Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2502

Vragen van de leden **Rajkowski** en **Brekelmans** (beiden VVD) aan de Ministers van Justitie en Veiligheid en van Buitenlandse Zaken over *berichten omtrent cyberaanvallen op Oekraïne en Nederlandse servers* (ingezonden 24 februari 2022).

Antwoord van Minister Yeşilgöz-Zegerius (Justitie en Veiligheid) (ontvangen 21 april 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2109.

Vraag 1
Bent u bekend met bovenstaande berichtgeving?[1]

Antwoord 1
Ja.

Vraag 2
Bent u ervan op de hoogte dat Nederlandse servers worden misbruikt door Rusland om cyberaanvallen uit te voeren in Oekraïne? Hoe beoordeelt u dit?

Antwoord 2
Het is bekend dat Nederlandse servers en infrastructuur misbruikt worden door criminelen voor het plegen van strafbare feiten, zoals DDoS- en ransomware-aanvallen. Dit is onwenselijk. Nederland heeft in vergelijking met andere EU-landen een relatief grote hosting sector. Dit heeft te maken met de uitstekende digitale infrastructuur waarover Nederland beschikt: het internet is betrouwbaar en snel. Zowel nationaal als internationaal maken personen, bedrijven en organisaties gebruik van de Nederlandse infrastructuur. Naast legitieme klanten, kunnen criminelen en andere kwaadwillenden misbruik maken van de Nederlandse hostingsector. De hostingprovider is zich hier niet altijd van bewust. Daarnaast bestaan er zogenaamde «bulletproof» hosters, die hun klanten willens en wetens faciliteren bij hun strafbare gedrag. Verder ziet Nederland het zorgvuldigheidsbeginsel als een verplichting binnen het

[1] NRC, 22 februari 2022, Cyberaanvallen op Oekraïne aangestuurd via Nederland (https://www.nrc.nl/nieuws/2022/02/22/cyberaanvallen-op-oekraine-aangestuurd-via-nederland-a4093039). BNR, 17 februari 2022, Nederlandse server betrokken bij cyberaanval Oekraine (https://www.bnr.nl/nieuws/technologie/10467810/nederlandse-server-betrokken-bij-cyberaanval-oekraine-offline-bedrijf-hostte-eerder-extreemrechtse-vizier-op-links).

ah-tk-20212022-2502
ISSN 0921 - 7398
's-Gravenhage 2022

internationaal recht. Zie hiervoor verder de kamerbrief Tegenmaatregelen ransomware-aanvallen van de Minister van Buitenlandse Zaken.[2]

Vraag 3
Hoeveel Nederlandse servers zijn de afgelopen weken misbruikt vanuit Rusland om cyberaanvallen uit te voeren? Heeft u een beeld om welke servers het gaat? Zo ja, zijn er stappen genomen om deze servers uit de lucht te halen? Zo nee, waarom niet?

Antwoord 3
Dergelijke digitale aanvallen worden uitgevoerd vanuit command-and-control servers. Deze staan wereldwijd in datacenters, waaronder ook in Nederland. Voor datacenters is het vrijwel onmogelijk om te controleren welke servers voor dergelijke malafide doeleinden worden ingezet. Voor elke aanval zou specifiek technisch onderzoek nodig zijn om te achterhalen via welke servers een aanval is uitgevoerd. Dergelijk technisch onderzoek is niet bij elke aanval mogelijk, vanwege de capaciteit die dit kost en gezien het aantal (pogingen tot) aanvallen.

Vraag 4
Klopt het dat Rusland ongezien Nederlandse servers kon huren voor zijn activiteiten en zo ongestoord cyberaanvallen kon uitvoeren op Oekraïne? Zo ja, in hoeverre worden huurders gescreend bij hostingbedrijven door hostingbedrijven zelf? Zijn hostingbedrijven verplicht om huurders te screenen? Zo ja, gebeurt dit ook en hoe vindt de controle plaats dat dit ook gebeurt? Zo nee, waarom niet?

Antwoord 4
Wie precies de servers heeft gehuurd voor de genoemde activiteiten is niet bekend. Het screenen van klanten door hostingproviders is geen wettelijke verplichting. Het gaat hier om private bedrijven, waarop in Nederland contractvrijheid van toepassing is. Zij mogen in beginsel zelf bepalen wie hun klanten zijn. Door de hostingsector is samen met het Ministerie van EZK een gedragscode opgesteld, om misbruik van hun servers tegen te gaan. Op EU-niveau heeft Nederland in het kader van de gesprekken over de Digital Services Act (DSA) gepleit voor het hierin opnemen van regels voor hostingproviders om crimineel misbruik te bemoeilijken, waaronder het vergaren van informatie over klanten. Hiervoor was onvoldoende steun.

Vraag 5
Welke rol speelt de politie in het screenen van huurders van hostingbedrijven? Wanneer screent de politie huurders van hostingbedrijven? Zijn hostingbedrijven verplicht om servers offline te halen als de politie hier melding van maakt? Zo ja, is dit ook afgelopen weken gebeurd? Zo nee, waarom niet?

Antwoord 5
Zoals bij vraag 4 is aangegeven, zijn hosters niet wettelijk verplicht om hun klanten te screenen. De politie heeft geen wettelijke bevoegdheden om klanten van hostingproviders te screenen. Daarnaast is het screenen van klanten een toezichtstaak die niet bij de politie thuis hoort. Bij vermoedens van illegale activiteiten op een server kan bij een hostingprovider een verzoek worden gedaan voor een vrijwillige notice-and-takedown. Indien de hoster daar geen gehoor aan geeft, kan de officier van justitie ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten een dienstverlener bevelen gegevens ontoegankelijk te maken (artikel 125p Wetboek van Strafvordering (Sv)) sturen naar een hostingprovider. Wanneer cybercriminelen gebruik maken van servers gehuurd bij buitenlandse *resellers* kan het doen van vorderingen worden bemoeilijkt, en daarmee het opsporingsonderzoek en het beëindigen van strafbare feiten.
Indien de politie weet heeft van strafbare feiten die via Nederlandse servers gepleegd worden, kan een opsporingsonderzoek worden gestart. Dit zal zich in beginsel richten op de plegers van strafbare feiten, zoals de daders van

[2] Kamerbrief Tegenmaatregelen ransomware-aanvallen, d.d. 6 oktober 2021.

een ransomware-aanval. Het opsporingsonderzoek kan zich ook richten op de hostingprovider of de reseller, mits zij worden verdacht van een strafbaar feit.

Vraag 6
Bent u het met de VVD-fractie eens dat het ongebreideld door kunnen verhuren van hostingruimte door resellers het wel erg makkelijk kan maken voor kwaadwillenden om een online rookgordijn te creëren? Zo ja, wat wilt u hieraan doen en welke mogelijkheden hebben hostingbedrijven en politie om gegevens over resellers op te vragen? Zo nee, waarom niet?

Antwoord 6
Het is onwenselijk dat kwaadwillenden Nederlandse servers misbruiken voor bijvoorbeeld het plegen van cyberaanvallen. De hostingsector heeft de gedragscode «abuse-bestrijding» ontwikkeld, die als doel heeft het schoon en veilig houden van het Nederlandse internet. Hierin is onder meer opgenomen dat hosters hun klanten kennen. Het blijft echter mogelijk dat klanten van hostingproviders deze serverruimte weer doorverhuren. Verder deelt het Clean Networks Initiatief[3] onder deelnemers geautomatiseerd actuele informatie over kwetsbaarheden en misbruik in de systemen van alle deelnemers, geprioriteerd op basis van urgentie en impact. Daarnaast is in 2020 het Anti Abuse Netwerk (AAN) opgericht. Deze coalitie van publieke en private partijen zet zich in voor de bestrijding van misbruik van de technische infrastructuur.
Recentelijk heeft de politie een lijst opgesteld met resellers die vaak laten doorschemeren of openlijk toegeven dat zij diensten leveren aan criminelen. Deze lijst is gedeeld met de Dutch Cloud Community (DCC). Zie hiervoor ook de beantwoording van de Kamervragen van het lid Rajkowski.[4] Naar aanleiding van deze beantwoording heeft DCC laten weten dat een aantal leden met bepaalde klanten geen zaken meer doet.[5]
Momenteel is in EU-verband de triloog-fase van de Digital Services Act begonnen. Deze verordening dient onder meer ter vernieuwing van de huidige E-Commerce richtlijn. In het voorstel worden hostingaanbieders onder andere verplicht een toegankelijk notificatiemechanisme in te stellen waarbij illegale inhoud gemeld kan worden en wordt verduidelijkt dat hostingproviders hun beperking van aansprakelijkheid kunnen verliezen wanneer zij na een melding van illegale inhoud deze niet prompt verwijderen of ontoegankelijk maken. Het kabinet steunt de invoering van deze maatregelen.

Vraag 7
Bent u het met de VVD-fractie eens dat het zeer zorgelijk is dat onze uitstekende digitale infrastructuur wordt misbruikt door landen als Rusland om cyberaanvallen uit te voeren op Oekraïne en dat Nederland daarmee onbewust en indirect de Russische aanval faciliteert? Zo ja, bent u bereid om hostingbedrijven strenger te controleren al dan niet via de politie? Zo nee, waarom niet?

Antwoord 7
Het is zeer onwenselijk dat Nederlandse infrastructuur wordt misbruikt voor het plegen van cyberaanvallen. Dit geldt ook in het geval van kwaadwillende cyberoperaties tegen Oekraïne. Zoals eerder is aangegeven zijn hostingbedrijven niet wettelijk verplicht om hun klanten te controleren. Het controleren van hostingbedrijven is bovendien geen taak van de politie. Bij het tegengaan van misbruik van Nederlandse netwerken blijft het belangrijk dat de samenwerking wordt gezocht tussen de hostingsector en de politie.

---

[3] www.cleannetworks.net.
[4] Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2257.
[5] Hosting-bedrijven stoppen met aantal foute resellers | Computable.nl.