

Meer grip op je slimme apparatuur? Huidige wetgeving schiet tekort

8.9.2026 - | Radboud Universiteit

Van slimme stofzuigers en deurbelcamera's tot complexe medische apparatuur in het ziekenhuis: steeds meer apparaten om ons heen zijn verbonden met het internet. Maar zijn we wel voldoende beschermd tegen de risico's die dat met zich meebrengt? Jurist Mattis van 't Schip pleit voor verbeterde Europese wetgeving die digitale apparaten als ecosystemen reguleert. Hij promoveert 16 september aan de Radboud Universiteit.

Van 't Schip onderzocht de afhankelijkheden van al die slimme apparatuur om ons heen. Want elk apparaat dat je in huis haalt, bevat chips en onderdelen van verschillende bedrijven. En de software waar het apparaat op loopt, is gebouwd op vele lagen aan software ontwikkeld door talloze partijen, van grote fabrikanten tot kleine hobbyisten. Al die partijen brengen hun eigen risico's met zich mee.

Ecosysteem

‘Eigenlijk schiet de huidige wetgeving tekort’, vertelt Van 't Schip. ‘Daarin wordt nog vaak gekeken naar individuele producten, maar we moeten het hele ecosysteem tegelijk aanpakken. Het gaat niet alleen om een laptop of slimme stofzuiger zelf, maar om het volledige netwerk van sensoren, leveranciers en cloudsysteem dat eraan vastzit. Als je het stikstofprobleem in een natuurgebied aanpakt, ga je ook niet elke boom op zichzelf beschermen.’

Door niet het hele ecosysteem in acht te nemen, kan een kleine kwetsbaarheid voor grote problemen zorgen. Van 't Schip: ‘Om een universiteit te hacken, hoef je niet per se de universiteit zelf aan te vallen. Je kunt ook gebruikmaken van een kwetsbaarheid van de laptops die medewerkers gebruiken en zo het netwerk binnendringen. Die laptops worden dan een soort modern Trojaans paard.’

Zo sterk als de zwakste schakel

‘Of het nu gaat om een huishouden, een universiteit, of een ziekenhuis: je cyberbeveiliging is zo sterk als je zwakste schakel,’ legt Van 't Schip uit. Wat gebeurt er bijvoorbeeld als de maker van je cameradeurbel failliet gaat, en een twijfelachtige andere partij het bedrijf overneemt?

Veel software leunt op open source-elementen. Van 't Schip: ‘Dat heeft veel voordelen: er is een actieve, enthousiaste gemeenschap van ontwikkelaars wereldwijd die vrijwillig helpen om software beter te maken. Ook is open source ontzettend transparant. Dat is een uitkomst: een apparaat maakt gebruik van tientallen soorten software, die vervolgens weer gebruikmaken van honderden andere softwarepakketten. Daarom is het voor wetgevers en organisaties enorm complex, maar wel noodzakelijk, om zicht te houden op wat er zich diep in die softwareketen afspeelt. Daar kunnen we veel leren van open source-software.’

Toch zijn ook hier soms risico's: ‘We hebben in het verleden al gezien dat kwaadwillenden jarenlang meewerken aan zo'n project om uiteindelijk een achterdeur in te bouwen. Maar door die transparantie komt zo iets vroeg of laat uiteindelijk gelukkig toch boven water.’

Verwachtingen van de consument

Uit onderzoek van Van 't Schip en collega's blijkt dat de meeste consumenten naar de fabrikant kijken als het om veiligheid gaat. 'Ze willen dat fabrikanten duidelijk communiceren als er een datalek is, en dat die problemen snel worden opgelost. Ook rekenen consumenten op ondersteuning gedurende de hele levensduur van het product.'

Volgens de jurist moeten er stappen gezet worden om consumenten minder afhankelijk te maken van fabrikanten. 'Veel apparaten zijn zo verweven met apps, online accounts en cloudservices dat consumenten nauwelijks invloed hebben op hun eigen digitale veiligheid. We moeten nadenken over manieren waarop mensen meer grip krijgen op hun eigen digitale omgeving, bijvoorbeeld door apparaten eenvoudiger los te koppelen van een dienst of uit een digitaal ecosysteem te halen.'

<https://www.ru.nl/onderzoek/onderzoeksnieuws/meer-grip-op-je-slimme-apparatuur-huidige-wetgeving-schiet-tekort>