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

Vaste commissie voor Veiligheid en Justitie

Betreft
Bijdrage Bits of Freedom voor rondetafelgesprek wetsvoorstel computercriminaliteit III

Amsterdam
08-02-2016

Volgens Bits of Freedom heeft het wetsvoorstel computercriminaliteit III een averechts effect op de Nederlandse cyber security omdat de hackbevoegdheid de Nederlandse internetter onveiliger maakt in plaats van veiliger. Daarnaast ontbreekt de noodzaak voor deze bevoegdheid. Ook zijn in het wetsvoorstel veel essentiële vragen niet beantwoord. Tot slot is het noodzakelijk dat er een commissie komt die onafhankelijk toezicht op de opsporingsdiensten uitoefent.

1. Noodzaak niet aangetoond

Sinds in 2012 het eerste plan voor de hackvoorstel werd aangekondigd, is de noodzaak voor deze nieuwe bevoegdheid nog nooit aangetoond. Dat gebeurde niet in de Memorie van Toelichting bij de internetconsultatie in 2013 en dat gebeurt evenmin in de Memorie van Toelichting bij het huidige wetsvoorstel.

Dat niet wordt aangetoond waarom deze bevoegdheid daadwerkelijk noodzakelijk is, is buitengewoon verontrustend. Zonder noodzaak is er geen reden voor het bestaan van de bevoegdheid. Het ministerie van Veiligheid en Justitie moet die noodzaak dan ook bewijzen vóór we kunnen nadenken hoe deze bevoegdheid ingeregeld zou moeten worden.

Het aantonen van die noodzaak is des te prangender omdat de hackbevoegdheid een perverse prikkel vormt voor de Nederlandse overheid met betrekking tot de veiligheid van de internetgebruiker. De Nederlandse overheid heeft immers een belang bij het bestaan van (meer) onveilige apparaten bij verdachten, terwijl diezelfde apparaten ook door onschuldige burgers worden gebruikt. Die kunnen de dupe worden als de Nederlandse overheid kennis over zwakheden in software heeft, maar deze niet met het bedrijfsleven en gebruikers deelt.

2. Wetsvoorstel roept veel vragen op

Zelfs als over de ontbrekende noodzaak en de negatieve werking van de bevoegdheid op de veiligheid van onze apparaten en infrastructuur wordt heengestapt, dan blijven er in het wetsvoorstel veel problemen onopgelost. Ter illustratie daarvan worden hieronder de drie belangrijkste besproken.

2.1 Ontbreken technische waarborgen

Bij een wetsvoorstel dat bij uitstek gaat over de inzet van een technisch middel zijn juridische waarborgen bij de inzet niet genoeg. De regels voor de beheersing en integriteit van de techniek zijn cruciaal. Het Besluit technische hulpmiddelen voldoet op dit moment niet aan de eisen van digitale opsporingsbevoegdheden en moet worden herzien. Dat vindt het ministerie van Veiligheid en Justitie gelukkig ook.

Maar de daadwerkelijke inhoud van het nieuwe Besluit is nog niet bekend. Dat betekent dat de wet die nu in het parlement behandeld wordt onvolledig is. Er is immers geen volledig overzicht van de waarborgen maar ook niet van de mogelijke niet afgedekte (technische) risico's.

Het is daarom essentieel dat het Besluit technische hulpmiddelen wordt herzien vóórdat het parlement zich uitspreekt over het voorliggende wetsvoorstel, met een voorhangprocedure waarbij het Besluit ook op internetconsultatie wordt geplaatst. Alleen dan wordt daadwerkelijk duidelijk of – en hoe – de risico's bij het gebruik van deze bevoegdheid worden ingedamd.

2.2 Reikwijdte geautomatiseerd werk

De reikwijdte van het begrip 'geautomatiseerd werk' is zodanig geformuleerd dat niet voorzienbaar is welk apparaat wel of niet gehackt mag worden door de politie. Onder de voorgestelde definitie valt eigenlijk elk apparaat dat met het internet verbonden is of zou kunnen zijn. In aanmerking genomen dat het aantal apparaten dat daaronder valt exponentieel gaat groeien bij de ontwikkeling van het 'Internet of Things' roept dat de vraag op: tot hoe ver mag deze bevoegdheid gaan bij apparaten die zich in of rond het menselijk lichaam begeven?

Staatssecretaris Dijkhoff stelt dat ook pacemakers onder de definitie vallen. Maar is het echt nodig om zulke apparaten onder de categorie te hacken apparaten te laten vallen? En is het bijvoorbeeld de bedoeling om in de toekomst auto's te hacken om die vervolgens stil te zetten als de politie een verdachte aan wil houden?

Als er bij het ministerie van Veiligheid en Justitie of bij de Nationale Politie over zulke inzetten wordt nagedacht, dan zou dat voor het publiek duidelijk moeten worden, zodat er een helder debat kan plaatsvinden over de reikwijdte van de bevoegdheid. Nu, maar ook in de toekomst.

2.3 Reikwijdte inzet bevoegdheid

De bevoegdheid is volgens de wet en de Memorie van Toelichting, anders dan vaak wordt gezegd, niet alleen gericht op cybercriminelen. Sterker nog, de bevoegdheid is van toepassing op een hele brede groep van misdrijven verdachte personen. Voor een bevoegdheid die wordt voorgesteld als een ultimum redium is dat veel te breed, zeker met inachtneming van het volgende.

In de jaren '70 van de vorige eeuw werd de telefoontap ingevoerd. In de Handelingen bij de invoering van de bevoegdheid werd aangegeven dat deze slechts enkele keren per jaar zou worden ingezet. Intussen weten we dat die situatie nogal gewijzigd is. Het is niet uit te sluiten dat dat in de toekomst voor de hackbevoegdheid ook zo zal gaan.

In de financiële paragraaf bij het huidige wetsvoorstel wordt al aangegeven dat er kosten kunnen worden bespaard met de inzet van deze bevoegdheid, omdat die andere bevoegdheden zou kunnen vervangen. Dat betekent dat de deur naar de inzet van de hackbevoegdheid als efficiënter middel in andere domeinen op zijn minst al op een kier staat.

Bits of Freedom vindt dat een dergelijke zware bevoegdheid nooit uit efficiëntie-overwegingen moet worden ingezet.

Tot slot zou Bits of Freedom nog het volgende willen meegeven.

3. Voer een onafhankelijke commissie in voor toezicht op opsporingsdiensten

Er zijn steeds meer opsporingsbevoegdheden die zich in het digitale domein afspelen. Denk bijvoorbeeld aan het controleren of observeren van sociale media, maar ook *predictive policing* en natuurlijk het voorliggende hackvoorstel. De controle op de inzet van zulke bevoegdheden, die naar hun aard heimelijk worden toegepast, is essentieel. Nu vindt die controle vooraf plaats via de rechter-commissaris en eventueel achteraf in de rechtszaal.

Maar veel verdachten komen uiteindelijk niet voor de rechter en de rechter-commissaris toetst het individuele geval, maar kijkt niet per se naar de samenhang met andere zaken en de controle op de inzet van die bevoegdheid. Daarnaast kunnen sommige misstanden bij de inzet in de rechtszaal door de advocaat niet worden tegengeworpen aan het Openbaar Ministerie. Er zijn op die manier ook weinig prikkels om in dat opzicht verbeteringen door te voeren.

Bits of Freedom acht het verstandig om daarvoor een onafhankelijke commissie in te stellen, in zekere zin vergelijkbaar met de huidige CTIVD voor de geheime diensten. Die commissie zou dan opsporingsbreed kunnen kijken naar het hele proces, van totstandkoming van verzoeken om bevoegdheden in te zetten tot en met de wijze waarop de inzet plaatsvindt.