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

2257

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Criminelen gebruiken foute hostingbedrijven voor activiteiten vanuit Nederland»* (ingezonden 15 februari 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 29 maart 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1975.

Vraag 1
Bent u bekend met het bericht «Criminelen gebruiken foute hostingbedrijven voor activiteiten vanuit Nederland»?[1]

Antwoord 1
Ja.

Vraag 2
In november waarschuwde de politie al voor 70 mogelijk malafide bedrijven die serverruimte doorverhuren aan criminelen, waar komen deze malafide bedrijven vandaan? Welke acties zijn daarna ondernomen tegen deze malafide bedrijven?

Antwoord 2
De politie geeft aan dat het om buitenlandse bedrijven gaat die gebruik maken van de Nederlandse infrastructuur. Bedrijven die serverruimte doorverhuren worden «resellers» genoemd. Deze resellers huren serverruimte van een in Nederland gevestigde hostingprovider, waarna ze deze doorverhuren aan een klant. Deze klanten kunnen personen zijn die een reguliere website willen laten draaien, maar dit kunnen ook cybercriminelen zijn die de zich in Nederland bevindende server misbruiken voor strafbare feiten. Op basis van openbaar toegankelijke informatie, zoals bepaalde internetfora, heeft de politie een lijst opgesteld van resellers die vaak laten doorschemeren of openlijk toegeven dat zij diensten leveren aan criminelen. Deze lijst is gedeeld met de leden van de brancheorganisatie van hostingproviders, de Dutch Cloud Community (DCC). Aan hen is gevraagd of zij deze

[1] NOS, 12 februari 2022, «Criminelen gebruiken foute hostingbedrijven voor activiteiten vanuit Nederland», https://nos.nl/artikel/2416934-criminelen-gebruiken-foute-hostingbedrijven-voor-activiteiten-vanuit-nederland.

ah-tk-20212022-2257
ISSN 0921 - 7398
's-Gravenhage 2022

resellers in hun klantenbestand hebben. Het is aan deze hostingproviders om eventueel actie te ondernemen op basis van deze lijst.

Vraag 3
Welke acties hebben hostingbedrijven uitgevoerd nadat de politie deze waarschuwing heeft verstuurd? Heeft de politie contact gehouden met de hostingbedrijven om te checken of hostingbedrijven wat met deze waarschuwing hebben gedaan?

Antwoord 3
De politie heeft DCC gevraagd naar hun ervaring met deze actie. DCC heeft aangegeven dat zij en haar leden overwegend positief zijn, met name over het feit dat de politie een dergelijke lijst heeft opgesteld en als waarschuwing heeft gedeeld. De hostingproviders hebben geen mededelingen gedaan over het al dan niet handelen naar aanleiding van de lijst.

Vraag 4
Zijn de tientallen criminele activiteiten die afgelopen maanden via de netwerken van bedrijven zijn ondernomen, zoals blijkt uit het onderzoek van Pointer en Spamhaus, bekend bij de politie? Zo ja, welke acties zijn hiertegen ondernomen?

Antwoord 4
Het feit dat misbruik wordt gemaakt van de Nederlandse infrastructuur is al langere tijd bekend bij de politie. De politie richt zicht binnen de opsporingsonderzoeken die zij uitvoeren onder meer op hostingbedrijven die bewust criminaliteit faciliteren. Daarop zijn reeds meerdere strafzaken gestart. Zoals ook in de beantwoording van Kamervragen van het lid Van Nispen[2] is aangegeven, is het strafrechtelijk vervolgen van hostingproviders lastig. Het opsporen en vervolgen van buitenlandse resellers is mogelijk nog complexer indien hiervoor samenwerking nodig is met een land waarmee Nederland geen of geen goede rechtshulprelatie heeft. De politie en het OM werken daarom niet alleen aan opsporing en vervolging, maar bijvoorbeeld ook aan slachtoffernotificatie en samenwerking met private partijen om de criminele activiteiten te verstoren.

Vraag 5
Om wat voor type criminele activiteiten gaat het in deze gevallen? Kunt u een inschatting maken van de schade die is toegebracht door de criminelen?

Antwoord 5
De politie geeft aan dat de resellers verschillende typen cyberdelicten faciliteren, zoals computervredebreuk, phishing-campagnes en ransomware-aanvallen. Vanwege het ontbreken van kwantitatieve gegevens en de lage aangiftebereidheid van cybercrimedelicten is een betrouwbare inschatting van de schade niet beschikbaar.

Vraag 6
Op welke manier werken hostingbedrijven en de politie samen om dit soort praktijken te voorkomen? Kan deze samenwerking verstevigd worden? Is het op een directe, dan wel indirecte manier mogelijk om hostingbedrijven aansprakelijk te stellen voor het verhuren van serverruimte aan malafide bedrijven?

Antwoord 6
De politie is deelnemer aan het Anti Abuse Netwerk (AAN). Deze coalitie van publieke en private partijen zet zich in voor de bestrijding van misbruik van de technische infrastructuur. Daarnaast wordt in individuele opsporingsonderzoeken waar nodig in contact getreden met hostingproviders.
In de huidige situatie zijn hostingproviders op grond van Europese regelgeving en de Nederlandse implementatie daarvan onder voorwaarden niet aansprakelijk voor de gedragingen van hun klanten, waaronder (klanten van) resellers. De beperking van aansprakelijkheid voor hostingproviders die wordt

[2] Aanhangsel van Handelingen, vergaderjaar 2020–2021, nr. 2608.

geregeld in artikel 14 van de E-Commerce-richtlijn, is geïmplementeerd in artikel 54a Sr. Artikel 54a Sr stelt dat hostingproviders in beginsel niet vervolgd kunnen worden vanwege wederrechtelijk materiaal dat door klanten op hun servers wordt geplaatst, indien zij doen wat redelijkerwijs van hen gevergd kan worden wanneer ze op bevel van de officier van justitie (125p Sv) gegevens ontoegankelijk moeten maken. Een bevel om een dienst ontoegankelijk te maken is gericht op individuele inhoud en niet op de hostingprovider als zodanig. Het voorkomt niet dat een hostingprovider opnieuw (dezelfde) klanten toelaat die wederrechtelijk materiaal plaatsen op de servers van de hostingproviders.

Vraag 7
Bent u het ermee eens dat het niet uit te leggen is dat via Nederlandse servers buitenlandse criminelen makkelijk hun gang kunnen gaan om vervolgens ernstige criminele activiteiten te plegen? Op welke manier kunt u ervoor zorgen dat malafide bedrijven minder kans krijgen om serverruimte van Nederlandse hostingbedrijven te kopen?

Antwoord 7
Het is belangrijk om ervoor te zorgen dat het Nederlandse netwerk veilig is en niet misbruikt wordt door criminelen. 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 notificatie-mechanisme 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.
De hostingsector heeft zelf reeds initiatieven ontplooid om het misbruik van Nederlandse netwerken tegen te gaan, zoals het eerdergenoemde Anti-Abuse Netwerk. Daarnaast heeft de hostingsector zelf een gedragscode «abuse-bestrijding» ontwikkeld, die als doel heeft het schoon en veilig houden van het Nederlandse internet. Hierin is ook opgenomen dat hosters hun klanten kennen. 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.

[3] www.cleannetworks.net.