Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

2166

Vragen van het lid **Hammelburg** (D66) aan de Minister van Defensie en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht dat de meest recente cyberaanval in Oekraïne verliep via Nederland* (ingezonden 17 februari 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid), mede namens de Minister van Defensie en Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 21 maart 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2014.

Vraag 1
Bent u bekend met het bericht van BNR «Cyberaanval Oekraïne verliep via Nederland»?[1]

Antwoord 1
Ja.

Vraag 2
Hoe oordeelt u over dit bericht?

Antwoord 2
Nederland heeft een relatief grote hosting sector. Dit heeft te maken met de uitstekende digitale infrastructuur waarover Nederland beschikt: het internet is hier van hoge kwaliteit, snel en goedkoop. Zowel nationaal als internationaal maken personen, bedrijven en organisaties gebruik van de diensten die deze hosting bedrijven aanbieden. Helaas maken ook kwaadwillende actoren (criminelen en staten) misbruik van Nederlandse hosting providers.

Vraag 3
Van wat voor aanval was hier sprake? Klopt het dat een DdoS-aanval werd gecombineerd met een desinformatieaanval?

Antwoord 3
Op 15 februari 2022 vonden diverse digitale aanvallen op verschillende doelwitten in Oekraïne plaats. Het ging onder andere om DDoS-aanvallen (Distributed Denial of Service) die ingezet worden om de capaciteit van online

[1] https://www.bnr.nl/nieuws/internationaal/10467674/cyberaanval-oekraine-verliep-via-nederland

ah-tk-20212022-2166
ISSN 0921 - 7398
's-Gravenhage 2022

diensten of de ondersteunende servers en netwerkapparatuur te raken. Het Oekraïense Ministerie van Defensie en twee nationale banken in Oekraïne werden getroffen. Op 15 februari 2022 vond ook een sms-campagne plaats, met de boodschap dat geldautomaten technische storingen zouden hebben. Officiële kanalen in Oekraïne geven aan dat dit desinformatie was. Er zou geen sprake zijn van dergelijke storingen.

Vraag 4
Hoeveel cyberaanvallen zijn er op Oekraïne geweest sinds het uitbreken van de oorlog in 2014?

Antwoord 4
Dit valt niet te zeggen. Oekraïne vormt namelijk al vele jaren doelwit van Russische cyberoperaties. De afgelopen maand zijn de digitale aanvallen op Oekraïne veel in het nieuws geweest. Op de website van het Nationaal Cyber Security Centrum (NCSC) is een tijdlijn terug te vinden met digitale aanvallen in relatie tot de huidige spanningen tussen Rusland en Oekraïne: Digitale aanvallen Oekraïne: een tijdlijn | Nieuwsbericht | Nationaal Cyber Security Centrum (ncsc.nl)

Vraag 5
Hoeveel van deze aanvallen liepen via Nederland?

Antwoord 5
Dit valt niet te zeggen. Dergelijke digitale aanvallen worden uitgevoerd vanuit command and control servers. Deze staan wereldwijd in datacenters, waaronder ook in Nederland. Voor datacenters is het vrijwel onmogelijk om te controleren welke servers voor dergelijke malafide doeleinden worden ingezet. Voor elke aanval zou specifiek technisch onderzoek nodig zijn om te achterhalen via welke servers een aanval is uitgevoerd. Dergelijk technisch onderzoek is niet bij elke aanval mogelijk, vanwege de capaciteit die dit kost en het aantal (pogingen tot) aanvallen.

Vraag 6
Welke risico's loopt Nederland in het geval een cyberaanval via Nederlandse servers loopt?

Antwoord 6
Zoals aangegeven in het antwoord op vraag 5 kunnen command and control servers geografisch overal ter wereld staan, ook in Nederland. Misbruik van Nederlandse infrastructuur bij het uitvoeren van digitale aanvallen komt vaker voor. Deze vorm van misbruik kan het internationale imago van Nederland schaden en slecht zijn voor bondgenootschappelijke belangen en de integriteit van de Nederlandse ICT-infrastructuur. Ook kunnen Nederlandse organisaties geraakt worden door eventuele tegenacties, zoals het uit de lucht halen van misbruikte infrastructuur door landen die door een digitale aanval getroffen zijn. Ook kunnen bedrijven waarvan IT apparatuur onbewust deel uitmaakt van een DDoS aanval daar beschikbaarheidsproblemen door ervaren. Er kunnen verbindingsproblemen optreden en ook kan een internet provider de verbinding afsluiten.
Nederland komt alleen als doelwit in beeld als onderdeel van EU/NAVO, wanneer er escalatie op mondiaal niveau plaatsvindt. Ook als Nederland niet primair doelwit is, blijft het risico van nevenschade bestaan. Dit is bijvoorbeeld het geval wanneer gebruikte malware «wormable»[2] is, met als bekendste voorbeeld NotPetya 2017[3]. Op dit moment zijn er voor zover bekend geen incidenten op dit vlak.
Het NCSC heeft op dit moment geen indicaties dat de aanvallen gevolgen hebben gehad voor Nederlandse belangen of organisaties. Ook zijn er op dit moment nog altijd geen indicaties bekend van grootschalige of ongecontro-

[2] Wormable malware is kwaadaardige code die zichzelf, zonder tussenkomst van een mens, vermenigvuldigt en verspreidt over verschillende digitale systemen.
[3] NotPetya (2017) is een bekend voorbeeld van wormable malware waarbij de initiële besmetting waarschijnlijk via een update van de boekhoudsoftware van een Oekraïens softwarebedrijf wereldwijd spillover effecten heeft gehad waaronder op de APM terminals in Rotterdam.

leerde verspreiding van malware buiten Oekraïne of van andere digitale incidenten met impact op Nederlandse belangen.

Vraag 7
Wat doet Nederland om deze aanvallen te stuiten?

Antwoord 7
Om aanvallen te stoppen kan, zodra duidelijk is om welke partij het gaat, een vordering of bevel worden uitgevaardigd naar de hoster om de server van de betreffende malafide afnemer offline te brengen. In de praktijk is een andere route gebruikelijk, waarbij een «notice and take down» (NTD)-verzoek naar de betreffende hoster wordt gestuurd met de mededeling dat er binnen zijn netwerk sprake is van onrechtmatige handelingen van een of meer afnemers van diens diensten.
Het NCSC heeft primair tot taak om organisaties die deel uitmaken van de rijksoverheid en vitale aanbieders bijstand te verlenen bij digitale dreigingen en incidenten. Daarnaast heeft het NCSC ook als taak het informeren van andere organisaties over dergelijke dreigingen en incidenten betreffende de rijksoverheid en vitale aanbieders. In het kader daarvan werkt het NCSC samen met andere veiligheidspartners in binnen- en buitenland, waaronder de samenwerking in de Cyber Intel/info Cel (CIIC), waarin NCSC, AIVD, MIVD, de politie en het OM informatie over cyberdreigingen en -incidenten bijeenbrengen en medewerkers van die organisaties die informatie gezamenlijk beoordelen ten behoeve van het versterken van het landelijk situationeel beeld en het bieden van handelingsperspectief aan belanghebbende partijen.
De AIVD en de MIVD doen onderzoek naar de dreiging die uitgaat van landen met een offensief cyberprogramma gericht tegen Nederland of Nederlandse belangen. Deze landen maken gebruik van veel verschillende digitale infrastructuur, waaronder die van Nederland, en wisselen daar snel tussen. Het onderzoek van de diensten is er onder andere op gericht om misbruik van Nederlandse infrastructuur te onderkennen.
Zoals eerder gemeld, wordt gewerkt aan een oplossing voor de knelpunten in het cyberdomein die de diensten ondervinden. De Ministers van Defensie en van Binnenlandse Zaken en Koninkrijksrelaties zullen, daarbij de motie van de heer Van der Staaij indachtig, zo snel mogelijk met een wetsvoorstel komen.[4]
Momenteel bezien het NCSC en het Digital Trust Center (DTC) samen met de hosting sector in de Anti-Abuse Network coalitie waar het mogelijk is om in ruimere mate informatie over kwetsbaarheden te delen. Daarnaast wordt binnen de genoemde sector het Clean Networks initiatief ontwikkeld, waarin van hosters wordt gevraagd zich in te spannen om hun netwerken schoon te houden van onrechtmatigheid door zich op private informatiebronnen, zoals die van de stichting Nationale Beheersorganisatie Internet Providers (NBIP), aan te sluiten.
Met betrekking tot DDoS aanvallen zet het Ministerie van Economische Zaken en Klimaat (EZK), en in het bijzonder het DTC, voornamelijk in op preventieve maatregelen die bijdragen aan het voorkomen dat IT-apparatuur, vaak onbewust, deel kan uitmaken aan een DDoS aanval. Het tijdig installeren van beveiligingsupdates is hierbij cruciaal. Het DTC heeft het belang van updaten opgenomen in de 5 Basisprincipes van veilig digitaal ondernemen en informeert de doelgroep van het niet-vitale bedrijfsleven wanneer belangrijke updates beschikbaar zijn in relatie tot ernstige beveiligingsproblemen. Ook IoT-apparaten (Internet of Things) worden ingezet om deel uit te maken van een DDoS aanval. Door de toename van IoT-apparatuur zet het Ministerie van EZK in op updaten middels de «doe je update» campagne. Deze campagne is met name gericht op consumenten zodat zij zich ook bewust zijn van de risico's en de noodzaak om IoT apparaten zoals routers, camera's en printers up-to-date te houden.

Vraag 8
Loopt Nederland meer risico voor cyberaanvallen, omdat het een hubfunctie heeft voor digitaal verkeer van grote delen van Europa?

[4] Kamerstuk 34 588, nr. 91, 24 februari 2022

Antwoord 8
Dit is op voorhand niet te zeggen. Er zijn geen aanwijzingen dat het gebruik van infrastructuur/servers in Nederland berust op een bepaalde strategische keuze van een kwaadwillende actor. Nederland is niet het enige Europese land met een goede infrastructuur, betrouwbare verbindingen en een grote hosting-sector die dit predicaat opeist. Het is niet duidelijk welke strategische afwegingen digitale aanvallers maken om de keuze te maken voor Nederland ten opzichte van andere landen met een eveneens uitstekende ICT-infrastructuur en hubfunctie.
Zie ook het antwoord op vraag 6.

Vraag 9
Is er een link te leggen tussen deze cyberaanvallen en de digitale steun die Nederland heeft aangeboden aan Oekraïne?

Antwoord 9
Het is te voorbarig om een dergelijke link te leggen wanneer attributie uitsluitend gebaseerd lijkt te zijn op het feit dat de tijdsspanne tussen de twee gebeurtenissen beperkt is.[5] Het is bijvoorbeeld niet te zeggen wie precies de servers heeft gehuurd voor de genoemde activiteiten.

Vraag 10
Zijn er, naast de cyberaanvallen op Oekraïne via Nederland, ook andere landen die periodiek worden aangevallen via Nederland?

Antwoord 10
Zoals aangegeven in het antwoord op vraag 5 en 6 worden dit soort digitale aanvallen uitgevoerd vanuit command en control servers. Deze staan wereldwijd in datacenters, waaronder ook in Nederland. Voor datacenters is het vrijwel onmogelijk om te controleren welke servers in Nederland worden ingezet voor dergelijke malafide doeleinden en richting welke landen.

Vraag 11
Kunt u deze vragen afzonderlijk beantwoorden?

Antwoord 11
Ja.

[5] Attributie in deze context betreft het duiden dat een bepaalde organisatie of groep aanvallers een aanval heeft uitgevoerd of dat heeft proberen te doen.