Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021 **Aanhangsel van de Handelingen**

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

3471

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «ISIDOOR 2021: NCTV en NCSC organiseren grootste cybercrisisoefening ooit.»* (ingezonden 14 juni 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 6 juli 2021).

Vraag 1
Bent u bekend met het bericht «ISIDOOR 2021: NCTV en NCSC organiseren grootste cybercrisisoefening ooit»?[1]

Antwoord 1
Ja.

Vraag 2
Is ISIDOOR 2021 naar uw mening succesvol verlopen? Kunt u uw mening toelichten?

Antwoord 2
Ja, ISIDOOR is naar mijn mening succesvol verlopen. Als verantwoordelijk Minister voor deze oefening kijk ik terug op succesvolle oefendagen mede dankzij de inzet van alle deelnemende organisaties. Tijdens ISIDOOR 2021 stond de beoefening van het Nationaal Crisisplan Digitaal centraal en de vele eigen crisisprocedures van de deelnemende organisaties. Het beoefenen van de onderlinge samenhang en samenwerking op basis van deze procedures maakte de oefening waardevol. De preparatie van de oefening heeft daarnaast ook praktische inzichten opgeleverd voor deelnemende organisaties, doordat in deze fase de rol- en taakverdelingen, de crisisstructuren en procedures tegen het licht werden gehouden.
Bij het samenstellen van het scenario, maar ook in de voorbereiding van de deelnemers via masterclasses, is expliciet rekening gehouden met zowel fysieke als digitale effecten. Voor een digitale crisis geldt immers dat die ook fysieke gevolgen kan hebben met een grote maatschappelijke impact.
ISIDOOR heeft mede daardoor bijgedragen aan een betere voorbereiding

[1] Website Nationaal Cyber Security Centrum, 10 juni 2021 (https://www.ncsc.nl/actueel/nieuws/2021/juni/10/isidoor-2021-nctv-en-ncsc-organiseren-grootste-cybercrisisoefening-ooit)

ah-tk-20202021-3471
ISSN 0921 - 7398
's-Gravenhage 2021

indien zich daadwerkelijk een digitaal incident met ook fysieke gevolgen voordoet.

Vraag 3
Hoe is de selectie van deelnemers van ISIDOOR 2021 tot stand gekomen? Welke criteria zijn hierbij gebruikt? Wat was de verhouding vitaal/niet-vitaal?

Antwoord 3
Om tot de deelnemerslijst te komen is allereerst door de departementale projectorganisatie, bestaande uit NCSC en NCTV, een uitvraag gedaan via het zogeheten ISAC-netwerk. Daarin zijn publieke en private organisaties in verschillende sectoren vertegenwoordigd. Vervolgens zijn ook verschillende interdepartementale gremia geattendeerd op de oefening. Zodoende is een lijst van vrijwillige aanmeldingen tot stand gekomen op basis waarvan de definitieve lijst is samengesteld. Deelnemende organisaties waren overwegend organisaties binnen de vitale infrastructuur, onderdelen van de rijksoverheid, veiligheidsregio's en partijen binnen het Landelijk Dekkend Stelsel van Cybersecurity samenwerkingsverbanden. Ook deed een aantal andere samenwerkingsverbanden mee en was het lokale en regionale perspectief in de oefening vertegenwoordigd. De volledigheid van de deelnemerslijst is in interdepartementaal overleg afgestemd. Het belangrijkste criterium voor deelname was de overweging of een organisatie een voorname rol heeft tijdens de aanpak van een nationale crisis, mede gebaseerd op het Nationaal Crisisplan Digitaal en het Nationaal Handboek Crisisbesluitvorming.

Vraag 4
Hoe hebben de deelnemers van ISIDOOR 2021 de oefening ervaren? Komt er een brede evaluatie onder alle deelnemers? Zo ja, op welke termijn en kunt u deze met de Kamer delen? Zo nee, waarom niet?

Antwoord 4
Uiteraard kan ik niet voor de deelnemende organisaties spreken, echter het overheersende beeld is dat er tevreden wordt teruggekeken op de oefening. Het scenario van deze derde (en grootste) editie van ISIDOOR was realistischer dan ooit omdat veel deelnemende organisaties ook via hun oefenleiding betrokken waren bij het bedenken van het scenario. Zo konden zij het hoofdscenario vertalen naar hun eigen achterban en de voor hen relevante oefendoelen uitwerken in het scenario.
Door het Instituut voor Veiligheids- en Crisismanagement (COT) wordt een overkoepelend evaluatierapport geschreven, dat zich richt op de oefendoelen van ISIDOOR 2021. Evalueren is expliciet onderdeel van het programma van ISIDOOR 2021. Er wordt daarom op zowel operationeel technisch niveau als op bestuurlijk niveau geëvalueerd. De overkoepelende evaluatie van het COT verwacht ik na de zomer met uw Kamer te kunnen delen. Ik roep daarnaast alle betrokken organisaties op om ISIDOOR zelf ook te evalueren, zodat de lessen voor de eigen organisaties gesignaleerd worden. Het is immers ook primair de verantwoordelijkheid van alle deelnemende organisaties zelf om de eigen deelname en processen te evalueren.
Zoals recent gemeld aan uw kamer worden de lessen van ISIDOOR 2021 meegenomen bij de actualisering van het Nationaal Crisisplan Digitaal en de doorontwikkeling van dit plan naar een landelijk crisisplan.[2]

Vraag 5
Bent u het ermee eens dat structureel oefenen met cybercrises van essentieel belang is voor (vitale) organisaties om hun cyberveiligheid te vergroten en om digitale ontwrichting te voorkomen? Zo ja, hoe staat het met de uitvoering van de motie-Weverling (Kamerstuk 24 095, nr. 496)? Hoe verhoudt ISIDOOR 2021 zich tot een structureel oefenprogramma conform de motie-Weverling? Met welke frequentie gaan dit soort oefeningen in de toekomst plaatsvinden?

[2] Slotbrief agenda risico- en crisisbeheersing, 30 april 2021 (Kamerstuk 30 821, nr. 129).

Antwoord 5
Ja, gezamenlijk oefenen is van essentieel belang om goed voorbereid te zijn op een cybercrisis. Dat is door het kabinet ook benadrukt in de kabinetsreactie op het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) «Voorbereiden op digitale ontwrichting»[3]. U noemt in dat kader ook naar de motie-Weverling. Daarover kan ik melden dat ISIDOOR 2021 deel uitmaakt van het oefen- en testprogramma dat is uitgewerkt naar aanleiding van de motie-Weverling en het versterkingsprogramma op de Nederlandse Cybersecurity Agenda (NCSA). Ik verwijs u ten aanzien van de uitwerking en de voorgang van het oefen- en testprogramma naar de beantwoording, in mijn brief van 25 mei 2020, van Kamervragen tijdens het Schriftelijk Overleg Cybersecurity. In de beantwoording ben ik in gegaan op de uitwerking van dit programma via de inzet op de verschillende sporen op oefenen[4]. Een nadere uitwerking en eerste voortgang is terug te vinden in de NCSA voortgangsrapportage 2020 die als bijlage is meegezonden per brief van 29 juni 2020[5]. Een eerstvolgende voortgang hiervan is opgenomen in de voortgangsbrief van de Nederlandse Cybersecurity Agenda die op 28 juni jl. naar uw Kamer is verzonden[6].
Ik zal het volgende kabinet adviseren om op basis van de evaluatie van ISIDOOR te kijken naar een juiste frequentie van deze oefening. ISIDOOR is een zeer complexe oefening waarvoor meerjarig veel capaciteit en voorbereidingstijd nodig is, maar het belang om te oefenen om goed voorbereid te zijn indien er toch iets mis gaat is evident. Ik moedig een volgende editie daarom van harte aan en in de tussentijd zet ik via de eerdergenoemde oefensporen in op oefenen.

[3] Kamerbrief evaluatie Citrix-problematiek en reactie rapport WRR (Kamerstuk 26 643, nr. 673)
[4] Kamerstuk 26 643, nr. 685
[5] Cybersecuritybeeld Nederland 2020 (CSBN 2020) en voortgangsrapportage NCSA (Kamerstuk 26 643, nr. 695)
[6] Kamerstuk nr. 11991