Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Ons kenmerk
9e25705a-or1-1.1

Uw kenmerk

Bijlagen
0

Datum 16 april 2025
Betreft Beantwoording Kamervragen m.b.t. bescherming tegen digitale aanvallen op internationale instellingen in NL

Hierbij stuur ik u de antwoorden op de vragen van het lid Kathmann (GroenLinks-PvdA) over bescherming tegen digitale aanvallen op internationale instellingen in Nederland.

De vragen werden ingezonden op 17 februari 2025 met kenmerk 2025Z02900.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.J.M. Uitermark

De antwoorden op de schriftelijke vragen van het lid Kathmann (GroenLinks-PvdA) over bescherming tegen digitale aanvallen op internationale instellingen in Nederland, ingezonden op 17 februari 2025.

1.Kent u het bericht 'Russische spionnen en de 'hack van Amsterdam''[1]?

Ja.

2. Deelt u de mening dat de in het bericht genoemde casus een indicatie is dat Nederland geen goed antwoord heeft op digitale aanvallen vanuit statelijke actoren waarbij Europese of internationale instellingen in Nederland doelwit zijn? Zo ja, hoe komt dat en wat is er nodig om dit te verbeteren? Zo, nee waar blijkt uit deze casus dan dat er wel sprake was van een goed antwoord?

De verantwoordelijkheid voor de cyberveiligheid van internationale organisaties ligt in de eerste plaats bij de organisaties zelf. Niettemin heeft het gastland ook een inspanningsverplichting om het goed en continu functioneren van de organisatie te waarborgen. De Kabinetsinzet op cyberweerbaarheid, zoals beschreven in de NLCS, draagt daar aan bij.
Daarnaast is sinds januari 2024 de Europese verordening 2023/2841 van kracht, waarmee is beoogd de weerbaarheid van Europese instellingen, maar ook van coördinatie en afhandeling als er cyberincidenten bij deze instellingen plaatsvinden te bevorderen. Zo zijn Europese instellingen verplicht om cyberveiligheidsmaatregelen te nemen en om cyberincidenten te melden bij CERT-EU. Onder de coördinatierol van CERT-EU in crisisafhandeling schakelen zij onder andere met het Europese CSIRT-netwerk. Nederland is hierin via het NCSC vertegenwoordigd.

3. Deelt u de mening dat, als Nederland geen bemoeienis heeft of mag hebben met het beschermen van internationale instellingen tegen digitale aanvallen, daarmee het risico op dergelijke aanvallen en schade kan toenemen? Zo ja, waarom? Zo nee, waarom niet?

Het kabinet hecht veel belang aan het werk van internationale organisaties en instellingen. Deze organisaties zijn vaak doelwit van cyberaanvallen. Ondanks dat de verantwoordelijkheid voor adequate cybersecuritymaatregelen in eerste instantie bij deze organisaties zelf ligt, kunnen deze organisaties, voor zover gevestigd in Nederland, in geval van een cyberincident een vrijwillige melding doen bij het Nationaal Cybersecurity Centrum (NCSC) en om bijstand vragen. Daarmee kan de Nederlandse staat in die gevallen een bijdrage leveren aan het tegengaan van digitale aanvallen.

Het gastland heeft als gesteld een inspanningsverplichting om het functioneren van de internationale organisaties te faciliteren, voor zowel het fysieke als digitale domein. Voor een goede invulling van die verplichting is een goede samenwerking cruciaal. Bovendien kan Nederland zich als lidstaat van internationale organisaties actief inzetten voor (verbetering van) de cyberveiligheid van die organisatie. Zo werd na de cyberaanval op het Internationaal Strafhof met steun van Nederland een fonds voor het verhogen van de cyberveiligheid van het Hof ingesteld waaraan

[1] *De Volkskrant, 14 februari 2025, 'Russische spionnen en de 'hack van Amsterdam', de verborgen zwakte van Europa' (https://www.volkskrant.nl/kijkverder/v/2025/ema-hack-europa-ruslandonderzoek~v1330314/?referrer=https%3A%2F%2Fwww.google.nl%2F).*

alle staten kunnen bijdragen.

4. Wat is de rol van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) in het geval een statelijke actor een digitale aanval op een Nederlandse organisatie dan wel een internationale organisatie in Nederland uitvoert? Is daar verschil tussen en zo ja, waarom?

De AIVD doet onderzoek naar de digitale dreiging van statelijke actoren in het belang van de nationale veiligheid, zoals benoemd in artikel 8, Wiv2017. In relatie tot de omgang van AIVD met slachtoffers van digitale aanvallen door statelijke actoren gebeurt dit, op basis van vrijwilligheid, eveneens binnen de kaders van de Wiv2017. Dit geldt zowel voor Nederlandse als voor internationale organisaties.

5. In welke mate verschilt bovengenoemde rol van de AIVD in vergelijkbare situaties van inlichtingen- en veiligheidsdiensten in andere lidstaten van de Europese Unie (EU)?

Iedere EU-lidstaat richt zijn inlichtingen- en veiligheidsdiensten evenals zijn taken en bevoegdheden naar eigen zienswijze in. Om die reden heb ik u in het commissiedebat van 23 oktober 2024[2] toegezegd om de situaties in andere landen te onderzoeken. Op de invulling van een dergelijk onderzoek zal ik terugkomen bij de gesprekken over de herziening van de WIV.

6. Welke Nederlandse of Europese instantie kan wel actie ondernemen in het geval er een internationale organisatie met vestiging in een lidstaat van de EU te maken krijgt met een digitale aanval? Zo er een dergelijke instantie is, welke afspraken zijn hiermee dan precies gemaakt? Kunt u hierbij ook het specifieke juridische kader schetsen?

Ten aanzien van internationale organisaties die in Nederland zijn gevestigd geldt, anders dan bijvoorbeeld voor organisaties die deel uitmaken van de rijksoverheid, dat het NCSC niet tot taak heeft om bij digitale dreigingen en incidenten ongevraagd bijstand te leveren. Wel kunnen deze internationale organisaties in geval van een incident met aanzienlijke gevolgen voor de continuïteit van de dienst van die organisatie, op grond van artikel 16 van de Wbni een vrijwillige melding doen bij het NCSC. Het NCSC kan in dat geval bijstand verlenen, mits het in behandeling nemen van de melding geen onevenredige of overmatige belasting voor het NCSC vormt.

Tevens doet de AIVD onderzoek naar dreigingen tegen de nationale veiligheid. Indien de AIVD constateert dat een organisatie in Nederland waarschijnlijk slachtoffer is van een digitale aanval, brengt de AIVD - vanuit de weerbaarheidstaak en binnen de kaders van de WIV2017- deze organisatie hiervan op de hoogte.

Voor in EU-lidstaten gevestigde EU-organisaties geldt dat zij andere Europese instellingen, organen en agentschappen zoals het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) of CERT-EU kunnen helpen voor het verhogen van de cyberweerbaarheid of vragen om ondersteuning bij cyberincidenten. De taken en bevoegdheden van ENISA en CERT-EU hieromtrent zijn vastgelegd in Verordening (EU) 2019/881 (de 'Cybersecurity Act'), Raadsbesluit (EU) 2022/2504 alsook de NIS2-richtlijn (EU) 2022/2555 en in

[2] Kamerstuk 34588, nr. 93 (vergaderjaar 2024-2025)

verordening 2023/2841 zoals in het antwoord op vraag 2 weergegeven. VN-instellingen kunnen zich richten tot het United Nations International Computing Centre (UNICC). In het UNICC Mandate and Governance Framework wordt bepaald dat UNICC diensten aanbiedt aan VN-entiteiten. Contractuele afspraken met VN-agentschappen zijn vastgelegd in Service Level Agreements.

7. Deelt u de mening dat het zeer zorgelijk is dat er in Europees verband kennelijk onvoldoende samenwerking is en dat een door de Nederlandse politie in 2021 gegeven waarschuwing aan andere lidstaten geen opvolging kreeg? Zo nee, waarom niet? Zo ja, wat gaat het kabinet doen om te zorgen dat hier in de toekomst wel op geacteerd wordt?

Cyberaanvallen en digitale netwerken zijn niet gebonden aan landgrenzen. Internationale samenwerking en een gecoördineerde aanpak en zijn daarom van groot belang. Het Kabinet hecht hier dan ook veel waarde aan en zet zich binnen de EU en andere gremia in voor de verbetering van deze samenwerking. Zo wordt er gewerkt aan de implementatie van de Europese NIS2-richtlijn in nationale wetgeving in de Cyberveiligheidswet. De NIS2-richtlijn biedt aan lidstaten meer mogelijkheden om informatie met landen zowel binnen als buiten de EU en relevante organisaties te delen. Dit zal ook de samenwerking met deze landen bevorderen. Met de inwerkingtreding van de NIS1-richtlijn en de NIS2-richtlijn is het Europese CSIRT-netwerk opgericht en versterkt. Het CSIRT-netwerk bestaat uit vertegenwoordigers van de nationale CSIRT's van de Europese lidstaten en het computercrisisresponsteam voor de instellingen, organen en instanties van de Unie (CERT-EU). Dit CSIRT-netwerk heeft onder meer tot taak het uitwisselen van informatie over incidenten, bijna-incidenten, cyberdreigingen, risico's en kwetsbaarheden, het uitvoeren van een gecoördineerde respons op incidenten, en het verlenen van bijstand aan de lidstaten bij de aanpak van grensoverschrijdende incidenten. Daarnaast bevordert ook de Europese verordening 2023/2841, zoals in het antwoord op vraag 2 weergegeven, de samenwerking.

8. Deelt u de mening dat er sprake is van een lacune in de hulp aan deze internationale organisaties in het geval van een digitale aanval van een statelijke actor? Zo ja, waarom, hoe komt dat en hoe moet deze lacune opgevuld gaan worden? Zo nee, waarom niet?

Zoals geschetst in het antwoord op vraag 6, kunnen internationale organisaties, voor zover gevestigd in Nederland, in geval van een cyberincident met aanzienlijke gevolgen voor de continuïteit van hun dienst, een vrijwillige melding doen bij het NCSC en vragen om bijstand. Hierbij wil ik benadrukken dat de verantwoordelijkheid van digitale veiligheid van organisaties in Nederland primair bij de organisaties zelf ligt.

9. Deelt u de mening dat uit de in het bericht genoemde casus blijkt dat de internationale samenwerking in het geval van digitale dreigingen niet optimaal werkt en verbetering behoeft? Zo ja, welke verbeteringen zijn er nodig en hoe en op welke termijn worden die bewerkstelligd? Zo nee, waarom niet en hoe kan het dan dat het weken duurt eer zelfs maar duidelijk is waar een verzoek tot onderzoek naar een dergelijke dreiging moet worden ingebracht?

Ik doe geen uitspraken over specifieke casussen van de AIVD. In het algemeen, zoals ook aangegeven bij vraag 7, zijn cyberaanvallen en digitale netwerken niet gebonden aan landgrenzen. Internationale samenwerking en een gecoördineerde

aanpak zijn daarom van groot belang. Het kabinet hecht hier dan ook veel waarde aan en zet zich binnen de EU en andere gremia in voor de verbetering van deze samenwerking, zoals ook aangegeven bij vraag 2. Zo wordt er gewerkt aan de implementatie van de Europese NIS2-richtlijnen in nationale wetgeving in de Cyberbeveiligingswet. De NIS2-richtlijn biedt aan lidstaten meer mogelijkheden om informatie met landen zowel binnen als buiten de EU en relevante organisaties te delen en versterkt de samenwerking binnen het Europese CSIRT-netwerk. Dit zal ook de samenwerking met deze landen bevorderen.

10. Kunt u deze vragen één voor één beantwoorden?
Ja.