Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres

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

**Onze referentie**
2025-0000302945

**Uw referentie**

Datum 6 mei 2025
Betreft Beantwoording Kamervragen lid Koekkoek (Volt) DDoS-aanvallen belgische overheidswebsites

Hierbij bied ik, mede namens de minister van Justitie en Veiligheid, de antwoorden aan van de op 27 maart 2025 ingediende Kamervragen van het lid Koekkoek (Volt) aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over het bericht 'Pro-Russische hackers nemen Belgische overheidswebsites op de korrel' met kenmerk: 2025Z05834[1].

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
*Digitalisering en Koninkrijksrelaties*

Zsolt Szabó

[1] NOS Nieuws, 24 maart 2025, 'Pro-Russische hackers nemen Belgische overheidswebsites op de korrel, raadpleegbaar via: Pro-Russische hackers nemen Belgische overheidswebsites op de korrel

**2025Z05834**

**Vraag 1**
**Bent u bekend met het bericht ‘Pro-Russische hackers nemen Belgische overheidswebsites op de korrel’?**

**Antwoord**:
Ja.

**Vraag 2**
**Deelt u de opvatting van het Belgische Centrum voor Cybersecurity dat een dergelijke DDoS-aanval ongevaarlijk is?**

**Antwoord:**
De impact van een DDoS-aanval is vaak beperkt en symbolisch van aard. Met een DDoS-aanval wordt de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur aangevallen. Er worden meerdere verzoeken verstuurd zodat de diensten als gevolg van overbelasting slecht of niet meer werken.

Door een DDoS-aanval krijgt de aanvaller geen toegang tot vertrouwelijke informatie. Ook is in veel gevallen de bedrijfsvoering van een organisatie beperkt of niet afhankelijk van een website. Daardoor blijft in veel gevallen de impact van een DDoS-aanval beperkt. Hoewel DDoS-aanvallen niet leiden tot dataverlies of systeeminbraak, kunnen ze wel (tijdelijk) invloed hebben op de beschikbaarheid, informatieverstrekking en/of dienstverlening van de getroffen websites. Dergelijke aanvallen moeten daarom wel serieus worden genomen.

**Vraag 3**
**Zijn Nederlandse overheidswebsites ook vatbaar voor dit soort aanvallen? Zo ja, op wat voor schaal komt dit voor?**

**Antwoord:**
Nederlandse overheidswebsites zijn, net zoals iedere andere website, vatbaar voor DDoS-aanvallen. Ongeacht de genomen maatregelen kan een aanval van een bepaalde schaalgrootte altijd een verstoring opleveren.

Het Nationaal Cyber Security Centrum (NCSC) is enkel op de hoogte van de DDoS-aanvallen die bij hen worden gemeld en beschikt daarom niet over een volledig beeld van de schaal. Organisaties die onder de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen hebben in het geval van ernstige incidenten een meldplicht bij het NCSC. Voor andere organisaties geldt dat zij vrijwillig een melding van een incident kunnen doen bij het NCSC, waarbij er dus geen sprake is van een meldplicht.

**Vraag 4**
**Wat voor risico's hebben cyberaanvallen op overheidswebsites voor het gebruik van de websites en de bescherming van data zoals persoonsgegevens?**

**Antwoord:**
Voor de beantwoording verwijs ik u naar vraag 2.

**Vraag 5**
**Is er onderzocht wat voor groepen verantwoordelijk zijn voor DDoS-aanvallen op bijvoorbeeld de DigiD? Zo ja, hoe wordt hierop gehandeld? Volgen hierop bijvoorbeeld diplomatieke stappen?**

**Antwoord:**
Organisaties zijn in de eerste plaats zelf verantwoordelijk voor adequate cybersecuritymaatregelen en voor het uitvoeren van onderzoek naar cyberaanvallen waardoor zij zijn getroffen. Daarnaast kunnen organisaties aangifte doen bij de Politie indien zij slachtoffer zijn van een DDoS-aanval. In het specifieke geval van de DDoS-aanvallen op DigiD worden deze per incident onderzocht en worden, waar mogelijk, aanvullende passende maatregelen genomen. Verder doet het NCSC onderzoek naar DDoS-aanvallen in het algemeen om een (situationeel) beeld te creëren over de techniek en de slachtoffers. Het NCSC doet daarbij niet aan attributie.

Doorgaans is het vanwege de aard van DDoS-aanvallen lastig om te achterhalen wie achter een aanval zit. Een DDoS-aanval kan worden uitgevoerd door zowel statelijke als niet-statelijke actoren. Deze actoren gebruiken diverse middelen en technieken om hun identiteit te verbergen. Dit doen zij o.a. met IP-spoofing, botnets of door middel van reflectie-aanvallen. Daarnaast kunnen kwaadwillenden gebruikmaken van betaalde DDoS-diensten, zogenaamde Booters.

Diplomatieke stappen worden per incident zorgvuldig gewogen. Nederland zet zich actief in om het kwaadwillend gedrag te adresseren zowel bilateraal als in coalitieverband via de EU of de NAVO. Afgelopen februari sprak Nederland steun uit voor de Australische sancties volgend op de cyberaanval op Medibank in 2022. In juli vorig jaar heeft Nederlandse inzet gezorgd voor EU-sancties tegen zes Russische cybercriminelen.

**Vraag 6**
**Is er sprake van een toename van Russische aanvallen met betrekking tot de veranderende geopolitieke situatie? Zo ja, hoe reageert de Nederlandse overheid hierop?**

**Antwoord:**
Zoals opgenomen in de jaarverslagen van de diensten en het jaarlijkse Cybersecuritybeeld Nederland is de dreiging van Russische cyberaanvallen al jaren onverminderd hoog.[2]

Als gevolg van de oorlog in Oekraïne is een toenemend aantal Russische operaties waarneembaar gericht op het ondermijnen en/of in kaart brengen van de Nederlandse steun aan Oekraïne. Incidenten kunnen voor een deel worden geplaatst in de context van geopolitieke spanningen en verschuivende internationale machtsverhoudingen. Opvallend is de toename van cyberaanvallen door hacktivisten waarbij organisaties om symbolische redenen doelwit worden, bijvoorbeeld omdat het land waarin ze opereren Oekraïne steunt.

Het kabinet reageert hier o.a. op door Oekraïne te ondersteunen in het versterken van hun cyberweerbaarheid, zowel civiel als militair. Doordat Russische cyberoperaties op Oekraïne ook spillover effecten kunnen hebben naar de rest van Europa, dient deze steun ook ons eigen nationale veiligheidsbelang.

In de Internationale Cyberstrategie 2023-2028 wordt beschreven hoe Nederland, binnen de turbulente geopolitieke context en de daaruit volgende cyberdreiging, vormgeeft aan de doelstelling om cyberdreigingen van staten en criminelen tegen te gaan.[3] Daarnaast wordt in de Nederlandse Cybersecuritystrategie (NLCS) de na-

[2] NCTV 2024, *Cybersecuritybeeld Nederland 2024,* Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid, 28 oktober 2024.
[3] Ministerie van Buitenlandse Zaken, *Internationale Cyberstrategie 2023–2028*, Den Haag: Rijksoverheid, 9 juni 2023.

tionale aanpak voor het versterken van de digitale weerbaarheid uiteengezet.[4] Hiermee maken we Nederland digitaal weerbaar in een situatie van toenemende hybride en militaire dreiging, zoals de Russische. Zo investeert het kabinet in het tegengaan van digitale dreigingen van staten en criminelen. Tevens is het versterken van de digitale weerbaarheid overheidsbreed een van de prioriteiten in de Nederlandse Digitaliseringsstrategie (NDS) die voor de zomer van 2025 gepubliceerd wordt.

[4] NCTV 2022, *Nederlandse Cybersecuritystrategie 2022–2028*, Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid, 6 december 2022.