Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 320

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 juli 2014

Tijdens het algemeen overleg Cybersecurity van 27 maart jongstleden (Kamerstuk 26 643, nr. 312) is een aantal vragen gesteld over de aanpak van botnets in Nederland. Deze vragen hebben betrekking op de verantwoordelijkheidsverdeling en de samenhang van de activiteiten van de private en publieke organisaties die betrokken zijn bij de aanpak van botnets, alsmede op aspecten als privacy en aansprakelijkheid. Met deze brief voldoe ik, mede namens mijn ambtgenoot van Economische Zaken, aan de toezegging uw Kamer voor de zomer te informeren over de aanpak van botnets in Nederland.

Met enige regelmaat worden burgers het slachtoffer van cybercriminaliteit. Daarbij maken criminelen geregeld gebruik van botnets. Een botnet is een netwerk van samenwerkende apparaten, meestal privé- of bedrijfscomputers, de zogeheten «bots», die met dezelfde malware zijn besmet. Criminelen kunnen een botnet centraal aansturen om de bots voor eigen doeleinden in te zetten. Deze problematiek is door het NCSC in de opeenvolgende Cyber Security Beelden Nederland geschetst.

De dreiging die uitgaat van botnets neemt het kabinet serieus. De aanpak van deze dreiging vraagt inzet van overheid, bedrijfsleven en burgers. De overheid handelt daarbij op verschillende vlakken en vanuit verschillende rollen, zoals hieronder wordt geschetst. Vanuit het bedrijfsleven pakken de Internet Service Providers een actieve rol in de bestrijding van botnets en geven daarbij invulling aan de in de tweede Nationale Cyber Security Strategie (NCSS 2)[1] beschreven zorgplicht die leveranciers jegens hun klanten hebben. Daarnaast ligt er voor burgers in de rol als eindgebruiker een belangrijke rol in het verbeteren van de eigen cyberhygiëne.

Bij het bestrijden van botnets is het van belang dat genoemde partijen de volgende maatregelen nemen: het verhogen van veiligheidsbewustzijn en het tegengaan van besmettingen, het actief bestrijden van besmettingen,

[1] Kamerstuk 26 643, nr. 291

kst-26643-320
ISSN 0921 - 7371
's-Gravenhage 2014

het opsporen en vervolgen van beheerders van botnets en het verstoren van de werking van botnets.

Verhogen van veiligheidsbewustzijn en het tegengaan van besmettingen

De eigenaar van een computer is zelf verantwoordelijk voor de eigen informatiebeveiliging en heeft daarmee de taak om voldoende maatregelen te nemen om zijn of haar computer vrij te houden van malware. De samenleving dient zich daarom in toenemende mate bewust te zijn van de dreigingen en daarbij bekwaam te handelen. Hiertoe zet de overheid vanuit de NCSS-2 actief in op het verhogen van dit bewustzijn en het versterken van de bekwaamheid. Van 27 oktober tot 6 november 2014 zal voor de derde keer de awareness-campagne Alert Online worden gehouden. Deze draagt bij aan de bewustwording van iedereen in de samenleving om veilig om te gaan met computers. Ook werkt het Ministerie van Economische Zaken samen met het Ministerie van Veiligheid en Justitie en ECP, platform voor de informatiesamenleving, aan een nieuwe informatiebron voor burgers, veiliginternetten.nl. Deze zal in het najaar tijdens de campagne Alert Online worden gelanceerd.

Bestrijden van besmettingen

Bij brief van 17 mei 2011 is uw Kamer geïnformeerd over de Digitale Agenda Nederland[2]. Hierin is de actielijn *Schone computers door aanpak van Botnets* opgenomen. Uit deze actielijn is met eenmalige steun van het Ministerie van Economische Zaken het private initiatief van de vereniging Abuse Information Exchange ontstaan. Deze vereniging van internet service providers heeft recent een centrum (Abuse HUB) opgericht dat centraal informatie over botnetbesmettingen verzamelt en verwerkt. Deze informatie wordt ter beschikking gesteld aan leden van de vereniging. Zij kunnen zo besmette computers sneller opmerken en hun klanten beter helpen bij de ontsmetting van hun computers. Bij Abuse Information Exchange zijn de meeste nationale internetproviders aangesloten, samen goed voor meer dan 90% van de vaste internettoegangsmarkt. Het Ministerie van Economische Zaken doet in 2014 onderzoek naar de vraag of botnetbesmettingen bij eindgebruikers in Nederland zijn afgenomen ten opzichte van landen die geen vergelijkbare initiatieven als Abuse Information Exchange hebben ontplooid. Eind 2014 zullen de uitkomsten daarvan beschikbaar zijn. Deze kunnen bruikbaar zijn voor de verbetering van de werking van Abuse HUB en van de aanpak van botnets in Nederland in het algemeen.

Opsporen en vervolgen van botnetbeheerders

Het creëren en gebruiken van een botnet is in Nederland strafbaar. De politie is belast met de opsporing, het Openbaar Ministerie is belast met de vervolging en heeft de leiding bij opsporingsonderzoeken. Botnets zijn een prioriteit voor het Team High Tech Crime (THTC) van de politie. Het THTC heeft in 2013 15 grote onderzoeken uitgevoerd. Bij het merendeel van die onderzoeken maakte een botnet deel uit van de werkwijze van de criminelen. Ook wordt door de politie bijgedragen aan gecoördineerde internationale acties tegen botnets. Botnets worden vaak aangestuurd via computers uit het buitenland. Het is mede daarom vaak lastig de identiteit en locatie van de desbetreffende crimineel te achterhalen. Indien het land waar de crimineel zich bevindt bekend is, dan kan een rechtshulpverzoek worden gedaan of kan de opsporing gezamenlijk ter hand worden genomen. Het is van belang dat het creëren en gebruiken van botnets ook

[2] Kamerstuk 29 515, nr. 331

in dat land strafbaar is en dat de autoriteiten voldoende capaciteit en expertise beschikbaar hebben om op te treden. Dat is helaas niet altijd het geval. Het kabinet zet daarom in op het versterken van de internationale samenwerking en het harmoniseren van de (straf)wetgeving. Richtlijn 2013/40 van de Europese Unie over aanvallen tegen informatiesystemen verplicht lidstaten onder meer het stellen van een bepaalde maximumstraf voor het gebruik van botnets bij bepaalde vormen van cybercrime in de strafwetgeving op te nemen. Ik heb een wetsvoorstel in procedure gebracht om de Nederlandse wetgeving in overeenstemming te brengen met deze richtlijn. Dit wetsvoorstel is thans aanhangig bij de afdeling advisering van de Raad van State.

Verstoren van de werking van botnets

Naast op het opsporen van daders, wordt ingezet op het effectief verstoren van botnets zodat burgers en bedrijven die als gevolg van een besmetting onderdeel zijn van een botnet, niet langer bloot staan aan de kwaadaardige invloed van de *comman and control server* (de centrale computer waarmee een botnet wordt aangestuurd). Bij het verstoren wordt veelal op vordering van het Openbaar Ministerie het dataverkeer van deze *command and control server* uitgeschakeld door de betrokken provider en worden de voor de opsporing relevante gegevens zeker gesteld. Verder vraagt het NCSC met enige regelmaat, bij gebleken aanwijzingen voor een botnet, nadrukkelijke aandacht hiervoor van de providers. Soms is er sprake van zogenoemde *bad hosters*. Dat zijn providers die bewust of onbewust een platform bieden aan *bad hosting*, het aanbieden van servers die onder meer gebruikt worden in botnets. In het najaar zullen politie en OM een pilot starten om *bad hosters* effectief aan te kunnen pakken. De pilot bestaat uit een samenwerking met de TU Delft om de omvang van *bad hosting* in kaart te brengen. Daarnaast worden publieke en private partners bij elkaar gebracht om tot een gezamenlijke aanpak van *bad hosters* te komen.

Rol van het NCSC

Het NCSC, als onderdeel van de NCTV van het Ministerie van Veiligheid en Justitie, vervult zijn taken ter voorkoming en beperking van verstoringen in het digitale domein in het belang van de nationale veiligheid. Het NCSC richt zich daarom op de (rijks)overheid en vitale sectoren. Als spin in het web heeft het centrum toegang tot een veelheid aan informatie over ICT-gerelateerde kwetsbaarheden en dreigingen, waaronder botnets. Wanneer het NCSC, zoals reeds geschetst in mijn brief d.d. 18 maart 2013[3] over de aanpak van het Pobelka-botnet, de beschikking krijgt over IP-adressen van computers die deel uit maken van een botnet, dan streeft het NCSC ernaar de eigenaar hiervan zo mogelijk op de hoogte te stellen. Bij vitale organisaties en (rijks)overheid gebeurt dat in de regel rechtstreeks. In andere gevallen wordt zo mogelijk samengewerkt met organisaties die op hun beurt de eigenaar op de hoogte stellen. In geval van een grootschalig cyberincident waar botnets bij betrokken zijn en dat kan leiden tot maatschappelijke ontwrichting zal het NCSC conform haar rol, met inachtneming van de bestaande publiek-private contacten en crisismanagementstructuren, de coördinatie op zich nemen voor een gezamenlijke respons. Daarbij voert het NCSC, in samenspraak met andere betrokken overheidspartijen, de eerste analyse uit van de aard van de verstoring en geeft een inschatting van de potentiële maatschappelijke gevolgen. Dit is bijvoorbeeld gebeurd bij het onderzoek naar het Pobelka

[3] Kamerstuk 26 643, nr. 268

botnet in het voorjaar van 2013, waarover ik uw Kamer per brief heb geïnformeerd[4].

Privacybescherming

Bij de activiteiten die worden ondernomen op het gebied van botnetbestrijding is het van belang om zorgvuldig om te gaan met informatiestromen, in het bijzonder daar waar het persoonsgegevens betreft. Bedrijven en overheden die persoonsgegevens verwerken moeten in beginsel aan de eisen van de Wet bescherming persoonsgegevens voldoen. Dit betekent onder meer het nemen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen, rekening houdend met de stand van de techniek en afgezet tegen de risico's die met de specifieke gegevensverwerking(en) zijn gemoeid. In specifieke gevallen kan in aanvulling hierop sectorale wet- en regelgeving van toepassing zijn. De politie verwerkt (persoons)gegevens op basis van een specifieke wet, te weten de Wet politiegegevens (Wpg). Het College bescherming persoonsgegevens is met het toezicht op de naleving en de handhaving van de Wbp en de Wpg belast.

Aansprakelijkheid

Op het punt van civielrechtelijke aansprakelijkheid geldt als uitgangspunt dat wanneer iemand als gevolg van handelen door de overheid of private partijen schade lijdt, ook als dat handelen plaatsvindt in het kader van de aanpak van botnets, in voorkomende gevallen een actie uit onrechtmatige daad kan worden gestart.

Ter afsluiting

Uit het bovenstaande wordt duidelijk dat de aanpak van botnets een samenspel van activiteiten van private en publieke partners vormt. Op 20 juni jongstleden heeft op initiatief van de Ministeries van Veiligheid en Justitie en Economische Zaken en ECP, een publiek-private bijeenkomst plaats gevonden om de aanpak van botnets te bespreken. Naar aanleiding van deze bijeenkomst is besloten tot het instellen een publiek-private botnetwerkgroep, waarin sleutelorganisaties bij botnetaanpak in Nederland vertegenwoordigd zullen zijn. ECP zal het secretariaat van deze werkgroep verzorgen. De werkgroep start na de zomer en zal voor afstemming en regie zorgen op de botnetaanpak in Nederland, kennis en informatie uitwisselen en nieuwe initiatieven ontwikkelen en aanjagen.

Hiermee is het kabinet van mening dat er een samenhangende, brede aanpak van botnets bestaat, die verder wordt uitgebouwd en verdiept. Een veiliger internet door minder botnets versterkt het vertrouwen van eindgebruikers bij het internetgebruik, geeft een impuls voor de ontwikkeling van meer online diensten en leidt tot meer economische groei. Zo wordt een bijdrage geleverd aan een samenleving waarin de kansen die digitalisering ons biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.

De Minister van Veiligheid en Justitie,
I.W. Opstelten

---

[4] Kamerstuk 26 643, nr. 272