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

1881

Vragen van het lid **Hijink** (SP) aan de Minister van Volksgezondheid, Welzijn en Sport over *het bericht «UMCG getroffen door Russische cyberaanval, meer ziekenhuizen onder vuur»* (ingezonden 2 februari 2023).

Antwoord van Minister **Kuipers** (Volksgezondheid, Welzijn en Sport) (ontvangen 16 maart 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 1676.

Vraag 1
Wat is uw reactie op het bericht «UMCG getroffen door Russische cyberaanval, meer ziekenhuizen onder vuur»?[1]

Antwoord 1
Ik vind het zeer zorgelijk dat Nederlandse ziekenhuizen het doelwit zijn van DDoS-aanvallen.

Vraag 2
Zijn er de afgelopen maanden meer van dit soort aanvallen geweest? Zo ja, kunt u vertellen welke ziekenhuizen of andere zorginstellingen hierdoor zijn getroffen?

Antwoord 2
Het digitaal aanvallen van Nederlandse ziekenhuizen door middel van DDoS-aanvallen is niet eerder waargenomen door het Computer Emergency Response Team voor de zorg (Z-CERT), het Nationaal Cyber Security Center (NCSC) of hun (internationale) partners.

Vraag 3
In hoeverre vormen deze aanvallen een risico voor de patiëntenzorg?

Antwoord 3
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

[1] Skipr, 30 januari 2023, «UMCG getroffen door Russische cyberaanval, meer ziekenhuizen onder vuur» (https://www.skipr.nl/nieuws/website-umcg-al-twee-dagen-onbereikbaar-door-cyberaanval/).

ah-tk-20222023-1881
ISSN 0921 - 7398
's-Gravenhage 2023

risico hierop wordt mede bepaald door de preventieve maatregelen van de zorgorganisatie, de inrichting van het netwerk en de eigenschappen van de DDoS-aanval.

Vraag 4
In hoeverre zijn Nederlandse ziekenhuizen in het algemeen voorbereid op cyberaanvallen, zoals DDoS-aanvallen?

Antwoord 4
Ziekenhuizen nemen maatregelen om de gevolgen van cyberaanvallen 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.
Nederlandse ziekenhuizen moeten daarnaast wettelijk verplicht voldoen aan normen voor informatiebeveiliging in de zorg: de NEN 7510, 7512 en 7513. De NEN-7510 schrijft onder andere voor dat ziekenhuizen de risico's voor informatiebeveiliging in kaart brengen en hiervoor passende maatregelen nemen. De norm vereist ook beheersmaatregelen voor de bescherming van netwerken, bedrijfscontinuïteit en bereikbaarheid.
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 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 NCSC.

Vraag 5
In hoeverre zijn ziekenhuizen voorbereid op het wegvallen van IT-systemen? Hoe groot is de kans dat ziekenhuizen helemaal stilvallen bij grotere cyberaanvallen?

Antwoord 5
Zorgaanbieders zijn verantwoordelijk voor het leveren van goede en veilige zorg. Een onderdeel daarvan is dat zij risico's inventariseren en bijpassende maatregelen treffen om deze risico's te beheersen. Een voorbeeld van een risicobeheersmaatregel is een noodscenario om bij uitval van ICT-systemen tijdelijk een alternatieve voorziening te gebruiken.

Vraag 6
Welke acties onderneemt u om ziekenhuizen en andere zorginstellingen te ondersteunen om zich beter tegen cyberaanvallen te beschermen?

Antwoord 6
Bewustwording van risico's en het belang van zorgvuldig handelen door eigen medewerkers is essentieel voor goede informatieveiligheid, ook in de zorg. Ik zet daarom ten eerste in op het stimuleren van informatieveilig gedrag van zorgprofessionals. Daarvoor is het Ministerie van VWS in 2019 het project informatieveilig gedrag gestart. Via dit project werk ik aan een gestructureerde methode voor gedragsverandering op het gebied van informatieveiligheid, toegespitst op de Nederlandse zorgsector. In mijn brief «Voortgang op elektronische gegevensuitwisseling» van 15 december 2022 heb ik uw Kamer hier nader over geïnformeerd.[2]
Daarnaast zorg ik er samen met het zorgveld voor dat we de eerder genoemde NEN-normen voor informatiebeveiliging blijven ontwikkelen, en breng ik deze normen actief onder de aandacht bij zorgaanbieders. Zo heb ik NEN in 2022 de opdracht gegeven om een herziening van de NEN-7510 te coördineren, en daarbij ook *implementatietools* te ontwikkelen.
Ook stimuleert het Ministerie van VWS op basis van een risicogebaseerde aansluitstrategie dat steeds meer zorgaanbieders lid worden van Z-CERT. Op dit moment zijn bijna 300 instellingen uit verschillende sub-sectoren

[2] Kamerstuk 27 529, nr. 288

aangesloten bij Z-CERT. Het Ministerie van VWS blijft zich inzetten om de dienstverlening van Z-CERT zo breed mogelijk beschikbaar te stellen binnen de gehele zorgsector. Daarbij wordt rekening gehouden met het absorptievermogen van Z-CERT.
In januari 2023 heeft het Ministerie van VWS daarnaast samen met ROAZ Zuidwest-Nederland en GHOR Zuid-Holland Zuid een grootschalige oefening georganiseerd. Hierbij is gezamenlijk geoefend met een scenario waarin sprake was van digitale verstoring van onder andere de ziekenhuiszorg. De lessen die hieruit zijn getrokken zullen de komende tijd worden gebruikt om de voorbereiding op dergelijke incidenten te verbeteren.
Tot slot wordt de komende tijd gewerkt aan de implementatie van nieuwe Europese richtlijnen met betrekking tot informatieveiligheid (NIB2) en algemene weerbaarheid (CER). Over de deze implementatie zal ik uw Kamer binnenkort nader informeren.

Vraag 7
Is deze cyberaanval op het Universitair Medisch Centrum Groningen (UMCG) voor u een aanleiding om aanvullende acties te ondernemen om de cyberveiligheid van Nederlandse zorginstellingen te versterken?

Antwoord 7
De cyberaanval op het UMCG onderstreept het belang van de cyberweerbaarheid van de Nederlandse samenleving in zijn geheel, en de zorgsector in het bijzonder. Het vergroten van de cyberweerbaarheid van de Nederlandse samenleving is een van de speerpunten van dit kabinet. In de Nationale Cybersecurity Strategie die in september 2022 is gepresenteerd heeft het Ministerie van VWS ook een aantal aanvullende acties gepresenteerd om de cyberweerbaarheid op peil te houden.