Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

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

1882

Vragen van het lid **Bontenbal** (CDA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Volksgezondheid, Welzijn en Sport over *het bericht «Pro-Russische DDoS-aanvallers hebben het gemunt op Nederlandse ziekenhuizen»* (ingezonden 3 februari 2023).

Antwoord van de Ministers **Kuipers** (Volksgezondheid, Welzijn en Sport) en **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 16 maart 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 1674.

Vraag 1
Bent u bekend met het bericht «Pro-Russische DDoS-aanvallers hebben het gemunt op Nederlandse ziekenhuizen»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u toelichten in hoeverre deze aanvallen gevolgen hebben voor de zorg in Nederland? Deelt u onze zorg dat deze cyberaanvallen potentieel ontwrichtende maatschappelijke gevolgen kunnen hebben?

Antwoord 2
Tijdens de DDoS-aanvallen waar het artikel naar verwijst is de zorgcontinuïteit niet in het geding geweest. Tegelijkertijd kunnen diensten die een rol spelen bij de zorg voor patiënten wel verstoord worden door een DDoS-aanval. Het risico hierop wordt mede bepaald door de preventieve maatregelen van de zorgorganisatie, de inrichting van het netwerk en de eigenschappen van de DDoS-aanval. Daarom is het ontzettend belangrijk dat ziekenhuizen digitaal weerbaar zijn en (preventieve) maatregelen nemen om de impact van dergelijke aanvallen te beperken.
Dat cyberaanvallen in ernstigere gevallen potentieel ontwrichtende maatschappelijke gevolgen kunnen hebben is echter zeker het geval, zoals ook al vaker is aangegeven in het jaarlijks gepubliceerde Cybersecuritybeeld

[1] NOS, 30 januari 2023, via https://nos.nl/artikel/2461833-pro-russische-ddos-aanvallers-hebben-het-gemunt-op-nederlandse-ziekenhuizen

ah-tk-20222023-1882
ISSN 0921 - 7398
's-Gravenhage 2023

Nederland.[2] Omdat digitale systemen het «zenuwstelsel» van onze maatschappij vormen, maakt het Kabinet zich hard voor de versterking van onze digitale weerbaarheid via de verschillende ambities die omschreven staan in de Nederlandse cybersecurity strategie.[3]

Vraag 3
Welke acties worden ondernomen om adequaat op deze cyberaanvallen te reageren en de gevolgen voor de zorg in Nederland zoveel mogelijk te beperken? Hoe worden de betreffende ziekenhuizen ondersteund?

Antwoord 3
Ziekenhuizen nemen maatregelen om de gevolgen van een cyberaanval te beperken, en waar nodig zo spoedig mogelijk te mitigeren. Zo hebben ziekenhuizen afspraken met hun ICT-leveranciers over veiligheidseisen aan ICT-producten, en over beheers- en mitigerende maatregelen. Diverse Nederlandse ziekenhuizen maken bijvoorbeeld gebruik van een DDoS-«wasstraat» die ze helpt om DDoS-aanvallen af te kunnen weren.
Alle ziekenhuizen in Nederland die lid van zijn van de Nederlandse Vereniging van Ziekenhuizen (NVZ) of de Nederlandse Federatie van Universitair Medische Centra (NFU) zijn daarnaast aangesloten bij Z-CERT. Z-CERT voorziet de ziekenhuizen van advies en dreigingsinformatie, en kan tevens netwerken monitoren op kwetsbaarheden of verdachte activiteiten. In het geval van een incident kan Z-CERT een ziekenhuis ondersteunen bij het mitigeren van de gevolgen van een cyberaanval. Daarbij heeft Z-CERT onder andere contact met Nationaal Cyber Security Centrum (NCSC).

Vraag 4
Klopt het dat het alleen om DDoS-aanvallen gaat, of is ook sprake van (dreiging van) andersoortige cyberaanvallen?

Antwoord 4
Dat klopt. Er is geen indicatie van een andersoortige cyberaanval.

Vraag 5
Wat zijn de meest effectieve maatregelen om DDoS-aanvallen te pareren?

Antwoord 5
Een combinatie van organisatorische- en technische maatregelen kan effectief een DDoS-aanval pareren. Het NCSC heeft deze maatregelen beschreven in een factsheet, die beschikbaar is op de website.[4]

Vraag 6
Kunt u garanderen dat (overheids)organisaties als Z-CERT die dreigingsinformatie over Russische cyberaanvallen ontvangen dit snel en volledig kunnen delen met betreffende bedrijven en sectoren?

Antwoord 6
In het huidige cybersecuritystelsel is op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni) de primaire taak van het NCSC het verlenen van bijstand aan vitale aanbieders en Rijksoverheidsorganisaties (doelgroeporganisaties) bij digitale dreigingen en incidenten. Dit om het uitvallen van de beschikbaarheid of het verlies van integriteit van netwerk- en informatiesystemen bij de doelgroeporganisaties te voorkomen of te beperken.
Het uitvallen van die netwerk- en informatiesystemen bij deze organisaties kan immers maatschappelijke gevolgen hebben. Denk bijvoorbeeld aan de gevolgen als de dienstverlening van een drinkwaterbedrijf uitvalt. Het NCSC

---

[2] CSBN 2019 (Kamerstuk 26 643, nr. 614),
CSBN 2020 (Kamerstuk 26 643, nr. 695),
CSBN 2021 (Kamerstuk 26 643, nr. 767),
en CSBN 2022 (Kamerstuk 26 643, nr. 891)
[3] NLCS (Kamerstuk 26 643, nr. 925)
[4] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten

deelt daarom zo snel en volledig mogelijk de dreigings- en incidentinformatie direct met de doelgroeporganisaties.
Voor het informeren en adviseren van andere organisaties dan de doelgroeporganisaties over digitale dreigingen en incidenten zijn er schakelorganisaties. Deze maken deel uit van het Landelijk Dekkend Stelsel. In dat stelsel verstrekt het NCSC vanuit zijn wettelijke operationele en coördinerende rol dreigings- en incidentinformatie aan schakelorganisaties om zo ook organisaties buiten de doelgroep van het NCSC te bereiken.
Het is de verantwoordelijkheid van de schakelorganisaties (zoals Z-CERT) om deze informatie zo snel mogelijk met de eigen achterban te delen. De schakelorganisaties zijn het meest bekend met de systemen van hun achterban, bijbehorende belangen, risico's en informatiebehoeften.

Vraag 7
Kunt u dit ook garanderen voor informatie afkomstig uit andere landen dan Nederland, of informatie uit Nederland die betrekking heeft op organisaties in andere landen?

Antwoord 7
Het NCSC staat als nationaal Computer Security Incident Response Team (CSIRT) in contact met het Europese CSIRT netwerk. Binnen dit netwerk wordt informatie over dreigingen en kwetsbaarheden ook zo snel en volledig mogelijk gedeeld

Vraag 8
Zijn er op dit moment wettelijke beperkingen die het delen van dreigingsinformatie bemoeilijken en zo ja, welke zijn dat specifiek?

Antwoord 8
De Wbni regelt dat het NCSC dreigings- en incidentinformatie kan verstrekken aan – in eerste instantie – haar doelgroeporganisaties, namelijk vitale aanbieders en rijksoverheidsorganisaties. Het NCSC doet dat om de meest ernstige maatschappelijke ontwrichting te voorkomen of te beperken. Bovendien kan het NCSC deze informatie aan organisaties verstrekken via schakelorganisaties. Zie ook het antwoord op vraag 6.
Onlangs (december 2022) is de Wbni gewijzigd om belangrijke wettelijke beperkingen voor het delen van informatie weg te nemen.[5] Door deze wijziging kan het NCSC dreigings- en incidentinformatie ook rechtstreeks verstrekken aan organisaties die niet onder de doelgroep van het NCSC vallen of waarvoor geen schakelorganisaties zijn. Denk bijvoorbeeld aan politieke partijen en veiligheidsregio's. Deze wetswijziging regelt ook dat meer dreigings- en incidentinformatie kan worden gedeeld met zogeheten OKTT's (schakelorganisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten).
Daarnaast is de nieuwe Europese richtlijn voor Netwerk- en Informatiebeveiliging (NIB2-richtlijn) in werking getreden. Op dit moment loopt een wetgevingstraject om de richtlijn in Nederlandse wetgeving te implementeren. De Minister van Justitie en Veiligheid zal u hierover nader informeren middels een brief aan uw Kamer in het voorjaar.

Vraag 9
Hoe werkt u in Europa samen om op deze cyberaanvallen, die ook andere landen raken, te reageren? Zijn er zaken die we kunnen leren van andere landen op dit punt?

Antwoord 9
Als Nationaal Computer Emergency Response Team (CERT) staat het NCSC in nauw contact met het speciaal voor de zorg opgerichte Computer Emergency Response Team (Z-CERT) en andere nationale samenwerkingspartners. Het NCSC is ook in contact met internationale (cyber) partners en werkt intensief samen met een uitgebreid (inter)nationaal netwerk van computercrisisteams, zoals het Europese CSIRT netwerk, het International Watch and Warning

[5] Staatsblad 2022, 441

Network (IWWN) en de European Government Cert-Group (EGC). Het NCSC kan, in samenwerking met deze internationale partners, de situatie monitoren en contact onderhouden over de te nemen vervolgacties tijdens incidenten zoals technisch onderzoek ten aanzien van de DDoS-aanvallen.
Ook op diplomatiek niveau is zowel in EU- als NAVO verband gedeeld dat Nederlandse ziekenhuizen zijn getroffen door DDoS-aanvallen. Hiermee dragen we bij aan een gedeeld situationeel bewustzijn bij onze partners.

Vraag 10
Heeft u informatie dat er ook sprake is van een verhoogde cyberdreiging vanuit Russische hackgroepen in andere vitale en/of niet-vitale sectoren? Zo ja, welke sectoren zijn dat en hoe worden betreffende sectoren geholpen om zich hiertegen te wapenen?

Antwoord 10
De kans op gerichte cyberaanvallen op Nederlandse belangen wordt vooralsnog laag ingeschat. Dit dreigingsbeeld lijkt stabiel maar kan abrupt veranderen. Nederlandse organisaties kunnen door ketenafhankelijkheden, bijvoorbeeld via een toeleverancier of dochterbedrijf, geraakt worden als gevolg van cyberaanvallen in relatie tot de oorlog in Oekraïne. Diverse cybersecurity(basis)maatregelen, ten behoeve van het creëren vanhandelingsperspectief om aanvallen te herkennen en voorkomen, zijn aan organisaties ter beschikking gesteld. Zie hiervoor de factsheet van het NCSC zoals benoemd in vraag 5, en ook de AIVD en MIVD publicatie over cyberaanvallen door statelijke actoren.[6]

Vraag 11
Wordt gemonitord welke organisaties en sectoren in andere landen die wapens aan Oekraïne leveren aangevallen worden, zodat deze organisaties en sectoren in Nederland zich op soortgelijke aanvallen kunnen voorbereiden?

Antwoord 11
Ja. Het NCSC monitort soortgelijke aanvallen.

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van de leden Hijink (SP), ingezonden 2 februari 2023 (Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 1881) en Tielen en Rajkowski (beiden VVD), ingezonden 2 februari 2023 (Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 1883).

[6] Publicatie AIVD & MIVD (2021). *Cyberaanvallen door statelijke actoren – zeven momenten om een aanval te stoppen*. link: https://www.aivd.nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen.