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

2623

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Oekraïense centrales slaan cyberaanval af»* (ingezonden 14 april 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 4 mei 2022).

Vraag 1
Bent u bekend met het bericht «Oekraïense centrales slaan cyberaanval af»?[1]?

Antwoord 1
Ja.

Vraag 2
Klopt het bericht dat Russische hackers een mislukte aanval op Oekraïense energiecentrales hebben uitgevoerd?

Antwoord 2
In publieke berichtgeving van het Oekraïense «Computer Emergency Response Team» (CERT-UA) en het beveiligingsbedrijf ESET wordt dit beeld geschetst.[2] [3] Hoewel dit zeer voorstelbaar is, is technische attributie complex en kan het bericht daarom niet met zekerheid door het kabinet worden bevestigd.

Vraag 3
Wat is bij u bekend over de nieuwste malware vorm «Industroyer» en de aan Russische veiligheidsdiensten gelieerde groep «Sandworm»? Is bekend welke veiligheidsmaatregelen moeten worden genomen tegen deze nieuwe malware? Zo ja, worden hier al stappen voor gezet? Zo nee, waarom niet?

Antwoord 3
Industroyer is kwaadaardige software die in 2016 is ingezet in Oekraïne om een gedeelte van de elektriciteitsvoorziening uit te schakelen. Het recent gebruikte Industroyer2 is een nieuwe variant van deze malware.

---

[1] Telegraaf, 12 april 2022 (https://www.telegraaf.nl/financieel/1074154850/oekraiense-centrales-slaan-cyberaanval-af?utm_internal=telegraaf-paywall-login-eigensite).
[2] https://cert.gov.ua/article/39518
[3] https://blog.eset.ie/2022/04/12/industroyer2-industroyer-reloaded/

ah-tk-20212022-2623
ISSN 0921 - 7398
's-Gravenhage 2022

De digitale aanval wordt door beveiligingsbedrijf ESET en CERT-UA met een hoge mate van zekerheid toegeschreven aan de Sandworm-groep. Deze groep wordt door Amerikaanse en Britse overheidsinstanties geacht gelieerd te zijn aan de Russische militaire inlichtingendienst de GRU en is door de EU in 2020 op de cybersanctielijst gezet.[4] In Nederland doen inlichtingen- en veiligheidsdiensten onderzoek naar statelijke actoren. Over dergelijke inlichtingenonderzoeken wordt doorgaans niet publiekelijk gecommuniceerd. De Industroyer2-malware is specifiek geconfigureerd om een Oekraïense energieleverancier aan te vallen. Aanvullend handelingsperspectief tegen deze malware is niet bekend, omdat de genomen maatregelen niet van toepassing zullen zijn op andere organisaties vanwege deze specifieke configuratie. Het Nationaal Cyber Security Centrum (NCSC) adviseert in algemene zin waakzaam te blijven en de basismaatregelen te treffen die op de website van het NCSC zijn gepubliceerd.[5]

Vraag 4
Is de gebruikte malware «Industroyer» ook al gebruikt als cyberaanval op Nederlandse organisaties? Zo ja, waar is deze malware gebruikt? Zo nee, verwacht u cyberaanvallen met de malware «Industroyer» op Nederlandse organisaties in de nabije toekomst?

Antwoord 4
Op dit moment zijn er bij het NCSC geen aanwijzingen van de inzet van een van de varianten van Industroyer in een cyberaanval op Nederlandse organisaties.
Toekomstige aanvallen en eventuele gevolgen daarvan voor Nederland kunnen echter niet worden uitgesloten. Daarom is het belangrijk dat ook Nederlandse organisaties waakzaam en alert blijven en zich voorbereiden op een mogelijk incident.

Vraag 5
Is er verhoogde paraatheid bij onze vitale aanbieders om een eventuele (indirecte) aanval met Industroyer af te wenden? Zo nee, waarom niet?

Antwoord 5
Ja. Het NCSC staat mede met oog op deze casus, samen met veiligheidspartners (onder andere met cybersecuritybedrijven en via de Cyber Intel/Info Cel), in nauw contact met vitale aanbieders in de energiesector.[6] Op 13 april jongstleden heeft het NCSC relevante vitale aanbieders geïnformeerd over Industroyer2. Vanwege de eerdere variant van Industroyer uit 2016 heeft dit type malware al langer de aandacht van het NCSC.

Vraag 6
Zijn er sinds de oorlog in Oekraïne al voorbeelden waarbij Russische hackers grootschalige cyberaanvallen uitvoeren op Nederlandse vitale bedrijven? Zo ja, hoe zijn deze cyberaanvallen verlopen? Zo nee, hoe groot acht u de kans dat deze bedrijven binnen korte tijd getroffen zullen worden door een grootschalige Russische cyberaanval?

Antwoord 6
Op basis van de huidige beschikbare informatie, kan geconcludeerd worden dat er vooralsnog geen grootschalige Russische cyberaanvallen op Nederlandse vitale bedrijven zijn uitgevoerd. Het NCSC houdt de situatie sinds de oorlog en de aanloop daarnaartoe nauwlettend in de gaten en heeft intensief contact met de inlichtingen- en veiligheidsdiensten.
Wel is het voorstelbaar dat Nederlandse belangen direct of indirect geschaad kunnen worden door digitale activiteiten omtrent de oorlog in Oekraïne. Het NCSC is dan ook waakzaam op eventuele veranderingen in de digitale dreiging richting Nederlandse belangen.

---

[4] Besluit (GBVB) 2020/1127 van de Raad van 30 juli 2020 tot wijziging van Besluit (GBVB) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.
[5] https://www.ncsc.nl/onderwerpen/basismaatregelen
[6] https://zoek.officielebekendmakingen.nl/stcrt-2020-30702.html

Vraag 7
In hoeverre worden Nederlandse bedrijven voorbereid op grootschalige Russische cyberaanvallen door de rijksoverheid?

Antwoord 7
De verantwoordelijkheid om beschermende maatregelen te nemen is primair de verantwoordelijkheid van de bedrijven die het betreft zelf. De overheid heeft echter ook tot taak bedrijven te informeren over digitale dreigingen, incidenten en weerbaarheid.
Om de risico's in de samenleving te beperken is er de afgelopen weken door het NCSC en het Digital Trust Center (DTC) extra aandacht gevraagd voor het belang van cyberweerbaarheid en waakzaamheid. Het NCSC voorziet daartoe in verschillende algemene producten en houdt een informatiepagina bij op de eigen website. Het DTC heeft op verschillende momenten partners en doelgroeporganisaties opgeroepen waakzaam te zijn, waarbij de nadruk wordt gelegd op het treffen van preventieve maatregelen.
Zo hebben het DTC en het NCSC op 9 maart gezamenlijk een online informatiesessie verzorgd met als titel «Huidig beeld en digitale impact van de oorlog in Oekraïne». Dit webinar was toegankelijk voor alle organisaties in Nederland en kan worden teruggekeken op het YouTube-kanaal van het DTC.[7] Deze informatiesessie is door ongeveer 4.000 bezoekers bekeken.
Ook het «Cyber Security Incident Response Team» voor digitale dienstverleners (CSIRT-DSP) verstrekt een wekelijks overzicht van (internationaal) cybersecurity nieuws gerelateerd aan de oorlog in Oekraïne aan digitale dienstverleners en monitort de situatie nauwlettend voor een actueel dreigingsbeeld voor digitale dienstverleners in Nederland.
Uit een recente sterke toename van het aantal bezoeken aan de Basisscan Cyberweerbaarheid lijkt de oproep tot verhoogde cyberweerbaarheid en waakzaamheid weerklank te vinden.[8]

Vraag 8
In hoeverre zijn kleinere bedrijven voldoende beschermd tegen cyberaanvallen vanuit Rusland? Wat is de status van de aangenomen motie Hermans c.s. (Kamerstuk 35 788, nr. 120) om ondernemers beter te beschermen tegen digitale aanvallen en dreigingen?

Antwoord 8
Ook hiervoor geldt dat de verantwoordelijkheid om beschermende maatregelen te nemen primair de verantwoordelijkheid is van de bedrijven zelf, en dat de overheid desalniettemin de taak heeft om bedrijven te informeren over digitale dreigingen, incidenten en weerbaarheid.
Naast de activiteiten uiteengezet in antwoord op vraag 7 publiceert het DTC sinds 2018 informatie over digitale dreigingen gericht op het Nederlandse bedrijfsleven. De vijf basisprincipes van veilig digitaal ondernemen zijn opgesteld om aanvallers, ongeacht de oorsprong, buiten de deur te houden. Daarnaast informeert het DTC sinds de zomer van 2021 individuele bedrijven over specifieke dreigingen en kwetsbaarheden in hun netwerk- en informatiesystemen.
De Tweede Kamer wordt voor de zomer geïnformeerd over de uitvoering van de motie Hermans c.s.[9]

---

[7] https://www.youtube.com/watch?v=bZoceLpruDQ
[8] De Basisscan Cyberweerbaarheid is een door het DTC aangeboden methode waarmee ondernemers op een laagdrempelige wijze hun digitale veiligheid kunnen doorlichten en verbeteren.
[9] Kamerstuk 35 788, nr. 120.