Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

26 643 Informatie- en communicatietechnologie (ICT)

29 911 Bestrijding georganiseerde criminaliteit

Nr. 1544

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 juli 2026

In 2025 bent u via de Kamerbrief «Integrale aanpak cybercrime» (Kamerstuk 26 643, nr. 1357) geïnformeerd over de verkenning naar de aanpak van bad hosting naar aanleiding van de toezegging tijdens het commissiedebat Cybercrime van 24 oktober 2024. In de verkenning is de, aan bad hosting gerelateerde, resellerproblematiek meegenomen. In deze brief wordt u geïnformeerd over de voortgang van maatregelen naar aanleiding van de verkenning. Het betreft activiteiten op het gebied van handhaving, wet- en regelgeving, enkele overige maatregelen en internationale samenwerking.

Hostingproblematiek

De hostingproblematiek in Nederland vormt al jaren een grote uitdaging voor opsporingsdiensten. Misbruik van hostingdiensten vormt een belangrijk onderdeel van meerdere vormen van online criminaliteit. Alhoewel het overgrote deel van de Nederlandse hostingsector zelf maatregelen neemt tegen het gebruik van hun diensten door criminelen, is er een deel dat onbewust *(bad hosting)* of bewust *(bullet proof hosting)* malafide activiteiten faciliteert. Dat maakt verschillende vormen van online criminaliteit lastig op te sporen, zoals phishing, ransomware, malware, DDoS-aanvallen, maar ook doxing, sextortion en de verspreiding van beeldmateriaal van seksueel kindermisbruik. Dit is met name het geval bij bullet proof hosting, waarbij criminelen serverruimte kunnen gebruiken van hostingaanbieders die nauwelijks toezicht houden op hun klanten, geen opvolging aan meldingen van misbruik geven, en in sommige gevallen adverteren met het niet meewerken aan verzoeken of bevelen van opsporingsdiensten. Daarnaast is er bij bad hosting veelal sprake van een resellerconstructie, waarbij diensten via meerdere tussenpartijen worden aangeboden of «doorverhuurd», waardoor het achterhalen van de verantwoordelijke partij wordt bemoeilijkt en criminelen makkelijker uit het zicht van opsporingsdiensten blijven.

kst-26643-1544
ISSN 0921 - 7371
's-Gravenhage 2026

Beeld en ontwikkeling

Volgens het Internet Organised Crime Threat Assessment 2026 (IOCTA 2026) van Europol speelt bullet proof hosting een steeds grotere rol binnen de cybercrime-economie. Cybercriminelen maken gebruik van complexe infrastructuren en technieken om buiten het zicht van opsporingsinstanties te blijven en hun servers moeilijk traceerbaar te maken. Daarbij worden activiteiten verspreid over meerdere servers in verschillende landen, waardoor verschillen in wetgeving, procedures en jurisdictie internationale opsporing kunnen vertragen. Hierdoor wordt het tijdig detecteren van malafide internetverkeer aanzienlijk lastiger gemaakt. Een opvallende en zorgelijke ontwikkeling is de overstap van criminelen naar het opzetten van eigen digitale infrastructuren, mogelijk om voorwaarden van een hostingaanbieder te omzeilen en de opsporing verder te bemoeilijken. Het gebruik van deze werkwijzen maken het zeer complex en tijdrovend om daders op te sporen en infrastructuur offline te halen.

Voortgang aanpak bad hosting

Hieronder worden enkele maatregelen en initiatieven nader toegelicht. Deze zijn in deze brief onderverdeeld in vier categorieën: handhaving, wet- en regelgeving, overige maatregelen en initiatieven, en Europese en internationale samenwerking.

1) Handhaving

Handhaving op grond van de Digitaledienstenverordening

De Digitaledienstenverordening (DSA) beoogt een veilige, voorspelbare en betrouwbare online omgeving te bevorderen en de verspreiding van illegale online inhoud aan te pakken. Daartoe bevat de DSA enerzijds een kader voor de aansprakelijkheid van aanbieders van tussenhandeldiensten, waaronder hostingdiensten en online platforms, en anderzijds een aantal zorgvuldigheidsverplichtingen waar deze diensten aan moeten voldoen.

Hostingdiensten en online platforms dienen illegale online content te verwijderen of ontoegankelijk te maken zodra zij hier kennis van hebben. Doen zij dat niet, dan kunnen zij geen beroep doen op de beperking van aansprakelijkheid die zij in beginsel genieten, en riskeren zij zelf aansprakelijkheid. Kennis kan onder meer ontstaan door de ontvangst van een melding van illegale online content. Daarnaast legt de DSA aan tussenhandeldiensten zorgvuldigheidsverplichtingen op, zoals het instellen van effectieve contactpunten voor gebruikers, bedrijven en bevoegde autoriteiten en het inrichten van kennisgevings- en actiemechanismen, zodat het melden van illegale online content voor iedereen eenvoudig en toegankelijk is. De DSA voorziet in maximumharmonisatie. Nationaal kunnen daarom geen aanvullende zorgvuldigheidsverplichtingen aan tussenhandeldiensten worden opgelegd.

De DSA biedt verschillende mogelijkheden om bad hostingdiensten aan te spreken op hun verantwoordelijkheid. In Nederland houdt de Autoriteit Consument en Markt (ACM) primair toezicht op de naleving van de DSA voor hier gevestigde tussenhandeldiensten. Voor de zogenoemde zeer grote online platforms (VLOP's) en zeer grote online zoekmachines (VLOSE's) ligt het toezicht primair bij de Europese Commissie. De ACM heeft zelf geen bevoegdheid tot het geven van bevelen voor het verwijderen van illegale inhoud. Het geven van verwijderbevelen of het optreden tegen bepaalde illegale inhoud is voorbehouden aan daartoe

bevoegde autoriteiten, zoals in Nederland het Openbaar Ministerie (OM) en de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM). Wel verplicht de DSA dat tussenhandeldiensten dergelijke bevelen onverwijld uitvoeren en de uitvaardigende autoriteit informeren over de genomen maatregelen.

Het OM en de politie maken bij voorkeur eerst gebruik van kennisgevings- en actiemechanismen voor het indienen van een verwijderverzoek bij de betreffende hostingdienst of het onlineplatform. Onder meer een deel van de hostingsector en het OM behoren tot de ondertekenaars van de Gedragscode Notice-and-Take Down (NTD).[1] In deze gedragscode zijn nadere praktische principes overeengekomen voor het doen en afhandelen van meldingen. Indien een melding via deze procedure niet tot het gewenste effect leidt, kan in specifieke gevallen en onder voorwaarden door de officier van justitie na machtiging van de rechter-commissaris een verwijderingsbevel worden gegeven op grond van artikel 125p van het Wetboek van Strafvordering (Sv).

Voor de bullet proof hostingdiensten, die bewust bijdragen aan criminele activiteiten, zal bovenstaande vaak onvoldoende zijn. Hiervoor bevat het strafrecht middelen om illegale praktijken tegen te gaan, bijvoorbeeld om in te zetten in een opsporingsonderzoek. Om de verschillende vormen van handhaving, zoals de bestuursrechtelijke en strafrechtelijke handhaving, bij illegale content te versterken, werken de verschillende toezichthouders samen binnen het Samenwerkingsplatform Digitale Toezichthouders (SDT), waarbinnen ook een DSA Kamer is ingericht. De ACM vervult hiervan het voorzitterschap vanuit haar rol als digitaledienstencoördinator onder de DSA. De DSA Kamer is opgericht om de handhaving van de DSA te coördineren en expertise over toezicht op online tussenhandeldiensten te bundelen. Zo wordt er momenteel in dat kader samengewerkt bij een onderzoek naar een specifieke hostingdienst.

Opsporingsonderzoek naar bullet proof hoster

De aanpak van bullet proof hosters is een aandachtspunt voor de politie in de opsporing. Een voorbeeld hiervan is een onderzoek naar een malafide hostingbedrijf dat in november 2025 heeft geleid tot de inbeslagname van maar liefst ruim 250 fysieke servers. Met de inbeslagname van de fysieke servers zijn duizenden virtuele servers uit de lucht gehaald. Het hostingbedrijf werd enkel gebruikt om criminele activiteiten te faciliteren en is al sinds 2022 in meer dan 80 onderzoeken naar cybercrimedelicten voorgekomen. De aanbieder verhuurde digitale ruimte aan criminelen voor onder andere ransomware-aanvallen, phishing en verspreiding van beeldmateriaal van seksueel kindermisbruik. Het hostingbedrijf profileerde zich als bullet proof hoster, beloofde volledige anonimiteit voor gebruikers en suggereerde niet mee te werken met opsporingsdiensten. Met de inbeslagname van de servers is het criminele proces verstoord waardoor deze servers niet meer voor malafide doeleinden kunnen worden gebruikt en verdere potentiële slachtoffers zijn voorkomen.

Hoewel dit een voorbeeld is van een succesvolle actie, blijkt ook uit deze casus dat strafrechtelijke opsporing en vervolging bij bad hosting complex en tijdsintensief zijn. Opsporingsonderzoeken kunnen maanden tot jaren duren, terwijl de meeste gevallen onverwijlde interventie vereisen om verdere schade te beperken of te voorkomen. De aanpak van bad hosting blijft daarom belangrijk en krijgt de nodige prioriteit.

[1] De Gedragscode Notice-and-Take-Down is in april 2026 geactualiseerd om onder andere beter aan te sluiten bij de DSA. Beschikbaar via: https://www.cleannetworks.net/wp-content/uploads/2026/04/Gedragscode-Notice-and-Take-Down-2026-2.0.pdf

Sancties

In het coalitieakkoord zijn ambities opgenomen ten aanzien van Europese sancties als instrument in de bestrijding van cybercriminelen. Een sanctie kan bestaan uit een inreisverbod en/of het bevriezen van tegoeden. Het is daarnaast verboden om diensten te leveren aan gesanctioneerde individuen of organisaties. Er geldt daarom een onderzoeksplicht voor Nederlandse en Europese organisaties om actief na te gaan of hun (potentiële) klant is opgenomen op de Europese sanctielijst. Deze plicht geldt ook voor hostingdiensten.

Het aanbieden van hosting- en vergelijkbare diensten aan gesanctioneerde personen en entiteiten is strafbaar en kan aanleiding geven tot strafrechtelijke vervolging. De handhaving op grond van sanctiewetgeving heeft de afgelopen jaren een prominentere rol gekregen in de aanpak van cybercrime. Zo heeft de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) op 18 mei 2026 twee verdachten aangehouden op grond van verdenking van het (indirect) ter beschikking stellen van economische middelen aan door de Europese Unie gesanctioneerde entiteiten. Het onderzoek richt zich op de rol van een bedrijf dat volgens de FIOD als dekmantel fungeerde voor een eerder gesanctioneerd webhostingbedrijf wegens het faciliteren van destabiliserende activiteiten (waaronder cyberaanvallen en verspreiding van desinformatie) gericht tegen de Europese Unie. Daarnaast wordt een tweede bedrijf onderzocht dat een faciliterende rol zou hebben gespeeld bij het leveren van internetverbindingen voor de servers van het hostingbedrijf. In het onderzoek zijn meerdere locaties en datacenters doorzocht en zijn ruim 800 servers in beslag genomen. Deze zaak onderstreept de verantwoordelijkheid van hostingproviders, datacenters en andere aanbieders van digitale infrastrictuur om na te gaan aan wie hun diensten worden aangeboden.

2) Wet- en regelgeving

Know your customer-beleid

Eén van de kansrijke maatregelen om bad hosting, en de hieraan gerelateerde resellerproblematiek, tegen te gaan, is het identificeren en verifiëren van de identiteit van klanten van hostingdiensten, ook wel *know your customer (KYC)-beleid*genoemd. Met een accuraat KYC-beleid kunnen verantwoordelijke partijen sneller worden achterhaald en worden aangesproken wanneer er sprake is van illegale content of andere vormen van online criminaliteit. Onder de DSA geldt momenteel geen algemene KYC-verplichting voor de hostingsector. Echter, KYC-beleid is niet nieuw voor de sector en wordt reeds op vrijwillige basis toegepast door diverse hostingaanbieders, onder meer door ondertekenaars van de Gedragscode Abusebestrijding. De Gedragscode Abusebestrijding is breed gedragen binnen de Nederlandse internetsector en betrokken stakeholders. Met de Gedragscode wordt aanbieders een handreiking gedaan om effectieve maatregelen te nemen tegen misbruik van hun diensten, zoals het invoeren van een KYC-beleid, het hanteren van de Gedragscode NTD en het zekerstellen van bereikbaarheid door het hebben van een algemeen, herkenbaar e-mailadres voor meldingen van misbruik dat dagelijks wordt uitgelezen.

Uit de verkenning naar bad hosting kwam naar voren dat een wettelijke verplichting van het KYC-beleid een goede maatregel kan zijn om bad hosting tegen te gaan. Op dit moment zijn hostingdiensten niet verplicht om een KYC-beleid te voeren, en kiezen sommige hostingdiensten er bewust voor om bijvoorbeeld de Gedragscode Abusebestrijding niet te ondertekenen. Om ervoor te zorgen dat het KYC-beleid door de gehele

sector wordt toegepast, bestaat de wens om dit wettelijk te verplichten voor alle hostingdiensten.

Bij de implementatie van een Nederlandse KYC-verplichting voor de hostingsector bestaat er een aanzienlijk risico dat de malafide hosters hun activiteiten verplaatsen naar andere Europese landen met een minder strikt regime. Hierdoor ontstaat er mogelijk een waterbedeffect, waarbij de problematiek wordt verplaatst in plaats van wordt tegengegaan. Vanuit deze landen kunnen criminelen namelijk alsnog (Nederlandse) slachtoffers blijven maken. Het kabinet zet daarom in op een Europese aanpak en de versterking van de samenwerking op internationaal niveau. In dit kader wordt de samenwerking gezocht met lidstaten die de hostingproblematiek herkennen en wordt dit op Europees niveau aangekaart.

DSA evaluatie

In 2027 is een evaluatie van de DSA door de Europese Commissie voorzien. In dat jaar zal ook de Nederlandse Uitvoeringswet digitaledienstenverordening worden geëvalueerd. De Staatssecretaris Digitale Economie en Soevereiniteit coördineert dit namens Nederland en zal bij de ministeries, toezichthouders en maatschappelijke organisaties inventariseren wat hun ervaringen zijn en welke wijzigingen van de DSA zij eventueel nodig en wenselijk achten. Dit zal worden meegenomen bij het bepalen van de Nederlandse inzet op EU-niveau. Daarbij kan Nederland pleiten voor aanscherpingen van de DSA, daarbij rekening houdend met het feit dat het nog relatief jonge wetgeving betreft. Ook hier valt te denken aan de introductie van een KYC-verplichting voor hostingdiensten.

Non-paper EU Tech Sovereignty Package

Naast de evaluatie van de DSA heeft de Europese Commissie onlangs een voorstel gedaan voor een Europees Tech Sovereignty Package. Met dit pakket beoogt de Europese Commissie digitale autonomie te bevorderen, onder meer door innovatie op het gebied van cloud en artificiële intelligentie te stimuleren. Deze ontwikkeling leidt naar verwachting tot een verdere opschaling van cloudinfrastructuur en datacenters binnen Europa, waardoor ook misbruik van deze infrastructuur (en hiermee de bad hostingproblematiek) kan toenemen. Voor de publicatie van het pakket is er in april een Nederlands non-paper over het EU Tech Sovereignty Package gepubliceerd. Hierin is onder andere aandacht gevraagd voor het risico van misbruik van diensten op digitale infrastructuur door criminelen of andere malafide entiteiten. Bij het uitwerken van nieuwe of aangepaste regelgeving is het noodzakelijk om in een vroeg stadium rekening te houden met de hostingproblematiek en mogelijk misbruik van de infrastructuur.

3) Overige maatregelen en initiatieven

Resellerbrief van de politie

In maart 2026 heeft de Nederlandse politie net als in voorgaande jaren een brief aan Nederlandse hostingbedrijven verstuurd, waarin zij worden gewaarschuwd voor het verhuren van serverruimte aan malafide resellers die cybercriminaliteit faciliteren. In de brief is een lijst opgenomen van bedrijven die zichzelf, via onder andere cybercriminele fora of op andere online platformen, presenteren als bullet proof dienstverlener, al dan niet onder vermelding van het specifieke delict dat zij faciliteren. De waarschuwingsbrief van de politie is een effectief middel gebleken. Het kan voor hostingpartijen een aanleiding zijn om de relatie met specifieke klanten te

beëindigen door de contractuele overeenkomst op te zeggen en geen diensten meer aan te bieden. Hostingbedrijven blijken zich niet altijd bewust te zijn van hun malafide klanten, en kunnen na ontvangst van de brief direct actie ondernemen.

Rijksinkoop

Het geven van het goede voorbeeld als rijksoverheid door het inkopen van hostingdiensten bij leveranciers die zich inzetten voor een schoner internet krijgt blijvende aandacht. Momenteel wordt in het kader van Maatschappelijk Verantwoord Opdrachtgeven en Inkopen (MVOI) vanuit het Ministerie van Justitie en Veiligheid bezien op welke wijze de inkoopregels voor hostingdiensten binnen de rijksoverheid kunnen worden aangescherpt, zodat uitsluitend diensten worden afgenomen van leveranciers die zich proactief inzetten voor een schoner internet en de Gedragscode Abusebestrijding onderschrijven. De overheid kan hiermee laten zien waarde te hechten aan de inspanningen die hostingpartijen leveren om zeker te stellen dat zij geen criminaliteit faciliteren.

Cyclotron use case bullet proof hosters

Cyclotron is een publiek-private samenwerking bij het NCSC gericht op het binnen een «trusted community» met elkaar delen van relevante informatie over digitale incidenten en dreigingen, deze gezamenlijk te analyseren en de opgedane inzichten en kennis te delen met een bredere groep. Vaak wordt hierbij gezamenlijk gewerkt aan een specifiek thema, ook wel «use case» genoemd. Het doel van de samenwerking is om Nederland weerbaarder te maken tegen cyberaanvallen. Binnen de samenwerking worden meerdere «use cases» uitgevoerd die door het NCSC worden gecoördineerd. In oktober 2025 is er een use case opgezet die is gericht op bullet proof hosting. Binnen deze use case wordt er door de Dutch Cloud Community, TU Delft, de politie en diverse cybersecurity-bedrijven samengewerkt om een methodiek te ontwikkelen die kan worden gebruikt om bullet proof hosters te identificeren. Hierbij wordt gebruikgemaakt van de kennis en data van de deelnemers van de use case.

Standaard Bedrijfsindeling – SBI

Momenteel is er geen eenduidig beeld van de hostingsector. Er bestaan verschillende soorten tussenpersonen die verschillende soorten hosting-diensten leveren. Bedrijven worden met een Standaard Bedrijfsindeling code (SBI) in het Handelsregister geregistreerd. Een SBI bestaat uit vier of vijf cijfers en geeft aan wat de hoofdactiviteit van een bedrijf of organisatie is. Om meer zicht op Nederlandse bedrijven te verkrijgen die hostingdiensten als hoofdactiviteit aanbieden, is door het Ministerie van Justitie en Veiligheid gezamenlijk met de ACM en de ATKM een verzoek bij het CBS (Centraal Bureau voor de Statistiek) ingediend voor de toekenning van een extra uitsplitsing op de bestaande SBI-code voor de hostingsector. Door de extra uitsplitsing wordt het zicht op de hosting-sector aangescherpt. 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.

4) Europese en internationale samenwerking

Europol

De aanpak van malafide hosters krijgt steeds meer internationale aandacht en wordt in toenemende mate gezamenlijk opgepakt door een groeiend aantal landen. Vaak gebeurt dit met ondersteuning van Europol, waarbij onder andere Nederland een leidende rol heeft. De deelnemende landen willen een waterbedeffect van de hostingproblematiek voorkomen. De samenwerking richt zich op de verstoring van criminele infrastructuur waarbij er een specifieke focus is op de bad hostingproblematiek, informatie-uitwisseling tussen Europol-landen, en de inzet op grond van de Europese sanctiewetgeving. De komende periode wordt deze operationele samenwerking verder vormgegeven en geconcretiseerd.

De Nederlandse politie heeft bovendien de eerder genoemde resellerbrief in Europol-verband met partners gedeeld, met het advies om in andere landen een soortgelijke actie te organiseren, waarbij de eigen sector voor bullet proof hosters en malafide resellers wordt gewaarschuwd.

Handelingskader voor internetserviceproviders

In november 2025 heeft het NCSC in samenwerking met de FBI en andere cyberagentschappen een document ten behoeve van internetproviders en cybersecurity specialisten gepubliceerd om bullet proof hosting tegen te gaan.[2] Dit document bevat richtlijnen om bullet proof hostingproviders te identificeren en aanbevelingen voor maatregelen die internetproviders kunnen nemen. In het document worden onder andere adviezen gegeven voor het inrichten van een KYC-beleid, waarbij persoonlijke gegevens van klanten worden opgevraagd en geverifieerd. Door deze maatregelen wordt het voor bullet proof hostingproviders moeilijker om hun activiteiten in stand te houden, omdat zij voor internettoegang en onderliggende netwerk- en infrastructuurdiensten afhankelijk zijn van internetproviders.

Counter Ransomware Initiative

Het *Counter Ransomware Initiative*is een internationaal samenwerkingsverband voor het tegengaan van ransomware. Nederland en het Verenigd Koninkrijk hebben het initiatief genomen binnen het *Counter Ransomware Initiative* aandacht te vragen voor de aanpak van bad hosting. Enerzijds wordt gewerkt aan het ontwikkelen en delen van betrouwbare data over het ecosysteem van bullet proof hosting, bijvoorbeeld over de omvang van de problematiek en in hoeverre het ransomware mogelijk maakt. De wens is om onderzoeken naar bullet proof hosting door andere landen te stimuleren en relevante kennis en inzicht te delen. Daarnaast wordt gewerkt aan een gedragscode om bullet proof hosting tegen te gaan. De bedoeling hiervan is dat zo veel mogelijk deelnemende landen binnen het CRI-netwerk de gedragscode ondersteunen door deze op nationaal niveau te implementeren en het gebruik ervan door de eigen sector te stimuleren. Bij het opstellen van de gedragscode binnen de CRI wordt de Nederlandse Gedragscode Abusebestrijding als voorbeeld gebruikt.

De Minister van Justitie en Veiligheid,
D.M. van Weel

[2] Bullet proof Defense: Mitigating Risks From Bullet proof Hosting Providers. Beschikbaar via: https://www.ic3.gov/CSA/2025/251119.pdf