# Tweede Kamer der Staten-Generaal

**2**

Vergaderjaar 2023–2024

**Aanhangsel van de Handelingen**


**Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden**

## 1892

Vragen van het lid **Kathmann** (GroenLinks-PvdA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de onbereikbaarheid van provinciewebsites als gevolg van DDoS-aanvallen:* (ingezonden 28 maart 2024).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 3 juni 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, nr. 1526.

Vraag 1
Kent u het bericht «Cyberaanval legt websites van meerdere provincies plat»?[1]

Antwoord 1
Ja

Vraag 2
Kunt u informatie verschaffen over wat de reden was van de onbereikbaarheid van de provinciewebsites? Betreft het bijvoorbeeld een technische storing of een cyberaanval? Zo nee, waarom niet?

Antwoord 2
Naar het zich laat aanzien zijn de betreffende provinciewebsites overbelast geraakt door zogenaamde Distributed Denial of Service (DDoS)-aanvallen. Organisaties kunnen een DDoS-aanval op een onlinedienst niet voorkomen, maar wel de effecten ervan beperken. Er zijn enkele technische maatregelen die organisaties kunnen treffen voor adequate detectie van en respons op een DDoS-aanval. Een DDoS- aanval is een poging van onbevoegden om een website onbereikbaar te maken voor gebruikers door ontzettend veel verzoeken naar deze website te versturen. Hierdoor raakt een website en het computersysteem erachter overbelast, en is het systeem onbereikbaar.
De getroffen provincies hebben de nodige maatregelen getroffen. De websites zijn op dezelfde dag weer in werking getreden.

[1] NU.nl, 25 maart 2024, Cyberaanval legt websites van meerdere provincies plat, https://www.nu.nl/tech/6306531/cyberaanval-legt-websites-van-meerdere-provincies-plat.html.


ah-tk-20232024-1892
ISSN 0921 - 7398
's-Gravenhage 2024

Ik onderschrijf het belang dat de overheid open communiceert over het verloop van dergelijke incidenten om de burger het vertrouwen te geven in een goede en veilig functionerende overheid.

Vraag 3
Kunt u aangeven of de attributie aan Russische hackers die in sommige media wordt gedaan klopt? Zo ja, waarom wel? Over welke aanwijzingen beschikt u? Zo nee, waarom niet?

Antwoord 3
Een hactivistische pro-Russische groepering claimt de DDoS-aanvallen; of dit terecht is, is zeer moeilijk vast te stellen. Met name de oorlog in Oekraïne heeft gezorgd voor een opleving van dit soort hactivistische activiteiten, ook tegen Nederlandse doelen. Dit soort DDoS-aanvallen passen dan ook in het dreigingsbeeld, zoals het Cybersecuritybeeld Nederland (CSBN) 2023 laat zien.

Vraag 4
Wat zijn voor particulieren en bedrijven de gevolgen geweest van de onbereikbaarheid van de provinciewebsites?

Antwoord 4
Mij is niet bekend of de korte uitval tot schade bij burgers of bedrijven heeft geleid. Naar waarschijnlijkheid is de impact beperkt gebleven door de korte uitvalduur en/of door de scheiding tussen de dienstverlening en bedrijfsvoering van de provinciewebsites.

Vraag 5
Heeft de dienstverlening van de getroffen provincies door de onbereikbaarheid van de websites geleden? Zo ja, wat waren de gevolgen daarvan?

Antwoord 5
Hierbij verwijs ik naar de beantwoording in vraag 4.

Vraag 6
Is er een overheidsbrede richtlijn voor overheden over hoe om te gaan met de mogelijke negatieve gevolgen voor particulieren en bedrijven door de onbereikbaarheid van overheidswebsites als gevolg van een cyberaanval? Zo ja, wordt deze richtlijn door alle provincies gevolgd?

Antwoord 6
De beveiligingsrichtlijn van de overheid de Baseline Informatieveiligheid Overheid (BIO) geeft aan dat maatregelen getroffen moeten worden om DDoS-aanvallen te signaleren en hierop te reageren. Naleving over het volgen van deze richtlijn is een zelfstandige verantwoordelijkheid van provincies waarover zij verantwoording afleggen aan de provinciale staten. Diverse organisaties zoals het Nationaal Cyber Security Centrum (NCSC), de AIVD en ook private organisaties geven technische achtergronden over hoe dit aan te pakken. Het NCSC heeft verschillende kennisproducten uitgebracht die organisaties kunnen helpen bij de mitigatie van DDoS-aanvallen.

Vraag 7
Indien deze richtlijn niet bestaat: kunt u een dergelijke richtlijn laten opstellen? Zo ja, wanneer denkt u een dergelijke richtlijn gereed te hebben? Zo nee, waarom niet?

Antwoord 7
Er bestaat een richtlijn. Hierbij verwijs ik naar de beantwoording in vraag 6.

Vraag 8
Kunt u aangeven hoe vaak overheidswebsites te maken krijgen met DDoS-aanvallen? Hoe vaak worden DDoS-aanvallen succesvol afgeslagen en hoe vaak slagen deze? Wat is de gemiddelde downtime als gevolg van DDoS-aanvallen op overheidswebsites? Zo nee, waarom niet?

Antwoord 8
Er is geen overzicht van DDoS-aanvallen binnen de overheid. Het NCSC ontvangt niet altijd meldingen over DDoS-aanvallen, daardoor beschikt het NCSC niet over een volledig beeld of statistieken. De impact van dergelijke aanvallen is vaak beperkt en symbolisch van aard. Toch kan een DDoS-aanval wel (tijdelijke) invloed hebben op de informatieverstrekking en/of dienstverlening van getroffen websites (zie hiervoor ook de beantwoording in vraag 2).

Vraag 9
Bent u bekend met de Anti-DDoS-coalitie?[2]

Antwoord 9
Ja.

Vraag 10
Maken de rijksoverheid en provincies gebruik van de kennis van deze coalitie om DDoS-aanvallen op hun websites af te slaan? Indien nee, welke niet en waarom niet?

Antwoord 10
Verschillende overheden nemen deel aan de coalitie, waaronder het NCSC en het Digital Trust Center (DTC). BZK en de gezamenlijke provincies hebben in het kader van de tweede Netwerk- en Informatiebeveiligingsrichtlijn (NIS2)[3] het voornemen de provincies aan te sluiten op het NCSC voor de uitvoering van hun Cyber Security Incident Response Team (CSIRT) taken. Zo krijgen zij directe toegang tot actuele dreigingsinformatie vanuit het NCSC. De CSIRT-samenwerking tussen de provincies en het NCSC wordt hierdoor versterkt. Binnen het CSIRT-stelsel wordt reeds actief samengewerkt in geval van dreigingen of incidenten. Hiermee worden niet direct DDoS-aanvallen afgeslagen, maar kan wel tijdig en in samenwerking gereageerd worden op incidenten. Verder zijn de getroffen provincies inmiddels aangesloten op een zogenaamde DDoS-wasstraat. Een wasstraat vergroot de weerbaarheid tegen DDoS-aanvallen door de bundeling van capaciteit, technologie, kennis en kunde.

Vraag 11
Bent u van zins om de provincies te wijzen op het bestaan van de Anti-DDoS-coalitie om de impact van mogelijke toekomstige DDoS-aanvallen te verkleinen? Indien nee, waarom niet?

Antwoord 11
Hierbij verwijs ik naar de beantwoording in vraag 10.

Vraag 12
Kunt u deze vragen afzonderlijk beantwoorden?

Antwoord 12
Ja.

[2] Anti-DDoS-Coalitie, https://www.nomoreddos.org/.
[3] De NIS2-richtlijn beschrijft maatregelen om het niveau van de digitale weerbaarheid van organisaties te verhogen.