Lange, Cremers, Abspoel, Banegas, Lambooij, Panny · ·

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Date
19 Aug 2018

Inbreng consultatie conceptvoorstel wijziging Wiv 2017

L.S.

Als cybersecurityonderzoekers zijn we bezorgd over de veiligheidsimplicaties van de Wiv. Wij zijn van mening dat in de voorgestelde wijzingen onvoldoende rekening is gehouden met een aantal negatieve effecten, en we moedigen de wetgever dan ook sterk aan om de wet opnieuw te overwegen met het oog op de volgende overwegingen. Wij gaan hierbij uitsluitend in op zaken binnen onze professionele expertise.

Kwetsbaarheden die niet zijn opgelost, maken iedereen minder veilig. Dit is inmiddels uitgebreid besproken in discussie rondom de wet. Wat in onze ogen onderbelicht is is dat de autorisatie om derden te hacken ook kan leiden tot het hacken van grote infrastructuursystemen, in plaats van enkel persoonlijke apparaten van doelwitten. Deze autorisatie zorgt voor een grotere kwetsbaarheid van systemen die een veel grotere impact hebben op de privacy van onschuldige burgers, en kunnen tevens zorgen voor grote economische schade aan bedrijven en particulieren.

Dat de regering ontstane kwetsbaarheden als potentiëel probleem ziet blijkt uit de voorgestelde amendementen. Er is een voorwaarde toegevoegd dat het hacken gericht moet zijn. Dit houdt echter onvoldoende rekening met dat hacken werkt via kwetsbaarheden in systemen, die noodzakelijkerwijs tevens aanwezig zijn op identieke systemen. In het geval van mobiele telefoons gaat het om miljoenen apparaten die hetzelfde besturingssysteem draaien. Omdat zulke kwetsbaarheden niet makkelijk te vinden zijn, zorgt de eis om in de toekomst een doelwit te kunnen hacken voor het bij voorzorg al zoeken naar kwetsbaarheden in systemen, en die vervolgens vast te houden, wat implicaties kan hebben voor miljoenen burgers. Van gericht hacken via derden is dan dus geen sprake.

Het argument dat dit zorgt voor een markt voor kwetsbaarheden, en dus een grotere vraag, is al veel behandeld in de eerste consultatie. Vaak lijkt er echter te worden uitgegaan van een situatie waarbij door betaling aan een exploitverkoper het alleenrecht wordt verworven. Dit lijkt ons uiterst onrealistisch; veel logischer is dat dezelfde kwetsbaarheden ook aan andere

overheden en bedrijven worden verkocht. Dat de Nederlandse overheid deze beveiligingsgaten zoekt zonder ze te dichten, zorgt dus direct voor beveiligings- en privacyrisico's van Nederlandse burgers en bedrijven, die niets te maken hebben met het directe doelwit.

Naast de mensenrechtenkwesties van massasurveillance zijn we ook bezorgd over de veiligheidsimplicaties van het plaatsen van afluisterapparatuur bij de providers en de Amsterdam Internet Exchange. De extra tappunten en de opslagplaatsen vormen een aantrekkelijk doelwit voor andere actoren dan de Nederlandse overheid. Daarnaast worden apparaten en programma's voor onderschepping mogelijk niet in huis geproduceerd en kunnen hun eigen achterdeuren bevatten. Dit kan worden opgevangen door audits, maar de richtlijnen bevatten ons inziens niet de juiste voorzieningen hiervoor. Erger nog, via overeenkomsten voor het delen van gegevens zullen sommige van deze gegevens buiten Nederland worden opgeslagen, mogelijk bij andere regeringen die niet dezelfde beveiligingsnormen hanteren.

We zijn blij met de aangebrachte wijzigingen die gebieden de mensenrechten te evalueren in landen waarmee een nieuwe overeenkomst voor het delen van gegevens wordt gesloten. Echter missen wij een evaluatie van bestaande samenwerkingsverbanden. Ook zien wij geen criterium dat veiligheidsgaranties en -geschiedenis van het andere land worden geëvalueerd. Belangrijker nog missen wij veiligheidsmaatregelen om te voorkomen dat bevriende landen mogelijk onze gegevens gebruiken om economische spionage tegen Nederlandse bedrijven uit te voeren.

Ten slotte beschouwen we het als een welkome ontwikkeling dat steeds meer mensen hun gesprekken en internetverbindingen beschermen met behulp van end-to-endencryptie. Echter maakt dit onderschepte gegevens natuurlijk minder nuttig voor de overheid. Wij zijn bang dat dit kan leiden naar eisen van achterdeurtjes in de cryptografie of het in het geheel verbieden van cryptografie, wat desastreuze gevolgen heeft voor de privacy van alle burgers tegen elke kwaadwillende derde.

Samengevat denken wij dat de voorgestelde aanpassingen aan de Wiv onvoldoende verbeteringen bieden, en te weinig rekening houden met alle potentiële negatieve gevolgen van de nieuwe wet. Wij zijn van mening dat de wet op essentiële punten herzien moet worden om de veiligheid van Nederlandse burgers en bedrijven in de toekomst te garanderen.

Hoogachtend,

prof. dr. Tanja Lange, Technische Universiteit Eindhoven
Prof. Dr. Cas Cremers, CISPA Helmholtz Centre i.G.
Mark Abspoel, CWI
Gustavo Banegas, Technische Universiteit Eindhoven
Eran Lambooij, University of Haifa
Lorenz Panny, Technische Universiteit Eindhoven

,