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**

## 974

Vragen van het lid **Rajkowski** (VVD) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat over *het bericht «Gestreste ondernemer is makkelijke prooi: trap niet in fraudeval»* (ingezonden 4 november 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) en van Minister **Adriaansens** (Economische Zaken en Klimaat) (ontvangen 8 december 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 848.

Vraag 1
Bent u bekend met het bericht «Gestreste ondernemer is makkelijke prooi: trap niet in fraudeval»[1]?

Antwoord 1
Ja.

Vraag 2
Herkent u de trend dat fraudeurs steeds geraffineerder te werk gaan waardoor ondernemers eerder slachtoffer zijn van phishing of gijzelsoftware? Zo ja, op welke manier worden ondernemers voorgelicht over deze steeds geraffineerdere manier van werken van fraudeurs?

Antwoord 2
Ja. Uit het in opdracht van het Ministerie van Economische Zaken en Klimaat uitgevoerde cybersecurity onderzoek Alert Online 2022 blijkt dat 56% van de onderzochte organisaties in de 12 maanden voor het onderzoek met phishing te maken heeft gehad. Dergelijke mails zijn een veel gebruikte methode om diverse vormen van criminaliteit te plegen, waaronder online fraude[2] en computervredebreuk. Ransomware (ook wel gijzelsoftware genoemd) betreft

[1] Telegraaf, 2 november 2022 (https://www.telegraaf.nl/financieel/1063054869/gestreste-ondernemer-is-makkelijke-prooi-trap-niet-in-fraudeval).

[2] Bij online fraude is sprake van online oplichting – bijvoorbeeld door het aannemen van een valse naam, identiteit of hoedanigheid – waarmee de fraudeur het slachtoffer digitaal beweegt tot de afgifte van goederen, diensten of andere financiële voordelen.

ah-tk-20222023-974
ISSN 0921 - 7398
's-Gravenhage 2022

een specifieke vorm van cybercrime.[3] Uit het cybersecurity onderzoek Alert Online 2022 blijkt dat ongeveer 1% van de organisaties met ransomware te maken kreeg. Kleinere organisaties blijken er vaker last van te hebben dan grotere. Van de kleine organisaties betrof het 2,4%.[4]
Het Ministerie van Economische Zaken en Klimaat (EZK) heeft het Digital Trust Center (hierna ook: DTC) opgericht met als taak het digitaal weerbaarder maken van ondernemers tegen toenemende cyberdreigingen. Het DTC deelt via de website, social media kanalen en de DTC Community de voor ondernemers relevante algemene informatie over cyberdreigingen en kwetsbaarheden. Bedrijfsspecifieke dreigingsinformatie wordt – proactief ongevraagd en in specifieke gevallen gevraagd – gedeeld met individuele bedrijven. U bent hierover geïnformeerd in de brief van 27 juni 2022 met betrekking tot de voortgang van de informatiedienst van het DTC.[5] Op deze manier kunnen bedrijven snel actie ondernemen om een cyberaanval te voorkomen of de schade te beperken.
Ook verspreidt het Digital Trust Center via de DTC Community dreigingsinformatie vanuit het Nationaal Cyber Security Centrum (hierna ook: NCSC), zijnde onderdeel van het Ministerie van Justitie en Veiligheid, en biedt het DTC via dit kanaal aangesloten bedrijven de mogelijkheid om, in een besloten omgeving, actuele en relevante informatie met elkaar uit te wisselen. Voorbeelden hiervan zijn vragen, discussies of onderzoeken over phishing en/of ransomware.
Tenslotte biedt het Digital Trust Center naast de phishing-quiz die op de website van het DTC staat, veel laagdrempelige informatie over onder andere phishing. Met een verscheidenheid aan tools en content op de website en social media kanalen van het DTC worden ondernemers geïnformeerd over het herkennen van phishing.
Het Ministerie van Justitie en Veiligheid is coördinator van de integrale aanpak online fraude en de integrale aanpak cybercrime. Voorts is in beide aanpakken aandacht voor de voorlichting van ondernemers over phishing. In het kader van de integrale aanpak online fraude loopt de verkenning naar welke wijze het bedrijfsleven het beste voorgelicht en ondersteund kan worden om slachtofferschap te voorkomen.
In de Kamerbrief naar aanleiding van de moties van de leden Ephraim en Hermans van 6 juli 2022[6] bent u geïnformeerd over de activiteiten om cybercrime in het midden- en kleinbedrijf tegen te gaan. In de Kamerbrief over de integrale aanpak van cybercrime van 4 november 2022[7] is een overzicht van activiteiten van de aanpak van cybercrime opgenomen. Het informeren van ondernemers over maatregelen die zij kunnen nemen om geen slachtoffer te worden en schade te beperken, maakt daar deel van uit. Het betreft onder meer een campagne voor het stimuleren van multifactorauthenticatie, de City Deal Lokale Weerbaarheid Cybercrime waarin gemeenten worden ondersteund door het Ministerie van Justitie en Veiligheid, om preventieve maatregelen te stimuleren, de factsheet Ransomware waarmee het NCSC en het DTC een overzicht geven van de verschillende soorten ransomware en maatregelen die organisaties kunnen nemen om een aanval te voorkomen, en het Incidentresponsplan ransomware van het NCSC met praktische handvatten om bij een ransomwareaanval adequaat te reageren.

---

[3] De term cybercrime betreft criminaliteit waarbij ICT-systemen zowel doel als middel zijn (ook wel cybercrime in enge zin genoemd). Voorbeelden daarvan zijn ransomware en het inbreken in computersystemen («hacken»). Criminaliteit waarbij ICT-middelen enkel faciliterend zijn, zoals eenvoudige online fraudevormen, wordt aangeduid met de term gedigitaliseerde criminaliteit. Overigens zijn er diverse criminele werkwijzen die elementen van cybercrime in enge zin en gedigitaliseerde criminaliteit combineren.

[4] https://www.rijksoverheid.nl/documenten/rapporten/2022/09/30/cybersecurity-onderzoek-alert-online-2022

[5] Brief van de Minister van Economische Zaken en Klimaat, 26 643, nr. 864.

[6] Kamerstuk 26 643 nr. 907.

[7] https://www.rijksoverheid.nl/Ministeries/Ministerie-van-justitie-en-veiligheid/documenten/kamerstukken/2022/11/04/tk-integrale-aanpak-cybercrime

Vraag 3
In hoeverre hebben ondernemers aangifte gedaan van phishing? Is hier sprake van een stijgende of dalende trend? Welke mogelijkheden ziet u om de aangiftebereidheid onder ondernemers te verhogen?

Antwoord 3
Aangiften van bedrijven worden vaak gedaan door een persoon en het bedrijf wordt niet altijd genoemd in de registratie. Hierdoor is het moeilijk vast te stellen hoe vaak ondernemers aangifte doen van phishing. Uit de aangiftecijfers van 2022 blijkt dat 2,5% van de aangiften van phishing is gedaan door een ondernemer. Er is sinds juni 2022 een stijgende trend te zien in het aantal aangiften van phishing door ondernemers. De reden hiervoor is onbekend. In het algemeen wordt een ieder aangespoord om aangifte te doen van een strafbaar feit. Het is mogelijk om digitaal aangifte te doen voor meerdere vormen van online criminaliteit waaronder phishing. Met deze optie wordt de drempel om aangifte te doen verlaagd.

Vraag 4
Bent u het ermee eens dat het niet altijd makkelijk is om in te schatten of je met een bonafide bedrijf of persoon zaken doet en contact hebt? Zo ja, welke rol zou de overheid hierin kunnen spelen? Zo nee, waarom niet?

Antwoord 4
Ja. Fraudeurs en cybercriminelen maken namelijk gebruik van social engineering, een techniek waarbij misbruik wordt gemaakt van de menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid.
Het Digital Trust Center, onderdeel van het Ministerie van Economische Zaken en Klimaat, publiceert adviezen, handelingsperspectieven en tools om de kennis bij ondernemers te verhogen, bijvoorbeeld door voorbeelden te geven van phishingmails. Het Ministerie van Justitie en Veiligheid en het Ministerie van Algemene Zaken verkennen welke interventies kunnen worden ingezet om veilig gedrag te bevorderen.
Meerdere partijen waarschuwen daarnaast voor verschillende vormen van online fraude en zetten gerichte campagnes daartoe in. Bijvoorbeeld door de Fraudehelpdesk, die volledig wordt gesubsidieerd door het Ministerie van Justitie en Veiligheid, tezamen met de Autoriteit Consument en Markt, de politie, het Europees Consumenten Centrum en de Consumentenbond waarschuwen het publiek rond Black Friday, Sinterklaas en Kerst voor nepwebshop en aan- en verkoopfraude met de campagne «Eerst Checken, dan bestellen».
Ook de Nederlandse Vereniging van Banken waarschuwt voor social engineering in de campagne «zo werkt een fraudeur». In deze campagne wordt de werkwijze van de fraudeurs uiteengezet, zodat men deze vormen van fraude snel kan herkennen.
Ten slotte heeft Slachtofferhulp Nederland in november een nieuwe campagne gelanceerd «online oplichting is een serieuze misdaad». Slachtoffers worden daarin opgeroepen hulp te zoeken bij Slachtofferhulp Nederland.

Vraag 5
Bent u het ermee eens dat de ondersteuning van gedupeerde ondernemers van phishing verbeterd moet worden? Zo ja, hoe gaat u dat doen? Zo nee, waarom niet?

Antwoord 5
Slachtoffer worden van phishing kan voor ondernemingen zeer ernstige gevolgen hebben. Daarom is het van groot belang dat ondernemers in eerste instantie zelf investeren in de eigen digitale veiligheid. Daarnaast is het mogelijk je te verzekeren bij een verzekeraar tegen schade als gevolg van cyberincidenten. Bij een cyberincident kan bovendien ondersteuning worden geboden door cybersecuritybedrijven. Met deze maatregelen kan een onderneming zelf de mogelijke schade voorkómen of beperken.
Er zijn verschillende instanties die ondernemers daarbij ondersteunen, zowel bij het voorkomen van schade als het oplossen daarvan. De Fraudehelpdesk, die volledig wordt gesubsidieerd door het Ministerie van Justitie en Veiligheid, kan adviseren en doorverwijzen naar instanties die specifiek verder

kunnen ondersteunen. Ook kunnen gedupeerde ondernemers aangifte doen bij de politie. Daarnaast biedt Slachtofferhulp Nederland de individuele slachtoffers van phishing ondersteuning en emotionele hulp.

Vraag 6
Bent u het ermee eens dat er ook voor de telecomsector een rol weggelegd is om frauduleuze telefoontjes en misbruik van nummers tegen te gaan? Zo ja, bent u bereid hierover met de sector in gesprek te gaan en te kijken waar aanvullende maatregelen mogelijk zijn en de Kamer hierover te informeren?

Antwoord 6
Ja. Hierover is de Minister van Economische Zaken en Klimaat, samen met de Autoriteit Consument en Markt, reeds in overleg met de sector. Dit overleg vindt plaats mede in het kader van een wetsvoorstel voor aanscherping van het spoofingverbod, een beperking van het gebruik van Nederlandse nummers vanuit het buitenland en flankerende maatregelen. Bij de aanpak door de telecomsector wordt aangesloten bij de integrale aanpak van online fraude. Hierover is uw Kamer geïnformeerd met de brief van 8 juli 2022.[8]

Vraag 7
Herkent u het beeld dat de vele campagnes en trainingen onvoldoende effect lijken te hebben en dat het essentieel is om van jongs af aan bewust te zijn van gevaren van de online wereld en bent u bereid om online oplichting een prominente plek te geven in de pilot cyberrijbewijs voor basisscholen? Zo nee, waarom niet? Zo ja, kunt u de Kamer hierover informeren?

Antwoord 7
Het effect van de combinatie van bewustwordingsmaatregelen is lastig te meten. Wel blijkt uit onder meer het Cybersecurity onderzoek Alert Online 2022 dat bewustwording nog nadere aandacht behoeft. Zo komt uit dit onderzoek naar voren dat een derde van de medewerkers van bedrijven hun kennis over online veiligheid als (zeer) slecht tot matig inschat.
Het project Mijn cyberrijbewijs is in samenwerking met FutureNL en het Ministerie van Justitie en Veiligheid ontwikkeld. Dit project maakt deel uit van de inspanningen om bewustwording te vergroten bij de jeugd. Begin oktober is de interventie Mijn Cyberrijbewijs gelanceerd: een gratis lesprogramma voor groep 7 en 8 van het primair onderwijs. Online oplichting krijgt hierin als fenomeen, een prominente plek. Naast kennis over schadelijke fenomenen geeft de verkenning «Online Ontspoord»[9] van het Rathenau Instituut aanknopingspunten om digitale weerbaarheid onder van doelgroep verder te ontwikkelen. In dit onderzoek zijn 18 mechanisme in kaart gebracht die ervoor zorgen dat online gedrag sneller ontspoort dan in het fysieke domein. Mijn Cyberrijbewijs maakt jonge mensen bewust van deze mechanismes en de online risico's.
Het ECP Platform voor de Informatiesamenleving vormt daarnaast samen met het expertisecentrum voor Online Kindermisbruik en het Netwerk Mediawijsheid Safer Internet Center voor kinderen een nationale invulling van de Europese strategie voor een beter internet voor kinderen. In het netwerk kijken overheid, bedrijfsleven en maatschappelijke organisaties hoe kinderen en jongeren op een veilige manier de digitale wereld kunnen betreden, bijvoorbeeld met lespakketten voor scholen of speciale uitgaven van de Donald Duck, de zogenaamde Digiducks.

Vraag 8
Welke belemmeringen ervaart de Fraudehelpdesk om ondernemers en burgers zo goed mogelijk te kunnen informeren over malafide personen, websites en bedrijven? Bent u bereid deze weg te nemen? Zo nee, waarom niet?

---

[8] Brief van de Ministers van Justitie en Veiligheid, van Financiën, van Economische Zaken en Klimaat en voor Rechtsbescherming, Kamerstuk 29 911, nr. 372.

[9] Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen).

Antwoord 8
Bij de Fraudehelpdesk, die volledig wordt gesubsidieerd door het Ministerie van Justitie en Veiligheid, kunnen slachtoffers melding maken van fraude en oplichting. De Fraudehelpdesk biedt voorlichting en verwijst slachtoffers zo nodig door voor hulp en het doen van aangifte. De Fraudehelpdesk wil voor een goed onderbouwd advies aan melders gegevens kunnen verwerken, zoals telefoonnummers, sms en mogelijk malafide links. De Fraudehelpdesk heeft hiervoor een vergunning aangevraagd, maar de Autoriteit Persoonsgegevens (AP) heeft de aanvraag afgewezen. De Fraudehelpdesk heeft hiertegen beroep ingesteld. Dit is nog onder de rechter.
Het is belangrijk dat relevante gegevens gedeeld kunnen worden, bijvoorbeeld over modus operandi. Zoals aangegeven in de brief van 8 juli jl. verkent het Ministerie van Justitie en Veiligheid o.a. met meldpunten, waaronder de Fraudehelpdesk, hoe we dit binnen de kaders van de AVG vorm kunnen geven.

Vraag 9
Bent u het ermee eens dat landen als België een zeer interessante aanpak hebben in het voorkomen van phishing door informatie over malafide websites snel binnen te halen en te verspreiden en daarmee slachtoffers te voorkomen? Zo nee, waarom niet? Zo ja, kunt u de Kamer informeren hoe u lessen gaat trekken van andere landen en daarmee Nederlanders een stukje veiliger houdt?

Antwoord 9
Ja. Zoals gemeld in de bijlage bij de Kamerbrief over de integrale aanpak van cybercrime van 4 november jl. verkent het Ministerie van Justitie en Veiligheid, tezamen met het NCSC of een «anti-phishing-schild» naar Belgisch voorbeeld ook in Nederland kan worden opgezet. Daarmee zou het mogelijk worden criminele links in berichten te melden om deze vervolgens onschadelijk te maken, dan wel van een waarschuwing te voorzien. Dit zou het slachtofferschap van phishing en daaropvolgende delicten kunnen tegengaan.