

De digitale inijkoperaties van de Politie Black Box (samenvatting I)

Nederlandse politie gebruikt spyware voor inlichtingenoperaties, inijkoperaties en andere opsporingsdoelen, niet voor het verzamelen van bewijs

De Nederlandse politie maakt de afgelopen jaren steeds vaker gebruik van spyware van commerciële bedrijven om laptops, computers, smartphones en andere gegevensdragers van verdachten binnen te dringen. Volgens de wet mag de politie alleen gebruik maken van haar hackbevoegdheid bij verdenkingen van terrorisme en ernstige criminaliteit. Door middel van spyware verkregen gegevens worden nauwelijks tot niet gebruikt als bewijs bij rechtszaken. Het lijkt erop dat de politie spyware tools gebruikt voor inlichtingenoperaties, inijkoperaties en andere opsporingsdoelen.

Inzet hackbevoegdheid voor andere doeleinden

Volgens de overheid gebruikt de politie haar hackbevoegdheid bij onderzoeken naar terrorisme en ernstige criminaliteit. Vanwege het ontbreken van transparante cijfers over de inzet van spyware valt moeilijk te beoordelen in hoeverre dit daadwerkelijk het geval is. Met behulp van spyware verkregen gegevens worden nauwelijks tot niet als bewijs ingebracht in rechtszaken.

De overheid geeft geen overzicht van het aantal en type onderzoeken waarbij spyware is ingezet, het aantal zaken waarin dit tot een veroordeling heeft geleid, en tot welke straf. Spyware kan ook worden ingezet bij onderzoeken naar minder zware vormen van criminaliteit, en ook tegen advocaten, journalisten en activisten.

Er zijn sterke aanwijzingen dat de politie voor andere doeleinden inzet dan het verkrijgen van bewijs in rechtszaken. Het lijkt erop dat de politie spyware tools gebruikt voor inlichtingenoperaties, inijkoperaties en andere opsporingsdoelen, zonder dat een rechtercommissaris toezicht houdt op de rechtmatigheid van de inzet.

Binnen Europa, zoals in Hongarije, Griekenland, Polen en Spanje, is de afgelopen jaren steeds meer bekend geworden over de inzet van spyware tegen oppositieleiden, journalisten en advocaten. Er is alle aanleiding tot zorg dat dit in Nederland ook het geval is. De Minister van Veiligheid en Justitie beantwoordde deze vraag in december 2022 bevestigend noch ontkennend.

Betrouwbaarheid verkregen bewijs in het geding

De betrouwbaarheid van met spyware verkregen bewijs is bij commerciële spyware in het geding. Spyware tools zijn een 'black box'. De politie heeft weinig inzicht in de werking van de tools, de wijze waarop een computer of smartphone wordt binnengedrongen, hoe gegevens worden verzameld en bewijs wordt verkregen en de aanwezigheid van backdoors kan niet worden uitgesloten.

Leveranciers van de spyware, en mogelijk derden, kunnen toegang verkrijgen tot de gegevensdragers van de verdachte, de spyware en de servers waarop de gegevens worden bewaard. Manipulatie van de gegevens en bewijs is dan ook mogelijk: door de politie verzamelde bewijslast kan veranderd of vernietigd kan worden, en gegevens kunnen worden toegevoegd aan de bewijslast.

De keuring om de integriteit van spyware tools te waarborgen is zeer beperkt, omdat leveranciers van de spyware onvoldoende inzicht geven in de broncode en weigeren mee te werken aan een goede keuring. De politie neemt de keuringen nauwelijks serieus en spyware tools worden meestal ingezet zonder voorafgaand te zijn gekeurd. Niet gekeurde of slecht gekeurde opsporingsmiddelen hebben gevolgen voor het gebruik van bewijsmateriaal in de rechtszaal.

Toezicht schiet tekort

Het toezicht op de toepassing van de hackbevoegdheid schiet tekort. De Inspectie Justitie en Veiligheid signaleert weliswaar problemen rond de betrouwbaarheid van door middel van de inzet van spyware verkregen bewijsmateriaal, de bewijslogging en keuring van de technische hulpmiddelen, maar op andere punten ontbreekt essentiële informatie in de verslagen van de Inspectie.

Zo publiceert de Inspectie niet het aantal bevelen van de inzet van spyware en het handmatig hacken. Hierdoor is niet duidelijk hoe vaak de politie daadwerkelijk gebruik maakt van de hackbevoegdheid, hoewel de politie steeds vaker hackt. De verslagen van de Inspectie bevatten ook geen overzicht van het aantal en type onderzoeken waarbij spyware is ingezet, het aantal zaken waarin dit tot een veroordeling heeft geleid, en tot welke straf.

Hierdoor is niet te beoordelen in hoeverre spyware alleen wordt ingezet bij onderzoeken naar terrorisme en georganiseerde ernstige criminaliteit. De proportionaliteit en subsidiariteit van de inzet kunnen hierdoor niet beoordeeld worden. Function creep ligt op de loer: er zijn sterke aanwijzingen dat spyware wordt ingezet voor andere doeleinden dan waarvoor zij wettelijk bedoeld is.

In het onderzoek 'Een politie black box, het gebruik van spyware door de Nederlandse politie' borduurt Buro Jansen & Janssen voort op eerdere onderzoeken van het Buro naar de cybersurveillance industrie en relatie tussen de Nederlandse politie en leveranciers van spyware. Er is gebruik gemaakt van openbare bronnen, Woo-verzoeken en rapporten van de Inspectie Justitie en Veiligheid.