BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KvK 34 12 12 86

M +31(0)646282693
E simone.halink@bof.nl
W https://www.bof.nl

Vast commissie voor Veiligheid en Justitie
Tweede Kamer der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Betreft
Bezwaren tegen hackplannen Opstelen

Amsterdam
30 november 2012

Geachte leden van de Commissie voor Veiligheid en Justitie,

Op 6 december 2012 spreekt de Vaste Commissie voor Veiligheid en Justitie over de brief van minister Opstelten aan het parlement van 15 oktober 2012 waarin wordt voorgesteld om politie en justitie de bevoegdheid te geven op afstand in te breken in computers. Deze bevoegdheden hebben verstrekkende implicaties: ze zullen Nederland niet veiliger, maar juist ónveiliger maken. In deze brief deelt digitale burgerrechtenbeweging Bits of Freedom haar zorgen met u.

In het kort zijn onze belangrijkste bezwaren dat het voorstel:

- leidt tot een disproportionele inperking van de privacy;
- onaanvaardbare gevolgen heeft voor de internetvrijheid en veiligheid van (Nederlandse) internetters; en
- leidt tot een schending de soevereiniteit van andere landen door Nederland. De tegenreactie die dit uitlokt heeft alarmerende gevolgen voor de soevereiniteit van Nederland en voor cybersecurity en mensenrechten wereldwijd.

Wij verzoeken u vriendelijk doch dringend om kennis te nemen van de inhoud van deze brief en de daarin gestelde vragen op 6 december 2012 aan de minister voor te leggen.

Inhoud voorstel

In zijn brief van 15 oktober 2012 stelt de minister voor om politie en justitie drie nieuwe bevoegdheden te geven[1]:

1 Daarnaast zou het strafbaar worden om (digitale) gegevens te helen. Bespreking van dit

1. Het inbreken op geautomatiseerde werken (zoals computers en routers, maar ook mobiele telefoons)(voor het gemak in deze brief gezamenlijk aangeduid als 'computers') via het internet en het installeren van spyware, waarmee de computer door de politie kan worden overgenomen.
2. Het inbreken op computers via het internet en die computers vervolgens doorzoeken, ook in het buitenland.
3. Het inbreken op computers en de gegevens daarop vernietigen, ook in het buitenland.

Volgens de minister zijn deze bevoegdheden nodig om cybercrime te bestrijden. Onderbouwing van enige noodzaak daartoe en van de proportionaliteit en effectiviteit van de voorgestelde bevoegdheden schiet echter ernstig tekort. De minister laat verder weten dat – ondanks dat de bevoegdheid daartoe blijkbaar ontbrak – de politie het afgelopen jaar al inbrak in computers, die computers doorzocht en zelfs gegevens heeft vernietigd op servers in het buitenland.

Noodzakelijkheid en proportionaliteit voorstel onvoldoende onderbouwd

De minister schrijft dat "een inhaalslag nodig is om de opsporing en vervolging van cybercrime te versterken". Vervolgens schetst de minister weliswaar een aantal problemen bij de opsporing, zoals de achterblijvende "kennis en ervaring binnen de strafrechtketen" en technische innovatie die handig wordt gebruikt door criminelen, maar hoe de voorgestelde maatregelen die problemen specifiek gaan oplossen en of ze noodzakelijk, proportioneel en effectief zijn, wordt niet onderbouwd. Het mag duidelijk zijn dat deze flinterdunne onderbouwing voor een wetsvoorstel onacceptabel is, zeker als het om zo een verstrekkend voorstel gaat.

Daarnaast zijn de bevoegdheden van de minister gericht op het bestrijden van strafbare feite nadat deze hebben plaatsgevonden. In cybersecurity is het echter zeer gebruikelijk om in plaats daarvan maatregelen te nemen om te zorgen dat bepaalde inbreuken niet plaatsvinden door het nemen van preventieve maatregelen, zoals het vergroten van de expertise en capaciteit op het gebied van cybersecurity. Het is opvallend dat de minister daaraan geen aandacht besteed.

Vraag: Hoe groot is het probleem van cybercriminaliteit? Groeit het probleem en, zo ja, hoe hard? Waaruit blijkt dat? Hoe groot is het probleem van cybercriminaliteit in verhouding tot andere vormen van criminaliteit?

Vraag: Waaruit blijkt dat de voorgestelde bevoegdheden, die reactief van

voorstel laten we in deze brief achterwege.

aard zijn, effectiever zijn dan preventieve maatregelen gericht op het verbeteren van kennis en capaciteit op het gebied van cybersecurity?

Het voorstel van de minister leidt tot een ernstige inperking van de privacy, niet alleen van de verdachte maar ook van onschuldige Nederlanders. Zo hebben de voorgestelde bevoegdheden veel grotere gevolgen voor de privacy van betrokkenen. Bij het aftappen van telefoongesprekken of het plaatsen van afluisterapparatuur geldt al dat niet alleen de verdachte wordt afgeluisterd maar ook al die personen waarmee de verdachte via die lijn of in die woning communiceert. De privacy-implicaties van het doorzoeken van computers zijn echter nog eens tien keer groter: alle mailtjes, alle foto's en alle berichten op sociale media die een verdachte met onschuldige Nederlanders heeft uitgewisseld, komen in het vizier van de opsporing.

Het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden vereist dat maatregelen die fundamentele rechten – zoals het recht op privacy – beperken, noodzakelijk in een democratische samenleving en proportioneel zijn. Dit moet voorafgaand aan de invoering van die maatregelen zijn aangetoond, zoals ook blijkt uit de motie Franken.[2] De minister schetst weliswaar een aantal problemen die moeilijk zijn voor opsporing, maar hoe de voorgestelde maatregelen die problemen specifiek gaan oplossen en of ze noodzakelijk, proportioneel en effectief zijn, wordt niet onderbouwd. Daarmee is het voorstel in strijd met voornoemd verdrag.

Vraag: Uit welke documenten blijkt dat de noodzaak, de proportionaliteit en de effectiviteit is onderzocht en afdoende is vastgesteld?

Voorstel vergroot cybersecurityrisico's

Als de politie bij computers moet kunnen inbreken, heeft ze er belang bij dat die systemen kwetsbaar blijven. De politie kan immers slechts inbreken bij systemen die onvoldoende beveiligd zijn. Dit geeft de overheid een perverse prikkel om informatie over kwetsbaarheden voor zichzelf te houden in plaats van deze te delen met Nederlandse internetgebruikers. Die kunnen hun eigen informatiesystemen daardoor minder goed beschermen. Dit staat lijnrecht tegenover alle investeringen van de overheid in cybersecurity over de afgelopen jaren.

Vraag: Als overheden op de hoogte zijn van het bestaan van kwetsbaarheden in computers, zijn er dan situaties denkbaar waarin zij

2 Motie Franken, Eerste Kamer, vergaderjaar 2010–2011, 31 051, D.

die kennis geheim moeten houden omwille van de opsporing? Hoe verhoudt dat zich tot de ambitie van de regering om de Nederlandse informatiesamenleving via overheidsorganisaties zoals het Nationaal Cyber Security Centrum (NCSC) te beschermen? Kunnen en mogen deze instanties dan nog optreden/waarschuwen richting overheden en het publiek wanneer dit een lopend onderzoek zou kunnen belemmeren?

Bovendien geldt dat spyware moeilijk binnen de perken te houden is. In Duitsland hebben ze dat al ervaren. Uit onderzoek van de hackersvereniging Chaos Computer Club bleek dat heimelijk door de politie geïnstalleerde afluistersoftware makkelijk te hacken was – via het internet.[3] Zodat niet alleen de politie een computer kon overnemen met behulp van spyware, maar dat ook criminelen diezelfde computer konden overnemen, omdat de spyware zélf gehackt was. De politie maakt zich in dat geval ook nog eens kwetsbaar voor computerinbraken via diezelfde software.

Verder bestaat het risico dat ingezette spyware zich verder verspreidt en onschuldige systemen infecteert; dit gebeurde onder meer bij het virus Stuxnet dat was ontwikkeld voor kernreactoren in Iran, maar ook systemen in de Verenigde Staten geïnfecteerd blijkt te hebben.

Vraag: Hoe gaat de politie spyware verspreiden? Gebeurt dit via exploits en, zo ja, hoe installeert zij die exploits? Via phishing-achtige e-mails? Wordt de hulp van internetproviders hierbij gevraagd? Of wordt er fysiek op de computer van de verdachte ingebroken om de spyware te installeren en, zo ja, wat gebeurt er dan als de locatie van de computer onbekend is?

Vraag: Hoe gaat de minister waarborgen dat de spyware van de Nederlandse politie niet wordt misbruikt door kwaadwillenden?

Vraag: Hoe wordt voorkomen dat de spyware zich verder verspreidt en onschuldige systemen infecteert?

Bovendien leiden de voorgestelde bevoegdheden tot veel praktische problemen. Hoe zal de overheid bijvoorbeeld omgaan met antivirussoftware? Immers, als antivirussoftware de spyware van de Nederlandse politie op een computer aantreft, zou dat in principe aan de gebruiker moeten worden gemeld. De vraag is dus of de overheid van antivirusbedrijven zal verwachten of hen ertoe zal verplichten dat ze overheids-spyware niet detecteren, melden of verwijderen,

3 Zie de analyse van Duitse securityvereniging Chaos Computer Club: http://ccc.de/en/updates/2011/staatstrojaner.

met het gevolg dat gebruikers extra kwetsbaar zijn.[4] Over dit probleem heeft Kamerlid Berndsen-Jansen (D66) de minister op 14 november 2012 reeds kritische vragen gesteld.[5]

> **Vraag:** Hoe gaat de minister zorgen dat de spyware die de politie inzet niet door antivirusbedrijven wordt opgemerkt?

Een ander praktisch probleem is dat de bevoegdheden erg makkelijk misbruikt kunnen worden. Juist doordat deze opsporingshandelingen digitaal zijn is het moeilijk na te gaan of bewijs is gefabriceerd of juist is achtergehouden. Een hieraan gerelateerd voorbeeld: in Duitsland is gebleken dat de spyware die bedoeld was om alleen Skype gesprekken af te luisteren, in de praktijk ook ingezet kon worden voor het op afstand aanzetten van de camera. In Duitsland trokken onderzoekers dan ook de conclusie dat deze software niet geschikt was voor bewijsvergaring.[6]

> **Vraag:** Hoe gaat de minister waarborgen dat deze nieuwe bevoegdheden niet misbruikt worden?

Voorstel leidt tot schending van soevereiniteit

In internationale context worden de hiervoor genoemde problemen alleen nog maar verder versterkt. Het voorstel geeft de politie namelijk de ruimte te hacken zonder rechtshulpverzoek, indien de locatie van de computer onbekend is. Dit is bijvoorbeeld het geval als gebruik wordt gemaakt van anonimiseringssoftware zoals Tor.

Schending van soevereiniteit van staten kan ertoe leiden dan ook andere landen het met het soeveriniteitsbeginsel niet zo nauw nemen, in het bijzonder in relatie tot Nederland. Dat kan leiden tot inbraken op computers vanuit andere landen om zeer uiteenlopende redenen zoals godslastering, haatzaaien en inbreuken op auteursrechten.

Burgers, dissidenten in het bijzonder, worden dan het slachtoffer van een wapenwedloop tussen hackende overheden. Internationale samenwerking op het gebied van cybercrime komt dan onder druk te staan.

> **Vraag:** Vindt de minister het acceptabel dat buitenlandse overheden op

4 Bart Jacobs, Policeware, Nederlands Juristenblad, afl. 39, p. 2764.
5 TK 2012–2013, Vraagnummer 2012Z19297, vraag 4.
6 Zie de analyse van Duitse securityvereniging Chaos Computer Club: http://ccc.de/en/updates/2011/staatstrojaner.

Nederlandse computers inbreken, data doorzoeken en/of data vernietigen? Zo nee, wat gaat de minister doen om dit te voorkomen?

De internationale gemeenschap maakt zich ernstig zorgen over de hiervoor genoemde punten, zoals blijkt uit bijgaande brief. Meer dan 40 organisaties die zich inzetten voor digitale burgerrechten hebben deze brief ondertekend. Gezien de grote risico's die het voorstel heeft voor cybersecurity en de bescherming van mensenrechten wereldwijd, roept een brede internationale coalitie van maatschappelijke organisaties de minister in die brief op om zijn voorstel in te trekken.

Vraag: Wat is de reactie van de minister op de brief van de internationale gemeenschap?

Ik houd me graag beschikbaar voor een toelichting, mocht daaraan behoefte bestaan.

Met vriendelijke groet,

Simone Halink
Bits of Freedom