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

2653

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Russische hackers trainen voor aanvallen op kritieke infrastructuur»* (ingezonden 5 april 2023).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 17 mei 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 2425.

Vraag 1
Bent u bekend met het bericht dat Russische hackers trainen voor aanvallen op kritieke infrastructuur?[1]

Antwoord 1
Ja.

Vraag 2
Bent u op de hoogte van softwareprogramma's en projecten, zoals Scan-V en Crystal-2V, die als doel hebben om cyberaanvallen (op kritieke infrastructuur) te stimuleren? Herkent het u dit verontrustende beeld van Russische cyberoperaties, gericht op onze vitale infrastructuur, zoals spoorwegen, vliegvelden, en elektriciteitsnetwerken? Zo ja, hoe beoordeelt u dit beeld?

Antwoord 2
Nederland wordt doorlopend geconfronteerd met digitale aanvallen. Dergelijke aanvallen neemt het kabinet uiterst serieus. Staten dienen zich te houden aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte. Rusland heeft een offensief cyberprogramma tegen Nederland. In het Dreigingsbeeld Statelijke Actoren 2 van november 2022 rapporteren AIVD, MIVD en NCTV over Russische dreiging tegen vitale infrastructuur[2]. Russische cyberactoren ondernemen activiteiten die duiden op spionage en op voorbereidingshandelingen voor verstoring en sabotage.
Nederlandse organisaties in vitale sectoren kunnen ook indirect door ketenafhankelijkheden geraakt worden als gevolg van aanvallen in relatie tot de Russische dreiging.

---

[1] NRC, 31 maart 2023, «Russische hackers trainen voor aanvallen op kritieke infrastructuur» (https://www.nrc.nl/nieuws/2023/03/31/russische-hackers-trainen-voor-aanvallen-op-kritieke-infrastructuur-a4160986).

[2] Kamerstuk 30 812 nr. 175.

ah-tk-20222023-2653
ISSN 0921 - 7398
's-Gravenhage 2023

De AIVD ziet daarnaast dat cyberactoren gebruik maken van commerciële software die ook wordt gebruikt door beveiligingsonderzoekers en cybercriminelen, en niet specifiek te herleiden is, om te voorkomen dat hun aanvallen worden ontdekt.
Daarmee past de berichtgeving over het vermeende gebruik van software van een commercieel bedrijf voor het offensieve cyberprogramma van Rusland in het dreigingsbeeld. Het Nationaal Cyber Security Centrum blijft waakzaam voor veranderingen in het dreigingsbeeld.

Vraag 3
Hoe staat het met de versterkte aanpak vitaal? Acht u de toegezegde stappen en acties afdoende in het kader van de Russische voornemens om cyberaanvallen op onze kritieke infrastructuur uit te voeren? Zo ja, kunt u dit toelichten? Zo nee, welke aanvullende acties acht u noodzakelijk?

Antwoord 3
Momenteel werkt het kabinet aan een versterkte aanpak voor de bescherming van de vitale infrastructuur (Aanpak vitaal). Hier wordt uw Kamer voor de zomer nader over geïnformeerd. Binnen de aanpak wordt ingezet op meer rechten en plichten voor alle vitale aanbieders en een verankering hiervan in de wet- en regelgeving. De herziene Network and Information Security (NIS2) richtlijn is hier een belangrijk onderdeel van.
De NIS2-richtlijn versterkt de bescherming van bedrijven en andere organisaties binnen de EU door hen te verplichten een hoog niveau van cyberbeveiliging te hebben. De richtlijn is van toepassing op organisaties in sectoren die van maatschappelijk belang zijn, zoals drinkwater en energie. Uit de richtlijn volgt een zorgplicht die deze organisaties verplicht zelf een risicobeoordeling uit te voeren, op basis waarvan zij passende maatregelen nemen om hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen. Ook schrijft de richtlijn voor dat die entiteiten incidenten binnen 24 uur melden bij de toezichthouder. In het geval van een dergelijk incident moet het ook gemeld worden bij het relevante Computer Security Incident Response Team (CSIRT), zoals het Nationaal Cyber Security Centrum, dat vervolgens hulp en bijstand kan leveren. Organisaties die onder de richtlijn vallen komen ook onder toezicht te staan, waarbij wordt gekeken naar de naleving van de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht.
De komende tijd wordt door het kabinet gewerkt aan de implementatie van de NIS2-richtlijn in Nederlandse wet- en regelgeving.
Het belang van het versterken van de digitale weerbaarheid en het beter beschermen van de vitale infrastructuur komt ook terug in de actielijnen van de vorige maand gepubliceerde Veiligheidsstrategie voor het Koninkrijk der Nederlanden[3].

Vraag 4
Welke maatregelen neemt u om onze vitale infrastructuur beter te beschermen tegen digitale aanvallen via de toeleveringsketen ook wel «supply chain» cyberaanvallen genoemd?

Antwoord 4
Het kabinet deelt de zorgen over cyberaanvallen op leveranciersketens, zoals onder andere is uiteengezet in het Cybersecuritybeeld Nederland 2022 (CSBN 2022)[4].
Mede daarom zet het kabinet dan ook stevig in op het verhogen van de digitale weerbaarheid van Nederland. In oktober 2022 is de Nederlandse Cybersecuritystrategie gepubliceerd. Een van de doelstellingen hiervan is te zorgen dat organisaties in de vitale infrastructuur goed beschermd zijn tegen digitale risico's, en hierin hun belang voor de sector en andere organisaties binnen de keten meenemen. In de hiervoor genoemde Aanpak vitaal is hier

[3] https://www.rijksoverheid.nl/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden.
[4] https://www.rijksoverheid.nl/documenten/rapporten/2022/07/04/cybersecuritybeeld-nederland-2022.

nadrukkelijk aandacht voor. Dit komt tot uiting in verschillende concrete acties, zoals de implementatie van de NIS2 en uitgebreide voorlichtingscampagnes.
Organisaties in de vitale infrastructuur hebben hierbij ook nadrukkelijk een eigen verantwoordelijkheid om hun digitale weerbaarheid op orde te hebben. Dit komt onder andere tot uitdrukking in de zorgplicht van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) ter implementatie van de Network and Information Security (NIS1)[5]-richtlijn, op basis waarvan aanbieders van essentiële diensten technische en organisatorische maatregelen moeten nemen om hun netwerk- en informatiesystemen te beveiligen (artikel 7). De NIS2-richtlijn kent ook een dergelijke zorgplicht, waarbij expliciet uit die richtlijn volgt dat de zorgplicht in enkel geval maatregelen omvat ter beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners (artikel 21, eerste lid, onderdeel d, van de NIS2-richtlijn).
De rijksoverheid is daarbij verantwoordelijk voor het creëren van een systeem waarbinnen organisaties de juiste maatregelen kunnen nemen om hun digitale weerbaarheid te vergroten en daarmee hun continuïteit en betrouwbaarheid te borgen.
Om de risico's van organisaties te beperken is er de afgelopen periode door het Nationaal Cyber Security Centrum en de Nationaal Coördinator Terrorismebestrijding en Veiligheid steeds nadruk gelegd op het belang van cyberweerbaarheid en waakzaamheid. Ook worden actuele dreigingsbeelden regelmatig gedeeld met organisaties in vitale sectoren.
Om voorbereid te zijn op een crisis in het digitale domein is het Landelijk Crisisplan Digitaal opgesteld (LCP-Digitaal). Het LCP-Digitaal is het overkoepelende kader dat overheden en bedrijven gebruiken voor de inrichting van de eigen cybercrisisplannen. In het LCP-Digitaal wordt ook aandacht besteed aan ketenafhankelijkheid in relatie tot digitale crises. Het LCP-Digitaal is op 23 december 2022 met uw Kamer gedeeld.[6] Ook wordt er geoefend met ketenafhankelijkheden, bijvoorbeeld in de nationale cybercrisisoefening ISIDOOR.
Concreet adviseert het Nationaal Cyber Security Centrum om de basismaatregelen in acht te nemen die te vinden zijn op www.ncsc.nl. Voorbeelden hiervan zijn het installeren van updates, het regelmatig maken van back-ups, en het versleutelen van gevoelige bedrijfsinformatie. Ook informeert het Nationaal Cyber Security Centrum organisaties binnen de vitale infrastructuur over digitale dreigingen via de toeleveringsketen.

Vraag 5
Kunt u een update geven over de voortgang en de uitkomsten van het overheidsbreed cyberprogramma? In hoeverre is Nederland voorbereid op eventuele cyberaanvallen?

Antwoord 5
Zie antwoord bij vraag 7.

Vraag 6
Hoe frequent wordt er binnen de vitale sectoren geoefend met het anticiperen op digitale aanvallen op onze vitale infrastructuur? Wordt hierbij ook geoefend op scenario's van uitval van kritieke diensten? Zo nee, waarom niet?

Antwoord 6
Op nationaal niveau wordt er circa eens in de twee jaar de grootschalige publiek-private cyberoefening ISIDOOR georganiseerd, waaraan organisaties uit de vitale infrastructuur deelnemen. Tijdens deze cyberoefening worden afspraken, structuren en processen uit het Landelijk Crisisplan Digitaal beoefend. Hierbij wordt ook op scenario's geoefend van uitval kritieke diensten, met de nadruk op digitale veiligheid. Ook worden er (cross-)

[5] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:32016L1148.
[6] https://www.rijksoverheid.nl/documenten/rapporten/2022/12/23/tk-bijlage-landelijk-crisisplan-digitaal.

sectorale oefeningen gehouden en is onder andere het Nationaal Cyber Security Centrum tijdens verschillende oefeningen actief betrokken. Voor zowel ISIDOOR als (cross-)sectorale cyberoefeningen wordt samengewerkt met andere ministeries.

Vraag 7
Wanneer was de laatste digitale oefening op cyberaanvallen en welke lessen zijn hieruit getrokken? Wat zijn de vervolgstappen om beter voorbereid te zijn op eventuele cyberaanvallen?

Antwoord 7
Sinds 2019 organiseert het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties jaarlijks in oktober, tijdens de maand van de cybersecurity, een cyberoefening van en voor de overheid. Deze overheidsbrede cyberoefening is aanvullend op wat verschillende bestuurslagen zelf al organiseren. Een voorbeeld hiervan zijn de oefenpakketten van de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG)[7]. Ook tijdens de coronapandemie zijn deze oefeningen georganiseerd en sindsdien zijn zij online te volgen. Vanaf 2022 is er naast een centraal te volgen crisisoefening ook de mogelijkheid om simultaan met de eigen organisatie mee te oefenen. Aan de meest recente oefening van oktober 2022 namen meer dan 70 overheidsinstanties deel aan het simultaan oefenen. Daarnaast volgden nog ruim 450 mensen de livestream van de centrale crisisoefening. Nadere informatie is te vinden op www.weerbaredigitaleoverheid.nl.
Inmiddels zijn ook drie edities van cybercrisisoefening ISIDOOR georganiseerd, dit is een door het Ministerie van Justitie en Veiligheid georganiseerde grootschalige oefening voor zowel publieke als private partijen. De laatste editie, ISIDOOR III, vond plaats in juni 2021. De lessen uit ISIDOOR III zijn gedeeld met uw Kamer[8], en zijn meegenomen in het Landelijk Crisisplan Digitaal (LCP-Digitaal). Deze lessen en aanbevelingen zagen onder andere toe op het vergroten van inzicht in rollen en routes in de crisisbeheersing, in zorgvuldigheid en snelheid van informatiedeling en crisisrespons, in het optimaal benutten van capaciteit en expertise en het samen met partners blijven werken aan de voorbereiding op cybercrises. Een nieuwe versie van het plan is eind december 2022 aangeboden aan de Kamer.[9]
Het LCP-Digitaal vormt de basis voor de volgende editie van ISIDOOR: ISIDOOR IV. Jaarlijks zal worden bezien of het LCP-Digitaal actualisatie behoeft, onder andere aan de hand van de nieuwe geleerde lessen uit incidenten en oefeningen (waaronder ISIDOOR IV) en andere relevante ontwikkelingen.
In februari 2023 vond ook een cross-sectorale digitale oefening plaats, waarin publieke en private organisaties getest hebben hoe goed hun systemen bestand zijn tegen zowel zware als ook slimmere DDoS-aanvallen. Traditionele DDoS-aanvallen zijn aanvallen waarbij een systeem wordt overladen met verzoeken, waardoor deze onbereikbaar wordt. Bij een slimme aanval krijgen de servers andere, zwaardere taken te vervullen, waardoor de capaciteit voor normaal gebruik wordt opgeslokt. De oefening werd georganiseerd tussen leden van de Anti-DDoS-Coalitie. Dit is een publiek-privaat samenwerkingsverband waar onder andere het Nationaal Cyber Security Centrum bij betrokken is

Vraag 8
Bent u het met de stelling eens dat het belangrijk is om regelmatig te oefenen met het bestrijden van cyberaanvallen zodat Nederland voorbereid is op actuele dreigingen? Zo ja, wanneer is de eerstvolgende cross-sectorale cyberoefening? Welke oefeningen staan gepland op de langere termijn? Hoe staat het met structureel organiseren van cross-sectorale cyberoefeningen? Zo nee, waarom niet?

---

[7] https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/.
[8] https://www.rijksoverheid.nl/documenten/rapporten/2021/09/14/tk-bijlage-isidoor-2021-evaluatierapportage.
[9] https://www.rijksoverheid.nl/documenten/rapporten/2022/12/23/tk-bijlage-landelijk-crisisplan-digitaal.

Antwoord 8
Effectieve crisisbeheersing vergt behalve gezamenlijke voorbereiding ook oefening. Het Ministerie van Justitie en Veiligheid heeft daarom een oefenprogramma ontwikkeld en in gebruik laten nemen. Dit is op 12 juni 2019 met uw Kamer gedeeld[10].
In dat programma wordt op drie sporen ingezet: het organiseren van grootschalige oefeningen, deelname van de overheid aan bestaande cyberoefeningen en het ontwikkelen van initiatieven op oefenen in publiek-privaat verband. Deze inzet blijft belangrijk onder de in oktober 2022 gepubliceerde Nederlandse Cybersecuritystrategie, waarin het belang wordt benadrukt van snel en adequaat reageren op cyberincidenten en -crises.
De oefening ISIDOOR vindt eens per twee jaar plaats. De organisatie van ISIDOOR IV is op dit moment al begonnen en in volle gang. De oefening zal naar verwachting eind 2023 plaatsvinden. Voor de meeste (cross-)sectorale oefeningen is geen vaste frequentie. De onder vraag 7 genoemde Anti-DDoS-coalitie beoogt om twee keer per jaar een oefening te organiseren over het omgaan met DDoS-aanvallen. Jaarlijks blijft ook de overheidsbrede cyberoefening plaatsvinden voor medeoverheden, waar ook bedrijven mogen aanhaken.

[10] Kamerbrief Beleidsreactie Cybersecuritybeeld Nederland 2019 en voortgangsrapportage Nederlandse Cybersecurity Agenda | Kamerstuk | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl).