Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

36 045 Situatie in de Oekraïne

Nr. 40 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 maart 2022

Aanleiding

In het debat over de situatie in Oekraïne van 28 februari 2022 (Handelingen II 2021/22, nr. 56, debat over de situatie in de Oekraïne) zijn vragen gesteld onder andere over de Nederlandse paraatheid in het cyberdomein en de cyberdreiging die voortkomt uit het huidige conflict.
Met deze brief informeert de Minister van Justitie en Veiligheid, mede namens de Minister van Defensie en de Minister van Binnenlandse Zaken en Koninkrijksrelatiesuw Kamer over de cyberdreiging die voortkomt uit de Russisch-Oekraïense oorlog en de stappen die worden genomen om eventuele dreiging of nevenschade in Nederland te voorkomen en te mitigeren. Onderstaande situatieschets is gebaseerd op open bronnen.

Situatieschets

De Russische militaire invasie in Oekraïne gaat gepaard met incidenten in het cyberdomein. Sinds 13 januari 2022 zijn diverse aanvallen en aanvalstypen in het conflict waargenomen, uitgevoerd door verschillende partijen.

- De websites van Oekraïense (overheids)instellingen zijn meermaals aangevallen, om ze te bekladden (defacement) of om deze ontoegankelijk te maken middels een DDoS-aanval.[1] Hierbij is ook gebruik gemaakt van een Nederlandse server. Daarnaast zijn Russische overheids- en mediawebsites recent doelwit geweest van DDoS-aanvallen.
- Verschillende typen malware zijn waargenomen in het conflict. Dit betreft met name nieuwe wiper malware die waargenomen is bij Oekraïense instellingen en bedrijven. In een geïnfecteerde computer verwijdert een wiper alle bestanden van de harde schijf.

[1] Met een (Distributed) Denial-of-Service (DDoS) aanval wordt de capaciteit van online diensten of de ondersteunende servers en netwerkapparatuur aangevallen. Hierdoor kunnen online diensten slecht of helemaal niet meer bereikbaar zijn.

kst-36045-40
ISSN 0921 - 7371
's-Gravenhage 2022

- Hackerscollectieven en niet-statelijke actoren hebben in open bronnen kenbaar gemaakt zich in het conflict te mengen. Ze richten zich tegen Rusland of tegen Oekraïne en westerse overheden. Inmiddels worden actief aanvallen uitgevoerd door deze collectieven. De inmenging van deze groeperingen maakt het dreigingsbeeld onvoorspelbaarder. Aanvallen kunnen (verkeerd) geïnterpreteerd worden en toegeschreven worden aan statelijke actoren. Statelijke actoren kunnen op hun beurt de eigen activiteiten verhullen door aanvallen toe te dichten aan deze hackerscollectieven.

Momenteel zijn er nog geen concrete aanwijzingen dat digitale aanvallen in relatie tot de oorlog in Oekraïne impact hebben op Nederland. Het kan echter niet uitgesloten worden dat toekomstige cyberaanvallen effect hebben in Nederland, of dat deze gericht zijn tegen de Nederlandse belangen. Nederlandse instellingen kunnen onbedoeld doelwit worden van een aanval. Ook zijn gerichte aanvallen mogelijk als vergelding voor bijvoorbeeld sancties. Daarnaast staat de Nederlandse digitale infrastructuur internationaal bekend als stabiel en robuust, deze kan door deelnemers aan het conflict misbruikt worden voor het uitvoeren van digitale aanvallen.

Bestuurlijke en operationele respons

De digitale dimensie rondom de Russisch-Oekraïense oorlog wordt continu gemonitord door betrokken Nederlandse overheidsinstellingen, in nauwe samenwerking met onze internationale partners.
De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) houdt specifiek oog voor mogelijke effecten van cyberaanvallen op de nationale veiligheid en coördineert samen met het Nationaal Cyber Security Centrum (NCSC) de afstemming tussen verschillende overheidspartners over analyses en duiding en eventuele maatregelen. Deze analyses, duiding en maatregelen worden, waar nodig en mogelijk, gedeeld met belanghebbende overheidsorganisaties en bedrijfsleven.
Het NCSC heeft op zijn website een tijdlijn geplaatst over de waargenomen ontwikkelingen en de mogelijke effecten in Nederland. Daarnaast heeft het NCSC op de website algemene adviezen geplaatst met daarin maatregelen en handelingsperspectieven in relatie tot specifieke dreigingen als ransomware/wiperware, DDoS-aanvallen, (spear)phishing. Daarnaast worden algemene maatregelen beschreven, zoals over de organisatie van incident respons.
In dit kader onderzoeken de Algemene Inlichtingen en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen en Veiligheidsdienst (MIVD) digitale aanvallen van statelijke actoren en kunnen op basis hiervan andere partijen informeren en in staat stellen mitigerende maatregelen te nemen. Ook levert de AIVD handelingsperspectief voor belanghebbende organisaties over hoe zij zich kunnen beschermen tegen cyberaanvallen van statelijke actoren. Deze weerbaarheidsadviezen zijn specifiek gebaseerd op inlichtingenonderzoek en worden nauw afgestemd met o.a. het NCSC en via de Cyber Intel Info Cel (CI-IC).[2]
Zoals in de jaarverslagen van de AIVD en de MIVD aangegeven, beschikt de Russische federatie over de capaciteiten en intenties om digitale aanvallen uit te voeren. Indien de inlichtingen- en veiligheidsdiensten over informatie beschikken waar zij de Tweede Kamer niet in het openbaar over kunnen informeren, zullen hiertoe de daarvoor geëigende kanalen worden gebruikt.
Ook het Ministerie van Defensie houdt de situatie nauwlettend in de gaten en is in directe verbinding met nationale partners en internationale

[2] De Cyber Intel Info Cel is een samenwerkingsverband op één fysieke locatie tussen AIVD, MIVD, het Openbaar Ministerie, de Nationale Politie en het NCSC.

bondgenoten. Zo kan informatie over cyberoperaties gericht op de krijgsmacht en op bondgenoten snel worden gedeeld en zo nodig worden gemitigeerd. Om partners te helpen heeft Defensie permanent capaciteit beschikbaar. Ook heeft Defensie enkele cyberspecialisten tijdelijk gedetacheerd naar de NAVO om de verbinding tussen het ministerie en de NAVO zo kort mogelijk te houden.
Wij hebben uw Kamer nog recentelijk geïnformeerd over het EU PESCO project *Cyber Rapid Response Teams* (Kamerstuk 36 045, nr. 3). Het team is nog steeds geactiveerd maar nog niet ingezet. De leiding van het team staat in contact met de Oekraïense overheid, maar tot op heden is daar nog geen concrete actie uit voort gekomen.
Met betrekking tot de Nederlandse server die misbruikt is voor het uitvoeren van een aanval op de Oekraïense overheid is door de Nationale Politie een «notice and take down» (NTD)-verzoek uitgevaardigd. De betreffende server is daarop offline gehaald. De beantwoording van de vragen van het lid Hammelburg (D66) over dit incident zullen spoedig aan uw kamer worden verzonden.

Vervolg

Analyses over de cyberdreiging rondom het conflict in Oekraïne en bovenbedoelde adviezen over maatregelen zullen continu worden geactualiseerd. Het NCSC blijft nauw contact onderhouden met Rijksorganisaties, vitale aanbieders en cybersecuritypartners in binnen- en buitenland. Op de website van het NCSC wordt steeds het meest actuele algemene handelingsperspectief gepubliceerd.
De situatie onderstreept eens te meer het belang om Nederland te beschermen tegen landen met een offensief cyberprogramma, zoals Rusland. Zoals al eerder gemeld, wordt gewerkt aan een oplossing voor de knelpunten in het cyberdomein die de AIVD en MIVD ondervinden. De Ministers van Defensie en van Binnenlandse Zaken en Koninkrijksrelaties zullen, daarbij de motie van de heer Van der Staaij indachtig (Kamerstuk 36 045, nr. 16), zo snel mogelijk met een wetsvoorstel komen.[3]
Er is op dit moment geen sprake van crisisopschaling op het cyberdomein. De reguliere lijnen voor ambtelijke en bestuurlijke afstemming worden gebruikt. In interdepartementaal overleg wordt de situatie ten aanzien van de ontwikkelingen in Oost-Europa nauwlettend gemonitord en daarbij de mogelijke gevolgen voor de Nederlandse nationale veiligheid in kaart gebracht zodat deze kunnen worden gekoppeld aan handelingsperspectief, indien dat nodig blijkt. Afhankelijk van de ontwikkeling van de situatie worden partijen aan dit overleg toegevoegd. Indien zich nieuwe ontwikkelingen voordoen zullen wij uw Kamer daarover informeren.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

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