BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank NL32ABNA0554706512
KvK 34 12 12 86

M +31 6 13380036
E ton.siedsma@bof.nl
W https://www.bof.nl

Eerste Kamercommissie voor Veiligheid en Justitie

Betreft
Bijdrage Bits of Freedom deskundigenbijeenkomst Wetsvoorstel computercriminaliteit III

Amsterdam
19-06-2017

Bits of Freedom komt op voor een open en vrij internet. We vinden het van groot belang dat burgers vrijelijk met elkaar kunnen communiceren zonder dat daarbij hun grondrechten geschonden worden, door andere burgers, bedrijven, of door overheden.[1]

Technologische vernieuwingen stellen overheden altijd voor complexe ordeningsvraagstukken. Dat is bij de digitaliserende samenleving niet anders. Er moet voor gewaakt worden dat bij het nastreven van, op zichzelf legitieme, beleidsdoelstellingen ongewenste neveneffecten optreden.

Het voorliggende Wetsvoorstel computercriminaliteit III, in het bijzonder de "hackbevoegdheid" waarmee de politie op afstand afstand apparaten kan hacken, toont aan dat op diverse punten onvoldoende is nagedacht over de consequenties van het wetsvoorstel. Zonder reparatie van die aspecten staan de rechten van onschuldige burgers op het spel. Hieronder zullen deze aspecten benoemd worden en zullen ook enkele suggesties worden gedaan hoe deze gerepareerd kunnen worden.

Een aantal aspecten zal daarbij niet behandeld worden. Het hacken in het buitenland, de reikwijdte van het begrip geautomatiseerd werk en de hoeveelheid bevoegdheden die ingezet kunnen worden na het hacken geven grote reden tot zorg, maar zullen vanwege de gevraagde beknoptheid van deze bijdrage niet nader toegelicht worden.

1 Waarbij moet worden opgemerkt dat voor die vrije communicatie vanzelfsprekend wettelijke beperkingen gelden.

1. Gebruik kwetsbaarheden riskant

De Nederlandse politie wil om te kunnen hacken (onbekende) kwetsbaarheden benutten. Dat betekent dat de Nederlandse politie een belang krijgt bij het voortbestaan van die kwetsbaarheden. Immers, als de kwetsbaarheden gedicht worden, dan kan de politie ze ook niet gebruiken.

Meer in het bijzonder wil de Nederlandse politie onbekende kwetsbaarheden achter kunnen houden. Dat zijn kwetsbaarheden die nog niet bekend zijn bij de maker van de software, die daardoor de kwetsbaarheid niet kan verhelpen. Die kwetsbaarheid zit dan niet alleen in het apparaat van de verdachte, maar in alle apparaten van dat type. Apparaten die ook door veel onschuldige burgers gebruikt worden. Die kwetsbaarheid zit dus kort gezegd niet alleen in de Samsung S8 van een verdachte, maar in alle Samsung S8's.

Het probleem daarbij is dat er geen enkele garantie dat de politie de enige partij is die die kwetsbaarheid kent. Criminelen zouden hem bijvoorbeeld ook kunnen kennen en misbruiken. Recente ervaringen, zoals bij Wannacry laten zien dat het achterhouden van zulke onbekende kwetsbaarheden ook in de praktijk grote risico's kan opleveren voor de onschuldige internetgebruiker.[2]

Bits of Freedom is dus tegen het gebruik van onbekende kwetsbaarheden vanwege het grote risico voor de onschuldige burger. Maar zelfs als die kwetsbaarheden toch ingezet zouden worden, dan moet er een helder beleid zijn over de inzet en het achterhouden van die kwetsbaarheden. Dit beleid ontbreekt op dit moment en moet worden vastgesteld voor de inwerkingtreding van het wetsvoorstel.

In het bijzonder moeten er nadere regels komen voor het maken van de afweging tussen het achterhouden van een kwetsbaarheid vanuit individueel opsporingsbelang en het algemene belang dat is gediend bij het zo snel mogelijk melden van kwetsbaarheden. Daarbij moeten er onafhankelijke, externe experts bij die afweging worden betrokken, die waar nodig tegenspraak en tegenwicht kunnen bieden.

2. Reguleer het gebruik van hacksoftware

Het beoogde gebruik van hacksoftware illustreert dat het kwetsbaarhedenbeleid onvoldoende doordacht is. De politie zal off the shelf hacksoftware gaan inkopen om verdachten te kunnen hacken, van bedrijven die ontzettend goed zijn in het maken van dat soort producten. Bij de wetsbehandeling bleek dat de onbekende kwetsbaarheden die met deze producten worden benut niet gemeld hoeven te worden, omdat de Nederlandse politie niet kan weten of deze producten gebruik maken van onbekende kwetsbaarheden om te hacken.

2 Zie bijvoorbeeld de Wannacry-uitbraak, die gebaseerd is op oorspronkelijk achtergehouden kwetsbaarheden. http://nos.nl/artikel/2172840-waarschuwing-voor-grote-internationale-gijzelsoftware-campagne.html.

Het is bij de parlementaire behandeling helder geworden dat juist dit soort software van derde partijen in de praktijk veelvuldig ingezet zal gaan worden. Dat betekent dat het moeten melden van kwetsbaarheden in theorie wel het uitgangspunt is, maar dat het achterhouden van kwetsbaarheden de gangbare praktijk zal blijken te zijn. Dat is natuurlijk onverteerbaar.

De Nederlandse regering mag zich niet verschuilen achter geheimzinnigheid of achter het feit dat een bedrijf geen openheid wil geven. Als het uitgangspunt is dat onbekende kwetsbaarheden gemeld moeten worden, dan moet dat gelden ongeacht de manier waarop die kwetsbaarheden gevonden zijn of worden gebruikt. Of dat nou via een vaardige politie-agent is of dat die kwetsbaarheden via deze hacksoftwarepakketten worden ingekocht: onbekende kwetsbaarheden moeten worden gemeld.

3. Technische waarborgen zijn onvoldoende

Dit wetsvoorstel ziet op het gebruik van technisch geavanceerde middelen om bevoegdheden in te kunnen zetten. Een vereiste daarvoor is dat niet alleen de juridische maar ook de technische waarborgen voldoende op orde zijn. Die bepalen namelijk voor een groot deel hoe groot het risico op (ongewenste) inbreuken daadwerkelijk is. Het voorgestelde "Besluit onderzoek in een geautomatiseerd werk" dient die technische waarborgen te garanderen maar slaagt daar op belangrijke onderdelen niet in.

Het Besluit moet voorzien in waarborgen vanaf het moment dat het hacken start. De risico's voor (de gebruiker) van een apparaat starten namelijk niet op het moment dat informatie wordt overgenomen, maar die starten op het moment dat het apparaat wordt betreden. Net zoals bij een doorzoeking van een huis de inbreuk niet begint vanaf dat de politie-agent in een woonkamer staat, maar vanaf het moment dat hij de deur wil forceren.

Het grootste pijnpunt is dan ook dat het Besluit ten onrechte geen waarborgen biedt vanaf het moment van hacken, maar pas nadat het apparaat gehackt is. Het Besluit moet daarom ook regels stellen voor de technische waarborgen bij het betreden van het apparaat. Zo moet er bijvoorbeeld vanaf de start van het hacken een deugdelijke logging zijn, zodat kan worden gecontroleerd of met de software waarmee gehackt wordt geen onverwachte of onrechtmatige handelingen zijn verricht.

Deze aanscherping is niet alleen nodig voor de verdachte, maar zorgt ook voor een effectiever toezicht op de uitoefening van deze bevoegdheid en dat er sneller bijgestuurd kan worden als onverhoopt blijkt dat de software waarmee wordt gehackt ongewenste bijwerkingen vertoont.