten. We kopen het zonder aarzelen in de winkel en vertrouwen erop dat het veilig is. Maar met de opkomst van het Internet of Things wordt een doos van Pandora geopend. Nu steeds meer producten worden voorzien van elektronica, software en netwerkverbindingen, worden ook nieuwe gevaren en risico's geïntroduceerd. De voorbeelden zijn legio: van genetwerkt speelgoed waarmee kinderen bespied kunnen worden tot auto's waarvan de besturing op afstand kan worden overgenomen.

Professor Ross Anderson en zijn collega's hebben onderzocht welke maatregelen er nodig zijn om traditionele productveiligheid te integreren met de komst van het IoT. Ze deden dit in opdracht van de Europese Commissie. De EU werkt aan nieuwe wetgeving om ook in de toekomst de veiligheid van producten te kunnen waarborgen. Ze vroegen Anderson om in kaart te brengen wat daar voor nodig is. Anderson, professor in Security Engineering, deed dat samen met zijn collega's Eirann Leverett, Senior Risk Researcher, en Richard Clayton, Security Researcher, allen verbonden aan de Cambridge Universiteit. Het rapport met hun bevindingen werd in 2017 gepubliceerd [1].

Trilemma

We hebben nog een lange weg te gaan, concluderen Anderson en zijn collega's. De kern van het probleem is dat de manier waarop de veiligheid van producten wordt gerealiseerd, wezenlijk verschilt van die van digitale technologieën. Producten worden getest en geïnspecteerd voordat ze op de markt worden gebracht en ontvangen dan een veiligheidscertificaat. Als er significante wijzigingen worden aangebracht in het product moet het opnieuw gecertificeerd worden. De veiligheid van software, daarentegen, is juist gebaat bij veranderingen. Software wordt continu gemonitord en regelmatig bijgewerkt met patches en updates. In een presentatie over het onderzoek, op het Chaos Communication Congress (CCC) in december 2019, gaat Anderson hier dieper op in [2]. Hij noemt dit het trilemma van IoT-producten. Als je vasthoudt aan voor-de-markt certificering, kan je je software niet bijwerken en is je product onveilig. Als je de software bijwerkt verlies je je certificering. Maar als je certificering en updates zou combineren – en dus na elke software-update het certificeringsproces opnieuw moet doorlopen – dan rijzen de kosten de pan uit.

Levensduur en complexiteit

Traditionele producten en digitale diensten hebben elk zo hun eigenaardigheden die nu bij elkaar komen. En we moeten er voor oppassen dat we niet het slechtste van beide werelden overnemen, zegt Anderson. Vergelijk bijvoorbeeld telefoons en auto's. De firmware en het beheersysteem van telefoons worden gemiddeld zo'n 3 jaar ondersteund. Nadat de ondersteuning eindigt, wordt de telefoon onveilig omdat kwetsbaarheden in de software niet meer worden gepatcht. Mensen zijn genoodzaakt om telefoons te vervangen ondanks dat de hardware vaak nog prima in orde is. We moeten voorkomen dat die werkwijze in de toekomst ook in de auto-industrie wordt toegepast, zegt Anderson.
Maar behoud van levensduur brengt nieuwe uitdagingen met zich mee. Stel dat een fabrikant verplicht wordt een bepaald model auto tenminste 20 jaar te ondersteunen. Een softwareengineer die vandaag een programma schrijft voor een auto die in 2022 op de markt komt, moet er dan rekening mee houden dat de code tot 2042 mee moet gaan.
Een andere uitdaging is complexiteit. Het idee van het IoT is dat apparaten met elkaar communiceren en zelfstandig tot actie kunnen overgaan. Zelfrijdende auto's die informatie uitwisselen met de weg-infrastructuur en koelkasten die zelf boodschappen bestellen. Vanuit het veiligheidsperspectief betekent dat dat het eigenlijk niet meer voldoende is om apparaten individueel te testen. Er moet ook gekeken worden naar de risico's die ontstaan door interactie met andere apparaten.

Aanbevelingen

Productveiligheid in het IoT-tijdperk is een complexe opgave die niet van vandaag op morgen kan worden gerealiseerd. In hun rapport voor de Europese Commissie doen de drie onderzoekers enkele aanbevelingen. De belangrijkste is het oprichten van een nieuw Europees instituut: de *European Safety and Security Engineering Agency* (ESSEA). ESSEA moet de technische kennis in huis hebben om onder andere standaarden te ontwikkelen en beleidsmakers te informeren. Daarnaast moet het onderdak bieden aan een centrale database waar informatie wordt verzameld over software-kwetsbaarheden, falende componenten en fouten bij systeemintegratie. Op dit

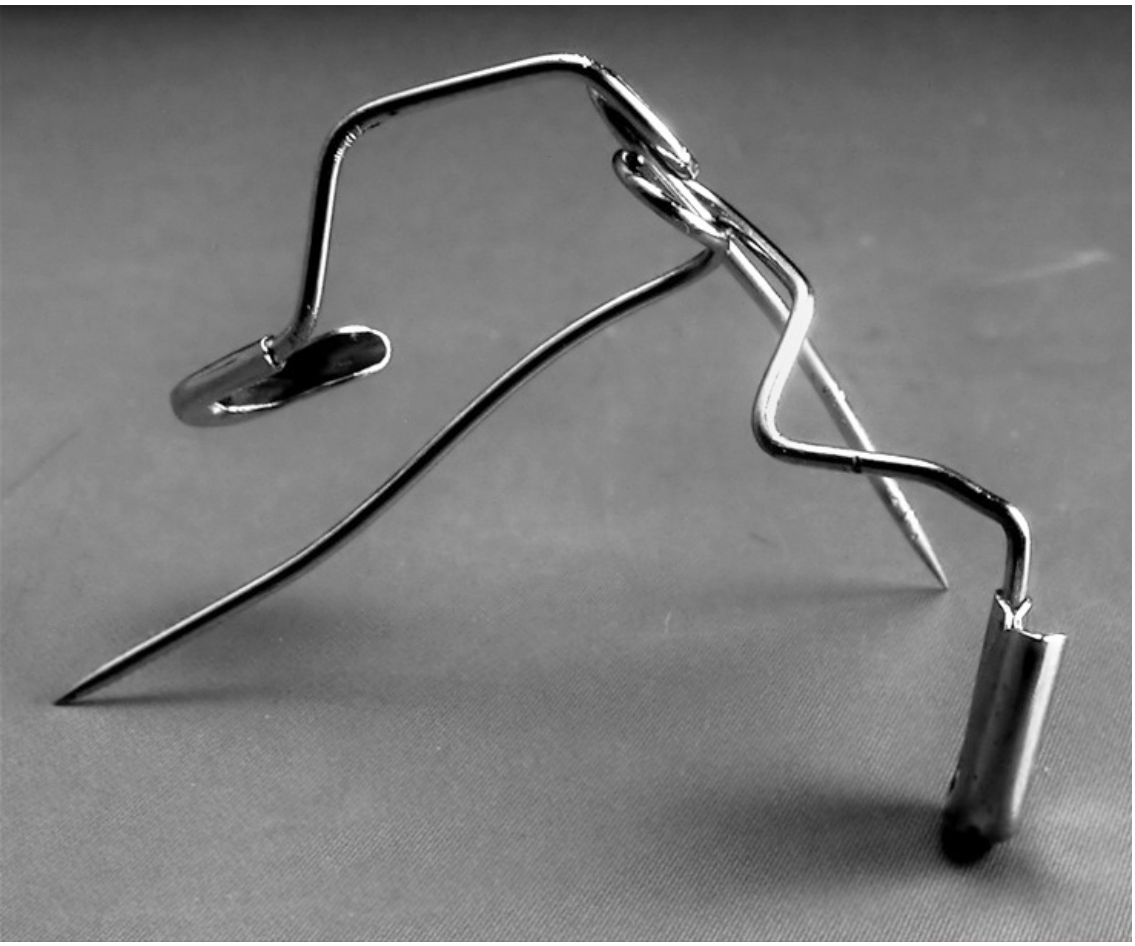

Foto: Safety door Gabor Kiss. CC BY 2.0 https://www.flickr.com/photos/-nevi-/5404057758/

moment wordt dat soort data bij verschillende instituten en bedrijven bewaard. Wanneer de data bij elkaar wordt gebracht kan iedereen van elkaar leren en worden niet steeds dezelfde fouten gemaakt.

Een andere aanbeveling is dat fabrikanten die netwerkcapaciteiten toevoegen aan hun producten, moeten garanderen dat het mogelijk is om software-updates uit te voeren.

Daarnaast zou de EU een aantal bestaande richtlijnen moeten aanpassen om de nieuwe ontwikkelingen te accommoderen. De richtlijn voor productaansprakelijkheid moet bijvoorbeeld worden uitgebreid zodat digitale diensten er ook onder vallen. Onder de huidige richtlijn kan een fabrikant van navigatieapparatuur wel aansprakelijk worden gesteld voor fouten, maar kunnen de makers van Google Maps dat niet.

De EU als verdedigingslinie tegen een Internet of Trash

Het is lastig gebleken om de aanbevelingen doorgevoerd te krijgen, zegt Anderson tijdens de presentatie op CCC. Er zijn veel verschillende spelers mee gemoeid die allemaal andere belangen hebben. Zo lobbyden Google en Facebook tegen het voorstel om digitale diensten onder de bestaande aansprakelijkheidsregels te laten vallen. Maar er zijn sinds het uitkomen van het rapport ook een aantal dingen bereikt. Zo is Richtlijn 2019/771 aangenomen waarin is vastgelegd dat consumenten van producten met digitale elementen het recht hebben op tenminste twee jaar updates, of langer als dat redelijkerwijs verwacht kan worden. Dat laatste betekent dat goederen die geacht worden langer mee te gaan (zoals wasmachines) ook langer updates moeten krijgen. De enorme taak die Anderson, Leverett en Clayton beschrijven om de veiligheid van IoT producten in de toekomst te waarborgen, staat in schril contrast met de trage besluitvorming van de Europese Unie. Toch is hun hoop gevestigd op de EU want, zo schrijven ze in een gerelateerd wetenschappelijk paper: “De EU is al ’s werelds voornaamste regelgever op het gebied van privacy. Dat komt omdat Washington daar niet in is geïnteresseerd en niemand anders groot genoeg is om voldoende gewicht in de schaal te leggen. De EU moet zich tot doel stellen om ook de voornaamste regelgever op het gebied van veiligheid te worden – of het risico lopen dat de huidige veiligheidsdoelstellingen in gevaar worden gebracht” [3].

200066-01

Links en literatuur

[1] Eireann Leverett, Richard Clayton, Ross Anderson, Editor G.Baldini, Standardisation and Certification of Safety, Security and Privacy in the ‘Internet of Things’, European Commission, Brussels, Belgium, 2017.

[2] The sustainability of safety, security and privacy [video]. Presentatie van Ros Anderson op het Choas Communication Congress in Leipzig, 28 december 2019: https://media.ccc.de/v/36c3-10924-the_sustainability_of_safety_security_and_privacy#t=1397

[3] Eireann Leverett, Richard Clayton, Ross Anderson, Standardisation and Certification of the ‘Internet of Things’, 2017.