Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Vragen gesteld door de leden der Kamer

2022Z03023

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).

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]

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?

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

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

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?

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?

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

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.[2]?
– 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.

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