Verkenning aanpak bad hosting

De Nederlandse hostingsector is groot en divers. Het heeft een goede naam door de snelle internetverbindingen in Nederland, de hoeveelheid datacenters en servers en de goede service die geleverd wordt. Naast de vele voordelen die dat biedt voor legale activiteiten betekent dat helaas ook dat criminaliteit ermee kan worden gefaciliteerd. Dit wordt door de hostingsector ook erkend en in het kader van zelfregulering zijn al afspraken gemaakt om de sector zo schoon mogelijk te krijgen en te houden. Maar net als in de offline wereld zijn er ook partijen die zich van dergelijke afspraken weinig aantrekken: er zijn malafide hostingbedrijven die bewust criminaliteit faciliteren (bulletproof hosting) dan wel onwetende hostingbedrijven die zeer weinig maatregelen nemen ter preventie van criminaliteit (bad hosting). De problematiek rondom bulletproof en bad hosting is in 2022 al aan de kaak gesteld door een bestuurlijk advies dat afgegeven is door de politie en het Openbaar Ministerie (OM) aan de ministeries van Justitie en Veiligheid, Economische Zaken en Financiën. In maart 2025 is door de veiligheidsdriehoek van Amsterdam ook een brief naar het kabinet verzonden om aandacht te vragen voor de problematiek. Het kabinet erkent de problemen en ziet dat er noodzaak is om bulletproof en bad hosters beter aan te kunnen pakken.

Hostingproviders weten vaak niet precies *welke* klanten hun diensten misbruiken voor criminele activiteiten. Bovendien kunnen klanten de dienstverlening doorverkopen. Er is dan sprake van zogenaamde reseller-constructie. Dit kan de opsporing en vervolging extra complex maken; een klant kan immers doorverkopen aan een klant, die het weer verder kan verkopen aan een andere klant en zo verder. Hoe een reseller-constructie ongeveer in elkaar steekt is hieronder in figuur 1 aangegeven.

Fig.1 Reseller-constructie

De minister van Justitie en Veiligheid heeft tijdens het commissiedebat cybercrime van 24 oktober 2024 de toezegging gedaan om samen met de minister van Economische Zaken te kijken naar de problematiek rondom bulletproof en bad hosting met specifieke aandacht voor *resellers* en te verkennen welke oplossingen hiervoor mogelijk zijn. Hierbij is expliciet aandacht gegeven aan de vraag of de verplichting voor een zogenaamd 'Know your customer' - beleid (hierna: KYC-beleid) een mogelijkheid is.

Aanpak

De verkenning is uitgevoerd door het ministerie van Justitie en Veiligheid om een zo breed mogelijk beeld te hebben en krijgen van de sector, de problematiek en kansrijke oplossingsrichtingen die door het kabinet verder verkend zullen worden. Hiervoor zijn verschillende gesprekken gevoerd met partijen binnen en buiten de Rijksoverheid, van sector tot handhaving. Ook is er een vragenlijst uitgestuurd naar Europese collega's om te inventariseren of de problematiek van bulletproof en bad hosting ook in andere jurisdicties herkend wordt.

Volgende stappen

Uit de verkenning vloeien een aantal kansrijke mogelijke oplossingen voort die het kabinet het komende jaar graag verder uit wil werken. Hier zal de Kamer in 2026 verder over worden geïnformeerd. De problematiek, huidige situatie en mogelijke oplossingen worden hieronder nader toegelicht.

1) Bestaande wet- en regelgeving

Het probleem van bulletproof en bad hosters is niet nieuw en verschillende wetgeving is al van toepassing of treedt binnenkort in werking. Hieronder worden kort de strafrechtelijke en bestuursrechtelijke mogelijkheden toegelicht die reeds bestaan om de problematiek aan te pakken.

Strafrecht

Hosting partijen – die in principe een tussenhandelsfunctie vervullen – zijn in principe niet verantwoordelijk voor hetgeen er op hun servers worden geplaatst. Dat zijn in eerste instantie hun klanten zelf. Uitzondering hierop is dat, op het moment dat de hosters op de hoogte worden gebracht van illegale activiteiten/content, zij dit wel dienen te verwijderen. In deze gevallen is artikel 54a Wetboek van Strafrecht (Sr) van toepassing. In artikel 54a Sr is gevolg gegeven aan de voorwaardelijke aansprakelijkheidsvrijstelling uit de Richtlijn inzake elektronische handel door middel van een vervolgingsuitsluitingsgrond. Deze regeling is gehandhaafd in de uitvoeringswet voor de digitaledienstenverordening. De regeling komt op het volgende neer: indien een strafbaar feit wordt begaan met gebruikmaking van een communicatiedienst, is strafrechtelijke vervolging van de tussenpersoon als zodanig uitgesloten indien hij voldoet aan een bevel tot ontoegankelijkmaking als bedoeld in artikel 125p van het Wetboek van Strafvordering (Sv) of een beslissing tot verwijdering als bedoeld in artikel 3, eerste lid, van de Verordening terroristische online-inhoud of een bevel tot ontoegankelijkmaking als bedoeld in artikel 6, eerste lid, van de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal. Voldoet een tussenpersoon hier *niet* aan dan is aansprakelijkheid niet uitgesloten en kan vervolging mogelijk zijn.

Dit heeft als gevolg dat kwaadwillende hosters zijn gevrijwaard van vervolging op het moment dat zij *wel* voldoen aan een bevel 125p. Een vervolging voor medeplegen/medeplichtigheid is daarom lastig, omdat er in een vrij vroeg stadium van een strafrechtelijk onderzoek aanwijzingen moeten zijn dat de hoster actief bijdraagt aan de strafbare feiten en/of deze bewust faciliteert. In een dergelijk geval is het proportioneel dat het OM niet eerst een vordering 125p uitvaardigt, waardoor de kwaadwillende hoster (vertraagd) de content kan verwijderen en daarmee gevrijwaard wordt van vervolging.[1]

Dit principe is recent bekrachtigd door een uitspraak van de Rechtbank Rotterdam over het medeplegen van medeplichtigheid aan computervredebreuk en medeplichtigheid aan medeplegen van het voorhanden hebben en verspreiden van een Mirai botnet.[2] De rechtbank oordeelde dat de verdachte en de medeverdachten door het ter beschikking stellen van servers en IP-adressen zich schuldig hebben gemaakt aan het faciliteren van een Mirai botnet-infrastructuur waarvan cybercriminelen gebruik konden maken om onder meer DDoS-aanvallen uit te voeren. In deze zaak was er geen sprake van een bevel op grond van 125p Sv, maar werd de tussenpersoon desondanks veroordeeld omdat duidelijk was dat hij kennis had van de illegale activiteit op zijn netwerk.

Bestuursrecht

Bulletproof of bad hosters kunnen ook via de bestuursrechtelijke weg worden aangepakt. De digitaledienstenverordening, die sinds februari 2024 van toepassing is, biedt hier handvaten voor. In Nederland wordt uitvoering gegeven aan de verordening door middel van de uitvoeringswet digitaledienstenverordening, die in februari 2025 in werking is getreden. In deze wet worden de bevoegde nationale autoriteiten aangewezen die bij niet-naleving van de digitaledienstenverordening handhavend kunnen optreden jegens in Nederland gevestigde tussenhandeldiensten. De digitaledienstenverordening bevat enerzijds een kader voor (de uitsluiting van) de aansprakelijkheid van aanbieders van tussenhandeldiensten, waaronder hostingproviders, voor informatie die door hun gebruikers wordt verstrekt en anderzijds een aantal zorgvuldigheidsverplichtingen waar deze aanbieders aan moeten voldoen bij het verlenen van hun diensten. Het aansprakelijkheidskader voor tussenhandeldiensten harmoniseert de voorwaarden op grond waarvan deze aanbieders niet aansprakelijk zijn voor informatie van derden die zij opslaan of doorgeven. Om een beroep te kunnen doen op de aansprakelijkheidsvrijstelling voor hostingdiensten mag de aanbieder niet daadwerkelijk kennis hebben van illegale inhoud die zijn klanten bij hem opslaan en moet hij, wanneer hij die kennis wel krijgt, prompt handelen om die inhoud te verwijderen of ontoegankelijk te maken. Voor een beroep op de vrijstelling is vereist dat dat de dienstverlener geen actieve rol speelt ten aanzien van de informatie die hij opslaat of doorgeeft, waardoor hij kennis heeft van of controle heeft over die inhoud. Overweging 20 bij de verordening verduidelijkt dat de vrijstelling niet van toepassing is wanneer een aanbieder opzettelijk samenwerkt met een afnemer om illegale activiteiten te ontplooien. Een dergelijke

[1] ECLI:NL:GHDHA:2022:1550, Gerechtshof Den Haag, 23 augustus 2022.
[2] ECLI:NL:RBROT:2025:2488; Rechtbank Rotterdam, 21 februari 2025.

dienstverlener verricht immers geen neutrale dienst. Van bulletproof hosters is duidelijk dat zij opzettelijk samenwerken met een afnemer om illegale activiteiten te ontplooien en uit dien hoofde geen beroep kunnen doen op de vrijstelling van aansprakelijkheid. Bij onwetende hostingbedrijven die zeer weinig maatregelen nemen (bad hosting), hangt het van de omstandigheden van het geval af of gesteld kan worden dat zij opzettelijk samenwerken met een afnemer om illegale activiteiten te ontplooien. Het uiteindelijke oordeel daarover is aan de rechter. Hoewel het in de praktijk uitdagend kan zijn om in cybercrimezaken opzet op samenwerking tot het ontplooien van illegale activiteiten of het hebben van kennis van de illegale activiteiten op het netwerk aan te tonen, kan de digitaledienstenverordening van grote toegevoegde waarde zijn voor de aanpak van bulletproof en bad hosters. Naast de regels over aansprakelijkheid, zijn onder meer de verplichting voor alle aanbieders van tussenhandeldiensten om centrale contactpunten in te stellen (artikel 11), wettelijke vertegenwoordigers aan te stellen als zij gevestigd zijn buiten de EU (artikel 13), de verplichting om te rapporteren over inhoudsmoderatie (artikel 15) en de verplichting om te voorzien in kennisgevings- en actiemechanismen (artikel 16) in dit kader relevant.

De handhaving van de digitaledienstenverordening in Nederland is hoofdzakelijk belegd bij de Autoriteit Consument en Markt (ACM). De ACM is als Nederlandse digitale diensten coördinator bevoegd om de DSA te handhaven ten aanzien van bedrijven die in Nederland een hoofdvestiging of een wettelijke vertegenwoordiger hebben. Wanneer dit in andere lidstaten is, is de digitaledienstencoördinator van die lidstaat bevoegd. De ACM richt zich ook op rol van webhostingdiensten in het tegengaan van illegale inhoud op het internet. Webhostingdiensten spelen een centrale rol in de verspreiding van informatie op het internet. Iedere aanbieder van een website maakt gebruik van een webhostingdienst om een website op het internet te plaatsen. De ACM onderzoekt en treedt indien nodig handhavend op tegen webhosters die hun verantwoordelijkheid niet nemen met betrekking tot het tegengaan van illegale inhoud.[3] Het is voor deze taak van belang dat er goede samenwerking is met andere handhavers die zicht hebben op de hostingsector, zoals de politie, het OM en de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM). Recent is er daarom een samenwerkingsovereenkomst getekend tussen de ACM en elf andere handhavers.[4]

De ATKM kan op basis van de uitvoeringswet verordening terroristische online inhoud (TOI) en de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal bevelen aan hostingbedrijven doen uitgaan ter ontoegankelijkmaking of verwijdering van online terroristisch materiaal en online materiaal van seksueel kindermisbruik. Bulletproof en bad hosters die klanten faciliteren voor dit specifieke online illegale materiaal kunnen boetes worden opgelegd indien zij niet voldoen aan de bevelen van de ATKM.

Andere nieuwe instrumenten die relevant zijn voor de hostingsector zijn de Network and Information Security regulation (NIS2-verordening) en de Network and Information Security Directive (NIS2-richtlijn). Deze worden in Nederland geïmplementeerd via de Wet beveiliging netwerk- en informatiesystemen en de Cyberbeveiligingswet (Cbw). Met de implementatie van deze wetgeving moeten de organisaties die hieronder vallen aan strengere cybersecuritymaatregelen voldoen. In bepaalde gevallen geldt er ook een meldingsplicht van incidenten. Hostingdiensten die binnen de reikwijdte van de Cbw vallen moeten hier uiteraard ook aan voldoen. Daarnaast vallen entiteiten die domeinnaamregistratiediensten aanbieden ook onder de Cbw. Dit kunnen ook partijen zijn die hostingdiensten aanbieden. Voor hen geldt er met de implementatie van de NIS2 de verplichting om bepaalde gegevens van domeinnaamregistratiediensten bij te houden in een database.

2) Overzicht van de sector

Een van de uitdagingen in de aanpak van bulletproof en bad hosters is dat er geen eenduidig beeld is van de sector. Er bestaan verschillende soorten tussenpersonen die verschillende soorten hostingdiensten leveren. Daarom is het van belang om beter onderscheid te kunnen maken op basis van de activiteiten en aangeboden diensten van een dienstverlener.

[3] https://www.acm.nl/system/files/documents/focus-op-digitale-economie-2025.pdf
[4] https://www.acm.nl/nl/publicaties/acm-tekent-samenwerkingsprotocol-over-dsa-met-elf-organisaties

In de digitaledienstenverordening wordt een hostingdienst gedefinieerd als een tussenhandeldienst die bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, op diens verzoek. Deze definitie omvat niet alleen traditionele Cloud computing- en webhostingdiensten of andere pure opslagdiensten, maar strekt zich blijkens de digitaledienstenverordening ook uit tot online platforms die informatie van afnemers opslaan en verspreiden bij het publiek. Hieronder vallen sociale media, reviewplatforms, discussiefora of webwinkels. Het verkrijgen van een eenduidig beeld van de hostingmarkt en de verschillende geleverde diensten is van belang voor het bepalen van de mate van aansprakelijkheid en welke wet- en regelgeving op de betreffende dienstverlener van toepassing is.

Om een duidelijker beeld te krijgen van tussenhandeldiensten die in Nederland zijn gevestigd, en of zij zijn aan te merken als hostingdienst en vervolgens welke mate van aansprakelijkheid dan van toepassing is, wordt geprobeerd om de zogenaamde SBI-codes voor de sector aan te scherpen door middel van het toevoegen van een vijfde cijfer op nationaal niveau. SBI staat voor Standaard Bedrijfsindeling en bestaat uit vier of vijf cijfers en geeft aan wat de activiteit van een bedrijf of organisatie is. Bedrijven worden met een dergelijke code in het Handelsregister geregistreerd. Door ontwikkeling in onder andere de IT-sector wordt de SBI in 2025 vernieuwd. Ondanks de invoering van de nieuwe SBI-codes geeft de code die van toepassing is op de hostingsector onvoldoende beeld op de sector voor de sector zelf, de opsporing en de handhaving. Door grote verscheidenheid aan activiteiten en soort dienstverlener binnen de sector geeft de nieuwe lijst onvoldoende inzicht in de specifieke aard van deze activiteiten. Dit geldt des te meer in verhouding tot de meer gedetailleerde codes die gelden voor de meer traditionelere bedrijfsactiviteiten. Met een scherpere code voor de hostingsector kan makkelijker informatie, zoals statistische gegevens over deze sector en de verschillende diensten, worden opgevraagd bij de Kamer van Koophandel.

Daarnaast is het kabinet voornemens om een onderzoek uit te laten voeren naar de exacte grootte van de sector, de verhouding van bulletproof en bad hosters daarin en de effecten van regelgeving en handhaving hierop. Het is hierbij belangrijk om inzicht te verkrijgen in de types hostingdiensten die een rol kunnen spelen bij criminele activiteiten, de verschillende activiteiten en diensten die door hostingdiensten worden aangeboden, de mate waarin een hostingdienst op de hoogte is van activiteiten op zijn servers, de rol van de dienstverlener en de klant, en welke maatregelen een dienstverlener kan treffen tegen een klant.

3) Zelfregulering

Cleannetworks project

Clean Networks verenigt twee belangrijke initiatieven om criminele inhoud en activiteiten (abuse) op het internet te bestrijden.[5] Binnen dit project worden partijen onder andere actief benaderd en voorzien van handelingsperspectieven wanneer er abuse op hun netwerken plaatsvindt. Deze initiatieven zijn het resultaat van jarenlange samenwerking tussen sectororganisaties, het bedrijfsleven, de overheid en betrokken individuen. Overheid, bedrijfsleven en private sector zien de bestrijding van abuse als een gezamenlijke verantwoordelijkheid. In 2023 heeft het ministerie van Justitie en Veiligheid een Europese subsidie uit het Fonds voor Interne Veiligheid toegekend gekregen om dit project in samenwerking met de Stichting Nationale Beheersorganisatie Internet Providers (NBIP) te versterken en verder te ontwikkelen.

Gedragscode Abusebestrijding

De Gedragscode Abusebestrijding is breed gedragen binnen de Nederlandse internetsector en betrokken stakeholders. Met de Gedragscode worden aanbieders een handreiking gedaan om effectieve maatregelen te nemen tegen abuse op het internet, zoals het invoeren van een know your customer beleid, het hanteren van de Gedragscode notice and takedown en een algemeen, herkenbaar e-mailadres voor abuse meldingen die dagelijks worden gelezen.

De gedragscode is vrijwillig en beschrijft de stappen die de aangesloten partijen moeten nemen om gebruik van hun digitale infrastructuur voor onrechtmatige activiteiten te voorkomen en te

[5] Clean Networks - Samen sterk tegen abuse

bestrijden. Onder digitale infrastructuur vallen ook mere conduit-, caching-, en hostingdiensten en online platforms in de zin van de digitaledienstenverordening. Onder onrechtmatige activiteiten worden zaken verstaan die illegale inhoud in de zin van de verordening kunnen zijn, zoals phishing, het verspreiden van malware of DDoS-aanvallen.

Het ondertekenen en hanteren van de Gedragscode helpt niet alleen bij het inrichten van effectieve maatregelen, maar geeft ook toegang tot het Clean Networks keurmerk. Met dit keurmerk onderscheiden aanbieders zich in de markt van aanbieders die geen duidelijk beleid hebben om misbruik tegen te gaan.

Ook de Rijksoverheid heeft een verantwoordelijkheid als het gaat om het inkopen van web- en clouddiensten. We bekijken Rijksbreed hoe we de inkoopregels kunnen aanpassen om als overheid het goede voorbeeld te geven door diensten in te kopen die zich inzetten voor een schoner internet en die de Gedragscode onderschrijven.

Publiek private samenwerking

Nederland heeft een lange traditie als het gaat om publiek-private samenwerking op het gebied van online veiligheid. In het kader van de aanpak van bulletproof en bad hosting dient daarom ook het Anti-Abuse Netwerk (AAN) genoemd te worden. Het AAN is een samenwerkingsverband van publiek en private partijen, waarin wordt gewerkt aan een veilige en betrouwbare digitale infrastructuur.

4) Know your customer-beleid

'Ken je klant'-beleid, ook wel 'Know your customer'-beleid of KYC-beleid genoemd, wordt als een van de oplossingen gezien om bulletproof en bad hosting beter aan te kunnen pakken. Het principe is al terug te vinden in de Gedragscode Abusebestrijding en de partijen in de hostingsector die hierbij zijn aangesloten voeren dit al grotendeels uit. Voor een KYC-beleid kan een voorbeeld worden genomen aan de gegevens en verificatie die vereist worden in artikel 28 van de NIS2-richtlijn. Dit artikel verplicht domeinnaamregistratiediensten een database met domeinnaamregistratiegegevens bij te houden. Onderdeel van de verkenning is om te bezien of er mogelijkheden zijn om het uitvoeren van KYC-beleid breder te verplichten, en zo ja welke oplossingsrichtingen kansrijk zijn om verder uit te werken.

Sanctiewetgeving

In EU verband bestaat al enkele jaren de mogelijkheid om entiteiten of personen onder het EU-Cybersanctieregime een sanctie op te leggen. De sanctie kan bestaan uit een inreisverbod en/of het bevriezen van tegoeden. Daarnaast zijn er ook indirecte consequenties, namelijk een verbod op het verlenen van zakelijke diensten aan de gesanctioneerde personen, waaronder bijvoorbeeld een verbod op het ter beschikking stellen van serverruimte aan bedrijven die eigendom zijn – of onder zeggenschap staan- van personen of bedrijven op de sanctielijst. Bovendien geldt ook een onderzoeksplicht voor bedrijven om te bezien of een klant op de sanctielijst is geplaatst. Voor personen en entiteiten die op de EU-sanctielijst zijn geplaatst bestaat er voor hostingbedrijven dus al een KYC-verplichting.

Gedragscode digitaledienstenverordening

Om betere samenwerking tussen lidstaten te bevorderen en te voorkomen dat bulletproof of bad hosters hun criminele activiteiten makkelijk kunnen verplaatsen naar een andere lidstaat kan er worden ingezet op Europese adoptie van de Gedragscode Abusebestrijding. Het kabinet zal gaan onderzoeken op welke wijze dit het beste zal kunnen plaatsvinden. Een van de mogelijkheden die zal worden bekeken is via de digitaledienstenverordening. In artikel 45 van de digitaledienstenverordening wordt de mogelijkheid beschreven voor het opstellen van vrijwillige gedragscodes op Unieniveau die bijdragen tot een correcte toepassing van de verordening, onder meer rekening houdend met de specifieke uitdagingen om diverse soorten illegale inhoud en systeemrisico's aan te pakken.

Analogie met de Wet ter voorkoming van witwassen en financieren van terrorisme

KYC-beleid verankeren in wetgeving is niet nieuw. In de wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) is een cliëntenonderzoek al een verplichting voor een aantal sectoren: instellingen en beroepsgroepen die burgers toegang geven tot het financiële stelsel zoals banken, makelaars en cryptobedrijven. Er kan verder onderzocht worden of een deel van de sector onder deze regeling valt of zou kunnen vallen; hierbij kan gedacht worden aan hostingservices die alleen een adres ter beschikking stellen (zogenaamde spookhosters) of hostingservices die cryptobetalingen en/of crypto exchanges mogelijk maken.

Bulletproof en Bad Hosting als economisch delict

Hostingservices die bewust of onbewust criminele activiteiten faciliteren brengen schade aan de sector als geheel. Het deel van de sector dat het schoonhouden van het internet serieus neemt, en bijvoorbeeld de Gedragscode onderschrijft, ondervindt oneerlijke concurrentie van diegenen die dat niet doen. Daarnaast zorgen hostingservices die online criminaliteit faciliteren voor economische schade aan Nederlandse bedrijven en burgers; in 2023 ging dat naar schatting om 707 miljoen euro.[6] Daarom zou er kunnen worden bezien in hoeverre bulletproof en/of bad hosting als een economisch delict kan worden gezien waarbij extra zorgvuldigheid van de sector gevraagd kan worden. Artikel 1 Wet Economische Delicten jo. Artikel 18.9 van de Telecommunicatiewet zouden hier eventueel een mogelijkheid voor kunnen bieden. Het kabinet zal deze optie in het vervolg verder uitwerken.

Financieel onderzoek en cryptobetalingen

Een van de onderdelen van een KYC-beleid kan zijn klanten te verifiëren middels het verifiëren van de betaling. Door te zorgen dat een eerste betaling via een reguliere banktransactie moet plaatsvinden, kan verificatie plaatsvinden van de identiteit en gegevens van de klant. Het volledig anoniem afnemen van hostingdiensten is dan niet meer mogelijk, waardoor het zicht op de *resellers* vergroot wordt. Deze maatregel verbiedt het indirect om de (eerste) betaling in cryptovaluta toe te staan. Het kabinet zal verder onderzoeken of dit ook wettelijk verankerd zou kunnen worden. Om zicht te houden op de keten van klanten bij het doorverkopen van hostingruimte kan het ook voor de opsporing van belang zijn om de betalingen te kunnen volgen.

5) Aanpak resellers

Hostingproviders weten vaak niet precies welke klanten hun diensten misbruiken voor criminele activiteiten. Bovendien kunnen klanten de dienstverlening doorverkopen. Er is dan sprake van zogenaamde resellers. Dit doorverkopen is niet verboden. Wel kan het zicht op mogelijke criminele activiteiten verder verminderen, met name omdat de klanten gemakkelijk anoniem kunnen blijven en/of zich in het buitenland bevinden of zich naar het buitenland verplaatsen. Dat maakt de opsporing van daders zeer lastig, zeker als ze naar landen vertrekken die buiten de EU liggen. Dit wordt ook door andere EU-landen gezien en onderkend, waardoor verdere samenwerking noodzakelijk is om meer informatie te kunnen vergaren. Bovendien werken resellers vaak niet mee als er gegevens ten behoeve van opsporingsdoeleinden worden gevorderd. Er wordt ofwel geen gehoor gegeven ofwel versleutelde data geleverd. Er bestaan al een aantal initiatieven en acties op vrijwillige basis om hiertegen op te treden, maar verdergaande oplossingsrichtingen zouden nog verder verkend kunnen worden.

Resellerbrief van de politie

Jaarlijks verstuurt de politie een brief aan Nederlandse hostingproviders waarin zij adviseert een eventuele overeenkomst met bepaalde resellers te herzien. De lijst van resellers wordt opgesteld op basis van openbare bronnen waaruit af te leiden valt dat de resellers zichzelf afficheren als criminele dienstverleners. Er is gebleken dat hostingbedrijven actie ondernemen naar aanleiding van de brief en dit is daarmee een efficiënt middel gebleken. Door de Tweede Kamer is met de motie Michon-Derkzen opgeroepen om te onderzoeken of het wenselijk is dat de jaarlijkse brief

[6] CBS Online Veiligheid en Criminaliteit 2024, https://www.cbs.nl/nl-nl/longread/rapportages/2025/online-veiligheid-en-criminaliteit-2024/7-online-criminaliteit-totaal

van de politie openbaar wordt gemaakt.[7] Er zijn hostingbedrijven die zich niet bewust zijn van malafide klanten maar wel actie ondernemen. Daarom kan het openbaar maken van de lijst een negatief beeld geven van partijen die het wel goed doen en wordt daarmee het risico op onterechte reputatieschade van deze partijen vergroot. Dat laat onverlet dat men binnen de sector zelf de brief openbaar kan maken om positieve reacties erop juist te benadrukken.

In het kader van het versterken van de internationale samenwerking zal er worden gekeken of de politie de lijst kan delen met andere opsporingsdiensten zodat ook zij een beter beeld hebben van de reseller-problematiek.

Know your customer beleid

Ook, of juist, voor de aanpak van resellers is het van belang om een stevig KYC-beleid te integreren in de processen. De verkenning rondom KYC-beleid staat verder toegelicht onder 4.

6) Europese samenwerking

Uitvraag bad hosting problematiek in het buitenland

Om te inventariseren in hoeverre andere landen met bulletproof of bad hosting te maken hebben is er via een korte vragenlijst informatie bij andere landen opgehaald. Hier hebben achttien landen op gereageerd, waarvan vijf landen buiten de EU. Over het algemeen ervaren landen een goede samenwerking met nationale hostingdiensten. Desondanks herkennen meerdere landen de hostingproblematiek en ervaren het als een uitdaging om bad hosting tegen te gaan. Het kan hierbij gaan om landen die zelf 'last' ervaren van malafide partijen die gebruik maken van hun hostingservers, landen die in opsporingsonderzoeken stuiten op malafide hostingdiensten in het buitenland die niet meewerken, of op een andere wijze betrokken geraken, bijvoorbeeld in internationale opsporingsonderzoeken naar cybercrimezaken. In sommige landen zijn er bijvoorbeeld geen bulletproof hosters bekend, maar is er wel een vermoeden dat er criminelen wonen die gebruik maken van hosting diensten in het buitenland. Alhoewel de hostingproblematiek in meerdere landen wordt herkend, wordt het niet overal als een even groot probleem gezien. Hierbij speelt wellicht een rol dat niet overal evenveel aandacht hieraan wordt besteed.

Net zoals in Nederland stuiten de meeste andere landen erop dat malafide partijen dan wel buiten de reikwijdte van de wet vallen en om die reden niet aan wettelijke verplichtingen hoeven te voldoen, dan wel dat de samenwerking moeizaam verloopt en het vergaren van bewijs voor strafrechtelijke aansprakelijkheid moeilijk wordt gemaakt. Ook in andere landen is er (nog) geen specifieke wet- en regelgeving voor de hostingsector om bad hosting tegen te gaan. Wel wordt de ernst van de problematiek erkend, en is de verwachting dat dit onderwerp op ten duur meer aandacht krijgt op Europees niveau.

Andere landen hebben geen verplicht KYC-beleid voor de hostingsector. Sommige hostingdiensten hebben een KYC-beleid op vrijwillige basis. Als de hostingdienst in het buitenland is gevestigd kan het vorderen van informatie van hostingdiensten moeizaam verlopen. Dit is vooral herkenbaar bij een resellers-constructie. In dat geval wordt getracht de informatie via internationale rechtshulp in strafzaken en operationele samenwerking via organisaties als Europol en Interpol te verkrijgen. Een Europees verplicht KYC-beleid zou hier een goede oplossing voor kunnen zijn.

Vooral gelet op de aard van de resellers-constructie is het belangrijk om de samenwerking in het kader van de aanpak tegen bulletproof en bad hosting op Europees niveau te versterken. Het kabinet zal zich daarom inzetten om dit onderwerp hoger op de Europese agenda te zetten.

Wetgeving op Europees niveau
Nederland heeft er tijdens de onderhandelingen over de digitaledienstenverordening op aangedrongen om een zorgplicht in de verordening op te nemen zodat hostingdiensten aan de voorkant meer verplicht zouden worden maatregelen te treffen om abuse op hun diensten en

[7] Kamerstukken II, 2024-2025, 26643, nr. 1250.

systemen te voorkomen. Destijds is daar geen meerderheid voor gevonden maar dat betekent niet dat hier op Europees niveau niet meer voor gelobbyd kan worden, bijvoorbeeld in het kader van de evaluatie van de digitaledienstenverordening. De hosting- en reseller-problematiek zijn grensoverschrijdend en samenwerking tussen lidstaten is van groot belang.

Samenwerking met Europa

De politie zoekt op het terrein van de aanpak van bad en bulletproof hosters ook de samenwerking via Europol. Om hier meer aandacht voor te vragen is er een video gemaakt met uitleg over de problematiek in Nederland. In de video nodigt de minister van Justitie en Veiligheid internationale collega's uit om mee te denken over een gezamenlijke gerichte aanpak.

Evenement ter promotie van Cleannetworks

Zoals eerder is geconstateerd is het de wens om ook in Europees verband meer aandacht te vragen voor het project Cleannetworks en de Gedragscode Abusebestrijding. Daarom is het kabinet voornemens om samen met de Stichting NBIP in het najaar van 2025 een workshop in Brussel te organiseren over de aanpak van bulletproof en bad hosting.