INTERNET

Maak de makers van software aansprakelijk

Axel Arnbak

Het internet der dingen is levensgevaarlijk. Die realiteit valt na de veelbesproken Jeep hack een paar weken terug niet meer te ontkennen. De beveiligingsonderzoekers konden vanaf thuis een rijdende Jeep laten afremmen, plankgas geven en de spiksplinternieuwe bolide zo de greppel insturen. Na alle ophef haalde Fiat Chrysler 1,4 miljoen Jeeps van de markt. Het kon zo misgaan omdat softwareontwikkelaars als Fiat Chrysler — want dat zijn ze — aansprakelijkheid voor schade in algemene voorwaarden kunnen vrijwaren, waar fabrikanten in andere sectoren allang bij wet opdraaien voor verwijtbare fouten. Dat moet ook de regel worden voor software, nu in het internet der dingen naast onze data ook onze levens op het spel staan.

De beveiligingsonderzoekers hackten de Jeep via het audiosysteem uConnect, dat audio streamt via het mobiele netwerk van telecomaanbieder Sprint. Via uConnect kwamen ze bij de centrale boordcomputer en bij alle functies van de auto. Bovendien ontdekten zij dat ze met een Sprint-simkaart niet alleen een al bekende Jeep konden manipuleren, maar het hele Sprintnetwerk konden scannen naar kwetsbare uConnects in Jeeps. Extreem ernstig.

Voor de Jeep hack is samenwerking gezocht met de ervaren Wired-journalist, Andy Greenberg. In een filmpje zie je Greenberg op de snelweg de controle verliezen, terwijl de onderzoekers aan de keukentafel de Jeep overnemen. Ze benaderden ook twee Amerikaanse senatoren, die op de dag van publicatie wetgeving voorstelden om politieke munt te slaan uit alle ophef. Deze Spy Car Act moet veiligheidsgaranties in autosoftware en aansprakelijkheid bij cyberincidenten regelen.

De Jeep barst van de beginnersfouten. Waarom staan je autoradio en gaspedaal überhaupt met elkaar in verbinding? Waarom zijn alle uConnect audiosystemen vindbaar met een Sprint-netwerkscan? Het antwoord is simpel. Beveiliging kost tijd en geld. En waarom zou je als softwaremaker tijd en geld verspillen, als je geen inzage in je software hoeft te geven en je aansprakelijkheid kan vrijwaren in de kleine lettertjes van de koopovereenkomst? Fiat Chrysler kreeg wel $ 100 mln boete van de verkeersautoriteit NHTSA voor het jarenlang negeren van waarschuwingen, maar deze recordboete is kinderspel vergeleken met de mogelijke schade als niet de onderzoekers, maar kwaadwillenden tienduizend Jeeps hadden laten crashen. De ervaren onderzoekers stellen dat deze hack mogelijk is bij talloze andere merken.

Al in 1750 v. chr. stelde Hammurabi's wetboek Babylonische huizenbouwers aansprakelijk voor verwijtbare fouten bij de bouw. Van kettingzagen tot keukenmachines, ja zelfs autofabrikanten zijn nu bij wet aansprakelijk. Zelfs als je een testrit maakt en de rem remt niet. Dat zorgt voor kwaliteitsgaranties vooraf. Maar faalt een autorem vanwege software, dan ontspringen softwareontwikkelaars als Fiat Chrysler de juridische dans. Onlangs nog, bij cybersecuritywetgeving van de EU. Software zou te complex zijn. Dat klopt en is juist een probleem. Microsoft Windows bestond tien jaar terug al uit 35 miljoen regels code en is nog altijd zo lek als een mandje. Iedere extra regel code kan een lek betekenen. Het bedrijf bouwde een softwaremonopolie op, zonder op te draaien voor wrakke beveiliging.

Zelfrijdende auto, slimme cv-ketel of zorgrobot, al die internetdingen zijn potentiële moordwapens

Een ander cruciaal probleem is geheimhouding: net als Windows, is de software van de Jeep niet openbaar. Zij kan niet gekeurd worden op softwarekwaliteit. Open source software is wél openbaar. Die transparantie leidt tot rigoureuze kwaliteitscontrole, minder ernstige lekken en veel snellere updates.

Wetgeving moet dat belonen. Geeft een softwareontwikkelaar geen openheid van zaken, dan moet hij bij wet opdraaien voor verwijtbare fouten. Wat verwijtbare fouten en schadevergoedingen zijn, zal de rechter per sector en geval moeten bepalen. Fiat Chrysler, de leverancier van uConnect en Sprint zouden dat in de rechtszaal moeten uitvechten.

Zonder robuuste beveiliging geen connected cars, zelfrijdende auto, slimme cv-ketel of zorgrobot. Al die internetdingen zijn potentiële moordwapens. Software-aansprakelijkheid spoort ontwikkelaars eindelijk aan orde op zaken te stellen. Uiteraard zullen softwareontwikkelaars blijven roepen dat aansprakelijkheid de doodsteek is voor de huidige software-industrie. De indieners van de Spy Car Act zullen zeggen: mensenlevens redden was nou net de bedoeling.

Axel Arnbak is onderzoeker cybersecurity en informatierecht aan het IViR (UvA) en het Berkman Center (Harvard). Reacties @axelarnbak