



> Retouradres Postbus 20301 2500 EH Den Haag

Aan

de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018 2500 EA
DEN HAAG

Datum 8 maart 2023
Onderwerp Terugkoppeling *reseller*-actie

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**

Directie Rechtshandhaving en
Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
4537140

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Criminelen op internet kunnen hostingdiensten misbruiken voor hun illegale activiteiten. Hostingproviders weten vaak niet welke klanten hun diensten misbruiken. Bovendien kunnen klanten de dienstverlening doorverkopen. Er is dan sprake van zogenaamde *resellers*. Dit doorverkopen is niet verboden. Wel kan het het zicht op mogelijke criminele activiteiten verder verminderen. Op 12 oktober jl. heeft de politie een brief aan Nederlandse hostingproviders gestuurd, waarin zij adviseert een eventuele overeenkomst met bepaalde specifieke *resellers* te herzien. De politie heeft op basis van openbare bronnen geconstateerd dat deze *resellers* zichzelf afficheren als dienstverleners die bereid zijn criminaliteit te faciliteren. Tijdens het vragenuur van 22 november jl. heb ik toegezegd terug te koppelen hoe deze actie heeft uitgedaakt en of aanvullende maatregelen wenselijk zijn.

Naar aanleiding van reacties van geadresseerden van een eerdere soortgelijke brief van de politie van 17 november 2021 heeft de politie de brief van afgelopen oktober gericht naar specifieke hostingproviders gestuurd en zijn specifieke *resellers* genoemd. De aangeschreven hostingproviders hebben naar aanleiding van een vragenlijst van de politie niet direct teruggekoppeld hoeveel malafide *resellers* er in hun klantenbestand waren opgenomen. Het betreft bedrijfsgevoelige informatie die zij niet specifiek wensen te delen. Wel heeft de brancheorganisatie *Dutch Cloud Community* gemeld dat enkele hostingproviders naar aanleiding van de brief van de politie actie hebben ondernomen richting in de brief genoemde *resellers*. Ook zijn er gesprekken tussen de politie en *Dutch Cloud Community* over mogelijkheden om signalen over malafide *resellers* structureel met hostingproviders te delen.

Naast het versturen van de genoemde brief hebben de politie en het Openbaar Ministerie enkele oplossingsrichtingen verkend om het leveren van hostingdiensten voor criminele doeleinden tegen te gaan. De belangrijkste daarvan zijn hieronder weergegeven. Deze oplossingsrichtingen zijn nog niet volledig uitgewerkt en verdienen nadere bestudering.

Een eerste richting betreft het ondersteunen van de sector met informatie over criminele handelingen. De Stichting Nationale Beheersorganisatie Internet Providers werkt samen met het Ministerie van Justitie en Veiligheid aan het project Cleannetworks. Dit project beoogt het opzetten van een systeem om hostingproviders structureel te informeren over actuele criminele handelingen en

kwetsbaarheden. Hierdoor kunnen zij deze activiteiten op hun eigen netwerken tegengaan en zich beveiligen tegen dreigingen. Het Ministerie van Justitie en Veiligheid ondersteunt het project financieel. Tevens is financiering uit het *Internal Security Fund* van de Europese Unie voorzien.

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving** Directie
Rechtshandhaving en
Criminaliteitsbestrijding

Met de wetwijziging van de Wet beveiliging netwerk- en informatiesystemen van 1 december 2022 kan de Stichting Nationale Beheersorganisatie Internet Providers als schakelorganisatie informatie over dreigingen en incidenten ontvangen van het Nationaal Cyber Security Centrum ten behoeve van hun achterban. In het kader van het project Cleannetworks wordt bezien of de informatievoorziening versterking behoeft.

Datum
16 maart 2023

Ons kenmerk4537140

Een tweede richting betreft het als Rijksoverheid geven van het goede voorbeeld door zelf te kiezen voor verantwoorde leveranciers van hostingdiensten. Daarvoor wordt de publiek-privaat opgestelde Gedragscode Abusebestrijding betrokken bij de inkoop van hostingdiensten voor de Rijksoverheid. Uitgangspunt is dat de opdrachtnemer de gedragscode onderschrijft en is aangesloten bij het publiek-private Anti Abuse Netwerk. Momenteel wordt bezien of dit breder navolging kan krijgen. In het kader van het project Cleannetworks wordt bovendien een keurmerk ontwikkeld, wat de keuze voor verantwoorde leveranciers kan ondersteunen.

Een derde richting betreft aanpassing van de wettelijke kaders. Voor hostingproviders die willens en wetens criminaliteit faciliteren kan een strafrechtelijke aanpak passend zijn. In 2022 heeft het Gerechtshof in Den Haag bepaald dat dergelijke dienstverleners onder omstandigheden niet zijn uitgesloten van strafrechtelijke aansprakelijkheid, ook niet als zij geen bevel tot ontoegankelijk maken van gegevens hebben ontvangen. Deze uitspraak biedt mogelijkheden voor vervolging van hostingproviders die criminelen actief helpen. Aanpassing van het Wetboek van Strafrecht hiervoor is daarom op dit moment niet voorzien.

Het Ministerie van Economische Zaken en Klimaat werkt momenteel aan de uitvoeringswetgeving voor de Digitale Dienstenverordening (*Digital Services Act*). Op dit moment wordt bezien of naar aanleiding van de uitspraak van het Gerechtshof in Den Haag verheldering van de grenzen van de uitsluiting van aansprakelijkheid in de Memorie van Toelichting bij het wetsvoorstel wenselijk is. Bovendien wordt bezien hoe de dienstverlening van *resellers* zich verhoudt tot de definitie van een aanbieder van hostingdiensten in de verordening. Waar deze definitie van toepassing is, zullen ook zij aan de verordening moeten voldoen. In dit kader wordt ook aandacht besteed aan de kwalificatie van malware.

Er zijn *resellers* die zowel malafide domeinen registeren als hostingdiensten aanbieden. De nieuwe Netwerk- en Informatiebeveiligingsrichtlijn verplicht entiteiten die domeinnaamregistratiediensten aanbieden om accurate domeinnaamregistratiegegevens (zoals e-mailadres en telefoonnummer van de afnemer van de dienst) bij te houden. Indien deze domeinnaamgegevens worden bijgehouden, kunnen de politie en het Openbaar Ministerie deze in het kader van een opsporingsonderzoek vorderen.

De hierboven genoemde oplossingsrichtingen worden de komende periode samen met de politie en het Openbaar Ministerie nader bestudeerd. Het tegengaan van het faciliteren van criminaliteit door hostingproviders is daarnaast een aandachtspunt voor de hostingproviders zelf. Veel hostingproviders treden hier

adequaaf tegen op. Het is van belang dat alle hostingproviders hier maatregelen tegen nemen. Aandacht vanuit zowel de overheid als de betrokken marktpartijen blijft nodig.

De Minister van Justitie en Veiligheid,

D. Yeşilgöz-Zegerius

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving** Directie
Rechtshandhaving en
Criminaliteitsbestrijding

Datum
16 maart 2023

Ons kenmerk4537140