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

2504

Vragen van het lid **Bontenbal** (CDA) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Online criminelen bestoken de wereld met cyberaanvallen vanuit Nederland»* (ingezonden 17 februari 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid), mede namens de Minister van Economische Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 21 april 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2012.

Vraag 1
Bent u bekend met het bericht «Online criminelen bestoken de wereld met cyberaanvallen vanuit Nederland» en de bijbehorende radioreportage «De makelaars van de cybercrime»?[1]

Antwoord 1
Ja.

Vraag 2
Herkent u de berichtgeving over cyberaanvallen via Nederlandse servers, mogelijk gemaakt door foute tussenpartijen uit het buitenland die deze serverruimte doorverhuren aan criminelen? Richten deze aanvallen zich vooral tegen bedrijven of in dezelfde mate tegen overheden en particulieren? Zijn er patronen in deze aanvallen te ontdekken, bijvoorbeeld in het type bedrijven waar criminelen het op gemunt hebben? Wat is u bekend over de aard en ernst van dit probleem? Bijvoorbeeld over de omvang van de aangerichte schade en het aantal aanvallen dat maandelijks plaatsvindt? Wordt dit bijgehouden en door wie? Ziet u het aantal aanvallen toenemen? Kunt u alle beschikbare informatie hieromtrent met de Kamer delen, eventueel in een vertrouwelijke technische briefing? Zijn met de door de politie samengestelde lijst alle foute tussenpartijen voldoende in beeld om te kunnen aanpakken? Gebeurt dit ook?

[1] Pointer, 12 februari 2022, https://pointer.kro-ncrv.nl/online-criminelen-bestoken-de-wereld-met-cyberaanvallen-vanuit-nederland

ah-tk-20212022-2504
ISSN 0921 - 7398
's-Gravenhage 2022

Antwoord 2
Het is bekend dat Nederlandse servers en infrastructuur misbruikt worden door criminelen voor het plegen van strafbare feiten, zoals ransomware-aanvallen. Het beeld van de politie is dat ransomware-aanvallen met name gericht zijn op het MKB en grote bedrijven. Hierin zijn patronen te herkennen, waarbij ongerichte aanvallen met name binnen het MKB voorkomen door het gebruik van Ransomware-as-a-service.[2] De meer gerichte aanvallen zien op grote organisaties, waarbij maatwerk wordt verricht om tot maximaal financieel gewin te komen.[3] Over de hoeveelheid ransomware-aanvallen in Nederland en de schade die deze aanvallen veroorzaken zijn weinig kwantitatieve gegevens beschikbaar. Het beeld, ook op basis van mediaberichtgeving, is dat het aantal aanvallen toeneemt en dat ook de hoogte van het geëiste losgeld toeneemt. De politie geeft aan dat zij jaarlijks rond de 200 aangiftes van ransomware ontvangt. De aangiftebereidheid bij cybercrimedelicten is echter laag, wat met name geldt voor ransomware. Het aantal aangiften is daarom geen goede weerspiegeling van de omvang van de problematiek. Ransomware-aanvallen kunnen grote maatschappelijke en economische impact hebben. Het Cybersecuritybeeld Nederland (CSBN) 2021 stelt dat ransomware een risico vormt voor de nationale veiligheid. Indien uw Kamer verzoekt om een technische briefing kan daarin worden voorzien.
Voor meer inzicht in de acties van de politie omtrent het delen van de lijst met hosting-resellers verwijs ik u naar de beantwoording van de Kamervragen van het lid Rajkowski over hetzelfde artikel.[4] Naar aanleiding van deze beantwoording heeft DCC laten weten dat een aantal leden met bepaalde klanten geen zaken meer doet.[5]

Vraag 3
Kunt u uiteenzetten hoe deze criminelen precies te werk (kunnen) gaan? Welke mogelijkheden zijn er op dit moment om deze specifieke vorm van cybercriminaliteit te verhinderen c.q. aan te pakken? Hoe vaak worden de internetcriminelen in kwestie en hun helpers opgespoord, aangehouden en vervolgd? Zijn er factoren die dit bemoeilijken? Wilt u een overzicht geven van alle wet- en regelgeving die hier van toepassing is? Wat zijn thans belemmeringen, zowel nationaal als Europees of internationaal, om dergelijke cyberaanvallen effectief te bestrijden, zoals juridische obstakels, een gebrek aan samenwerking of capaciteitsproblemen? Welke partijen, in binnen- en buitenland, zijn nodig om dit probleem te helpen aanpakken? Hoe verloopt nu de samenwerking tussen deze partijen?

Antwoord 3
In het Cybersecurity Beeld Nederland (CSBN) 2021 zijn de verschillende fasen in het delictsproces van ransomware beschreven. Kortweg bestaat een ransomware-aanval uit het verkrijgen van initiële toegang tot een ICT-netwerk, het consolideren van de positie, het wegsluizen van informatie, het inzetten van ransomware en de financiële afhandeling. In het CSBN 2021 wordt hier dieper op ingegaan.[6] Het effectief tegengaan van ransomware vraagt meerdere soorten maatregelen. Zo is het belangrijk om ransomware te voorkomen, doordat bedrijven en organisaties de juiste preventieve maatregelen nemen. Zie hiervoor ook vraag 5. Daarnaast heeft de politie de Ransomware Taskforce opgericht, die proactief onderzoek doet naar het hele criminele ecosysteem rondom ransomware. Het doel is om schade en slachtoffers te voorkomen, het criminele proces te verstoren en daders op te sporen.
Het opsporen van verdachten van cybercrime is echter complex, zie hierover ook de brief die eerder naar uw Kamer is gestuurd over de dilemma's die de politie en het OM tegenkomen bij opsporing in het digitale domein.[7] Daders hoeven zich niet in Nederland te bevinden, verdachten kunnen met techni-

---

[2] Bij ransomware-as-a-service bieden ransomware-ontwikkelaars een product aan waarmee minder technische criminelen ransomware-aanvallen kunnen plegen
[3] Cybersecurity Beeld Nederland (CSBN) 2021.
[4] Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2257
[5] Hosting-bedrijven stoppen met aantal foute resellers | Computable.nl
[6] Cybersecuritybeeld Nederland 2021 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)
[7] Kamerstuk 28 648, nr. 621

sche mogelijkheden hun identiteit en locatie gemakkelijk afschermen en het internet is grenzeloos. Internationale samenwerking is daarom belangrijk, hetgeen ook blijkt uit de internationale actie waarbij een ransomware-bende is opgepakt.[8] De politie neemt onder andere deel in de Joint Cybercrime Action Taskforce van Europol. Om de grensoverschrijdende opsporing in het digitale domein te versterken heeft Nederland de afgelopen jaren actief deelgenomen aan de gesprekken over de E-Evidence verordening van de EU en over het tweede protocol bij het Cybercrimeverdrag in het kader van de Raad van Europa. Het concept protocol is goedgekeurd in 2021. Na goedkeuring op politiek niveau en ratificatie zal snellere en meer efficiënte samenwerking in opsporingsonderzoeken mogelijk zijn.
Zoals eerder vermeld in de beantwoording van Kamervragen van het lid Van Raak, is het niet bekend hoeveel veroordelingen voor ransomware er precies zijn geweest.[9] Ransomware aanvallen zijn niet onder één specifiek wetsartikel te scharen en worden niet als zodanig geregistreerd door het OM en de Raad voor de rechtspraak. Ook gaat het vaak om buitenlandse daders.

Vraag 4
Klopt het dat cybercriminelen hun illegale activiteiten graag via Nederland ontplooien vanwege de goede digitale infrastructuur hier? Welke (nationale) maatregelen gaat u nemen om van deze status af te komen? Staat dit onderwerp ook op de Europese agenda? Bent u bereid het bij de eerstvolgende gelegenheid (weer) te agenderen?

Antwoord 4
Nederlandse hostingdiensten worden inderdaad misbruikt voor het plegen van cybercrime en andere vormen van online criminaliteit, via malafide hostingbedrijven, maar ook via hostingbedrijven die zich daar niet van bewust zijn. De hostingsector heeft daarom zelf een gedragscode «abusebestrijding» 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[10] 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. Tot slot richten het OM en de politie zich binnen de opsporingsonderzoeken die zij uitvoeren onder meer op hostingbedrijven die bewust criminaliteit faciliteren. Echter, hostingproviders zijn op basis van de huidige wet- en regelgeving onder voorwaarden niet strafrechtelijk aansprakelijk voor hetgeen zich op hun netwerken bevindt. Zie hiervoor ook de beantwoording van eerdere Kamervragen van het lid Van Nispen.[11]
In EU-verband is de triloog-fase van de Digital Services Act begonnen. Deze conceptverordening 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.
Het belang van een schoon en veilig internet en de rol die tussenpersonen zoals hostingproviders hierin spelen, is groot en zal steeds in EU-verband benadrukt worden.

Vraag 5
Op welke wijze(n) staat u bedrijven en overheden bij om weerbaar te worden tegen cybercriminaliteit en wordt ondersteuning en nazorg geboden als zich een aanval heeft voorgedaan? Hoe is geborgd dat uit iedere (poging tot een) cyberaanval lessen worden getrokken om volgende aanvallen te voorkomen c.q. af te slaan? Waar is bij bedrijven en overheden behoefte aan? Indien u dit

[8] Ransomware-bende opgerold wegens vernietigende aanvallen op kritieke infrastructuur | politie.nl
[9] Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 1383
[10] www.cleannetworks.net
[11] Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 2608

niet weet, wilt u dit nagaan via bijvoorbeeld een uitvraag bij de VNG of ondernemersorganisaties?

Antwoord 5
Het is wenselijk om slachtofferschap van cybercriminaliteit, zoals ransomware-aanvallen, bij bedrijven te voorkomen. Bedrijven zijn verantwoordelijk voor hun eigen cybersecurity en moeten hiervoor de juiste maatregelen treffen. De overheid kan daarbij ondersteuning bieden. Daarom biedt het Digital Trust Center (DTC) van het Ministerie van EZK verschillende kennisproducten aan om de cyberweerbaarheid van bedrijven te vergroten. Deze bevatten adviezen voor ondernemers om besmetting met ransomware te voorkomen en adequaat te reageren als het toch gebeurt. Het DTC biedt ook een basisscan aan, zodat bedrijven hun cyberweerbaarheid kunnen testen. Met het delen van verhalen van ondernemers die slachtoffer zijn geworden van ransomware probeert het DTC bedrijven en ondernemers te wijzen op de risico's. Ook is het DTC begonnen met het waarschuwen van individuele bedrijven bij ernstige cyberdreigingen. Inmiddels zijn er al meer dan 300 bedrijven gewaarschuwd.
Het Nationaal Cyber Security Centrum (NCSC) informeert organisaties in de vitale sectoren en de rijksoverheid proactief over digitale dreigingen en levert hen bijstand bij incidenten. Ook deelt het NCSC informatie over digitale dreigingen en incidenten via aangewezen schakelorganisaties in het Landelijk Dekkend Stelsel van cybersecuritysamenwerkingsverbanden. Het NCSC werkt bovendien samen met vitale én niet-vitale organisaties die kunnen bijdragen aan het versterken van het actuele situationeel beeld, onder andere op het gebied van ransomware dreigingen. Zo wordt er samengewerkt met securityleveranciers, multinationals en onderzoekers zoals het Dutch Institute for Vulnerability Disclosure (DIVD). In dit kader werken het DTC en het NCSC nauw samen.
De moties Ephraim[12] en Hermans[13] verzoeken de regering om te komen met een voorlichtingsplan voor ondernemers ten aanzien van de risico's van cybercrime en concrete maatregelen om ondernemers beter te beschermen tegen digitale dreigingen en cybercriminelen. Bij de uitvoering van deze moties worden de behoeften die er op dit vlak bij organisaties zijn meegenomen.
Het Ministerie van BZK ziet het als haar taak kaderstellend, ondersteunend, en waar nodig aanjagend te zijn naar alle overheidslagen. Daartoe stelt het Ministerie van BZK randvoorwaarden op, zoals met de Baseline Informatieveiligheid Overheid (BIO). De BIO geldt overheidsbreed als het minimumkader voor informatieveiligheid. De individuele overheidsorganisaties moeten hun informatiebeveiliging primair zelf op orde hebben en houden, waarbij zij ondersteund worden door hun koepelorganisaties. Zo ondersteunt de VNG gemeentebestuurders met de Agenda Digitale Veiligheid. Begin 2021 werd de Resolutie Digitale Veiligheid [14] vastgesteld, waaraan gemeenten zich gecommitteerd hebben. Hierin wordt de noodzaak onderstreept dat gemeenten hun digitale weerbaarheid versterken. Daarnaast worden gemeenten ondersteund door de Informatiebeveiligingsdienst (IBD), die actuele producten en diensten ter ondersteuning van de BIO aanbiedt en het programma Verhogen Digitale Weerbaarheid verzorgt. Ook is de IBD de sectorale CERT/CSIRT[15] voor Nederlandse gemeenten, die crisismanagementteams ondersteunt in het geval van incidenten. Het Ministerie van BZK werkt hierbij samen met de VNG en de IBD.
Ook ondersteunt het Ministerie van BZK het delen van informatie met alle overheden via een bijdrage aan het Centrum voor Informatiebeveiliging en Privacybescherming (CIP).[16] Zie hiervoor ook de beantwoording van schriftelijke vragen van het lid Kathmann.[17] Verder wordt jaarlijks in oktober–de maand van cybersecurity- de overheidsbrede cyberoefening

[12] Kamerstuk 28 684, nr. 682
[13] Kamerstuk 35 788, nr. 120
[14] https://vng.nl/sites/default/files/2020–12/resolutie-digitale-veiligheid-versie-3-december-2020.pdf
[15] Computer Emergency Response Team/Computer Security Incident Response Team
[16] Op de website van het CIP zijn de diverse ontwikkelende producten te vinden: www.cip-overheid.nl
[17] Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1852

georganiseerd.[18] Deze oefening, die is bedoeld voor Rijks- en uitvoeringsorganisaties, provincies, gemeenten en waterschappen en laat zich ieder jaar inspireren door recente en actuele dreigingen en cyberaanvallen. Naast deze oefening zijn er webinars, die men ook kan terugkijken.[19] Speciaal voor gemeenten zijn een drietal cyberoefenpakketten ontwikkeld door het Instituut voor Veiligheids- en Crisismanagement. Deze zijn online raadpleegbaar en gratis af te nemen voor alle gemeenten.[20]
Tot slot bevat de I-strategie 2021 – 2025 voor de rijksoverheid een stevige inzet op het thema digitale weerbaarheid, die ook de weerbaarheid tegen ransomware zal verhogen, onder meer via kennisproducten. De bijbehorende roadmap wordt voor de zomer aan uw Kamer gestuurd door de Staatssecretaris van BZK.

Vraag 6
Kunt u per volgende afspraak uit het coalitieakkoord Omzien naar elkaar, vooruitkijken naar de toekomst aangeven hoe en op welke termijn het kabinet hier uitwerking aan gaat geven (pag.[21]?
– We nemen het voortouw en zetten in Europees verband in op versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en «open source».
– We willen dat inlichtingendiensten beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om nieuwe en toenemende digitale dreigingen en aanvallen assertief op te sporen en te bestrijden, met waarborgen voor goed en effectief toezicht en digitale burgerrechten.
– We beschermen onze bedrijven, vitale infrastructuur en economisch kapitaal beter door centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en «hacks».
– Cybercriminaliteit zoals «ransomware» is zeer ondermijnend. We investeren daarom in een brede meerjarige cybersecurity aanpak en in cyberexpertise bij de politie, rechtspraak, het Openbaar Ministerie (OM) en defensie.

Antwoord 6
Het coalitieakkoord wordt nog uitgewerkt. De hoofdlijnenbrief Justitie en Veiligheid van 9 februari jl. toont een eerste overzicht van de maatregelen die voortvloeien uit het coalitieakkoord.[22] Sinds 2018 is de Kamer jaarlijks geïnformeerd over de integrale aanpak van cybercrime.[23] Deze aanpak bestaat uit vier pijlers, namelijk preventie, slachtofferondersteuning, wetenschappelijk onderzoek en opsporing, vervolging en verstoring. De mate waarin het beleid en de strafrechtsketen kan worden versterkt om cybercriminaliteit, waaronder ransomware, aan te pakken, is mede afhankelijk van de uitkomst van de uitwerking van het coalitieakkoord en het beschikbaar komen van middelen voor cybercrime.
Ten aanzien van de slagkracht van de inlichtingendiensten verwijs ik naar de brief van 24 februari 2022 van de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan uw Kamer over de impact van het coalitieakkoord en de stand van zaken wijziging Wiv 2017.
Tot slot zet de hoofdlijnenbrief digitalisering[24] van 8 maart jl. van de Staatssecretaris voor Koninkrijksrelaties en Digitalisering, de Minister van Justitie en Veiligheid, de Minister van Economische Zaken en Klimaat en de

---

[18] https://www.weerbaredigitaleoverheid.nl/
[19] De webinars van de cyberoefening van 2021 zijn tot en met maart 2022 terug te kijken.
[20] Te vinden op de website van de Informatiebeveiligingsdienst gemeenten (IBD): https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vngoefenscenarios-digitale-incidenten/
[21] Pointer, 12 februari 2022, https://pointer.kro-ncrv.nl/online-criminelen-bestoken-de-wereld-met-cyberaanvallen-vanuit-nederland
[22] Kamerstuk 35 925, nr. 132
[23] Kamerstuk 26 642, nr. 768
[24] Kamerstuk 26 643, nr. 842

Minister voor Rechtsbescherming de ambities en doelen uiteen voor de digitale transitie van onze samenleving. Dit gebeurt langs vier thema's, te weten: het digitale fundament, de digitale overheid, de digitale samenleving en de digitale economie. Deze brief benoemt ook de inzet op Europees verband op het gebied van digitalisering, zoals AI en digitale identiteit. De hoofdlijnenbrief is het startpunt voor de kabinetsbrede werkagenda digitalisering. Deze wordt de komende maanden geconcretiseerd met alle betrokken departementen, belanghebbenden uit de samenleving, wetenschap en bedrijfsleven, en medeoverheden. Ook wordt deze besproken met Europese partners.