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

3031

Vragen van lid **Dekker-Abdulaziz** (D66) aan de Minister van Justitie en Veiligheid over *het bericht ongeveer 2,2 miljoen mensen vorig jaar getroffen door cybercriminaliteit* (ingezonden 12 mei 2023).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 28 juni 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 2780.

Vraag 1
Bent u bekend met bovenstaand bericht?[1]

Antwoord 1
Ja.

Vraag 2
Wat is uw reactie op de schatting van het Centraal Bureau voor de Statistiek dat 2,2 miljoen mensen vorig jaar zijn getroffen door cybercriminaliteit?

Antwoord 2
Het getal is zorgelijk. De hoge slachtofferaantallen in het rapport onderschrijven dat onze inzet om online criminaliteit tegen te gaan onverminderd nodig is. De aanpak van diverse vormen van online criminaliteit, zoals cybercrime en online fraude, heeft al langer mijn aandacht. Daar bent u eerder over geïnformeerd in onder meer de Kamerbrief over de integrale aanpak cybercrime,[2] de Kamerbrief over de integrale aanpak online fraude[3] en de Kamerbrief over de preventie cybercrime voor het midden- en kleinbedrijf.[4]

Vraag 3
Gestolen inloggegevens zijn onderdeel van de ondergrondse online economie en zijn een bron van vele soorten online criminaliteit, dit komt ook voor bij overheidsorganisaties. Welke maatregelen neemt u om datalekken binnen de overheid te voorkomen?

---

[1] NOS, 11 mei 2023, Ongeveer 2,2, miljoen mensen vorig jaar getroffen door cybercriminaliteit (nos.nl/artikel/2474634-ongeveer-2–2-miljoen-mensen-vorig-jaar-getroffen-door-cybercriminaliteit).
[2] Kamerstuk 26 643, nr. 930.
[3] Kamerstuk 29 911, nr. 372.
[4] Kamerstuk 26 643, nr. 907.

ah-tk-20222023-3031
ISSN 0921 - 7398
's-Gravenhage 2023

Antwoord 3
Uit de Algemene Verordening Gegevensbescherming (AVG) volgt dat de verwerking van persoonsgegevens aan bepaalde eisen dient te voldoen. Zo schrijft de AVG voor dat persoonsgegevens deugdelijk dienen te worden beveiligd.[5] Overheidsorganisaties nemen mede om die reden verschillende beschermingsmaatregelen om datalekken[6] of andere incidenten te voorkomen. De Baseline Informatiebeveiliging Overheid, het basisnormenkader voor informatiebeveiliging bij de overheid, bevat bijvoorbeeld een minimale set aan maatregelen voor overheidsorganisaties om beter beschermd te zijn tegen digitale dreigingen. Het doel hiervan is om zoveel mogelijk te voorkomen dat overheidsorganisaties slachtoffer worden van digitale aanvallen.
De overheid neemt verschillende maatregen om voorbereid te zijn indien, ondanks de genomen maatregelen, toch incidenten plaatsvinden. Een voorbeeld hiervan is de jaarlijkse Overheidsbrede Cyberoefening waar verschillende overheidsorganisaties oefenen met gesimuleerde hackaanvallen. Op deze manier worden bestaande crisisplannen getest in de praktijk en leren organisaties hoe ze moeten handelen tijdens incidenten. Aan de meest recente oefening van oktober 2022 hebben meer dan 70 overheidsinstanties deelgenomen. Daarnaast hebben ruim 450 mensen de livestream van de centrale crisisoefening gevolgd. Deze Overheidsbrede Cyberoefening is aanvullend op wat de verschillende bestuurslagen zelf al organiseren, zoals de oefenpakketten van de Informatiebeveiligingsdienst van de Vereniging Nederlandse Gemeenten [7].
De Netwerk- en informatiebeveiligingsrichtlijn (NIS2) geeft handvatten om maatregelen van de Baseline Informatiebeveiliging Overheid wettelijk te verankeren en het toezicht op de overheid in te richten. Deze richtlijn wordt momenteel omgezet in nationale wetgeving. Het toezicht op informatieveiligheid bij de gehele overheid zorgt dat de maatregelen zoals benoemd in de Baseline Informatiebeveiliging Overheid op een goede manier worden toegepast.

Vraag 4
Ransomsware komt steeds vaker voor bij grote bedrijven en het mkb. U adviseert dringend om geen losgeld te betalen. Wat zijn volgens u adequate stappen die een bedrijf kan zetten als er cruciale data zijn gestolen en worden aangeboden voor losgeld?

Antwoord 4
Als organisaties als gevolg van een ransomware-aanval te maken krijgen met een datalek, is het belangrijk dat er direct actie wordt ondernomen, zoals het melden van het datalek bij de Autoriteit Persoonsgegevens en het informeren van de slachtoffers. Door het informeren van de slachtoffers kunnen zij (tijdig) maatregelen treffen om verdere schade te beperken. De Autoriteit geeft op haar website advies over de maatregelen die moeten worden genomen bij een datalek.[8] Bij een complex datalek, zoals vaak het geval is bij een ransomware-aanval, adviseert de Autoriteit om een expert in te schakelen, bijvoorbeeld een forensisch expert.
Het Digital Trust Center (van het Ministerie van Economische Zaken en Klimaat biedt op haar website handelingsperspectieven voor ondernemers bij een ransomware-aanval.[9] Naast de handelingsperspectieven van het Digital Trust Center, geeft het incidentresponseplan van het Nationaal Cyber Security Centrum praktische handvatten voor de voorbereiding op en ondersteuning

---

[5] Artikel 32 Avg.
[6] Volgens de Autoriteit Persoonsgegevens is er sprake van een datalek bij toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie.
[7] https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/.
[8] https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen.
[9] https://www.digitaltrustcenter.nl/informatie-advies/ransomware/wat-te-doen-bij-een-ransomware-aanval.

bij een ransomware-aanval voor organisaties. Het plan gaat onder meer in op de situatie waarin data zijn gestolen[10] en voor losgeld worden aangeboden. Slachtoffers van ransomware worden uitdrukkelijk opgeroepen aangifte of melding te doen bij de politie. Het dringende advies blijft om geen losgeld te betalen. Het betalen van losgeld biedt geen garantie dat data niet verder zullen worden verhandeld en/of criminelen de systemen weer toegankelijk maken. Bovendien wordt door het betalen van losgeld het criminele verdienmodel in stand gehouden.
Op de website NoMoreRansom.org, mede beheerd door de politie, worden slachtoffers van ransomware geholpen om versleutelde data te herstellen zonder dat het slachtoffer losgeld betaalt. Ook kan de politie in bepaalde gevallen andere (potentiële) slachtoffers van ransomware tijdig waarschuwen om beschermingsmaatregelen te treffen.

Vraag 5
Hoe kijkt u in dat kader naar het recente voorbeeld van de woningcorporatie uit Zwijndrecht die een aanzienlijk bedrag aan losgeld zou hebben betaald?[11]

Antwoord 5
Slachtoffer worden van een ransomware-aanval kan veel impact hebben. De schade kan enorm oplopen. Ik begrijp dat dit slachtoffers in een moeilijke positie plaatst, zeker als cruciale gegevens zijn gestolen. Het advies blijft echter om geen losgeld te betalen. Misdaad mag niet lonen. Het betalen van losgeld houdt het criminele verdienmodel in stand en kan meer criminaliteit stimuleren. Door het betalen van losgeld wordt het signaal aan cybercriminelen afgegeven dat ransomware effectief en lucratief is. Cybercriminelen raken hierdoor gemotiveerd om hun criminele activiteiten verder te ontplooien. Bovendien biedt het betalen van losgeld geen garantie dat de gestolen gegevens worden hersteld of niet verder worden verhandeld.

Vraag 6
Hoe kijkt u naar de oprichting van een gemeenschappelijk fonds voor mkb, waaruit losgeld zou kunnen worden betaald als hier goede reden toe is? Zo kan ook gezamenlijk worden geïnvesteerd in preventie en signalering.

Antwoord 6
Om criminaliteit tegen te gaan en weerbaarder te zijn tegen aanvallen is het onder meer van belang de eigen beveiliging op orde te hebben. Organisaties zijn verantwoordelijk voor hun eigen digitale beveiliging en moeten hiervoor de juiste preventieve maatregelen treffen. Organisaties kunnen hierin worden ondersteund door commerciële cybersecuritydiensten. Vanuit de overheid wordt op meerdere manieren voorlichting gegeven en worden hulpmiddelen ter beschikking gesteld via het Nationaal Cyber Security Centrum en het Digital Trust Centre. Ook waarschuwen het Nationaal Cyber Security Centrum en het Digital Trust Centre in meer algemene zin voor kwetsbaarheden en dreigingen.
Het betalen van losgeld houdt het criminele verdienmodel in stand en kan meer criminaliteit stimuleren. Zie ook het antwoord op vraag 5. De markt voorziet overigens reeds in cyberverzekeringen voor geleden schade na een ransomware-aanval. Een fonds om losgeld te betalen lijkt niet de juiste weg voorwaarts.

Vraag 7
Heeft u in beeld hoeveel procent van de ransomware-aanvallen resulteert in een aangifte?

---

[10] In juridische zin is hier geen sprake van diefstal in de zin van het Wetboek van Strafrecht (Sr). Met het woord «gestolen» in deze context wordt bedoeld het opzettelijk en wederrechtelijk overnemen van niet-openbare gegevens in de zin van artikel 138c Sr.

[11] RTL Nieuws, 9 mei 2023, Woningcorporatie betaalt losgeld na ransomware-aanval: «Gaat om tonnen» (www.rtlnieuws.nl/nieuws/nederland/artikel/5383064/woonkracht10-ransomware-losgeld-play-cybercriminelen).

Antwoord 7
Over de hoeveelheid ransomware-aanvallen in Nederland en de schade die deze aanvallen veroorzaken zijn weinig kwantitatieve gegevens beschikbaar. Het beeld, mede op basis van het Cybersecuritybeeld Nederland van 2022 en mediaberichtgeving, is dat het aantal aanvallen toeneemt en dat de hoogte van het geëiste losgeld toeneemt. De politie geeft aan dat zij jaarlijks rond de 200 aangiftes van ransomware ontvangt. De aangiftebereidheid bij cybercrimedelicten is echter laag, wat ook geldt voor ransomware. Het aantal aangiften is daarom naar verwachting geen goede weerspiegeling van de omvang van de problematiek.

Vraag 8
Welke stappen neemt u om de aangiftebereidheid onder getroffen bedrijven/personen te verhogen?

Antwoord 8
De politie heeft het voor diverse cybercriminele fenomenen mogelijk gemaakt om online aangifte doen, waardoor aangifte doen eenvoudiger is geworden en minder tijd kost. Zoals afgesproken in de Veiligheidsagenda 2023–2026 maakt de politie vanaf 2023 voor meer fenomenen digitale aangifte mogelijk. Heden wordt er gewerkt om online aangifte voor ransomware in het derde kwartaal van 2023 mogelijk te maken.
Het Digital Trust Centre en het Nationaal Cyber Security Centrum adviseren bedrijven altijd om aangifte te doen indien zij slachtoffer van een digitaal misdrijf zijn geworden. Daarnaast heeft het Nationaal Cyber Security Centrum samen met de politie, het Openbaar Ministerie en Cyberveilig Nederland in januari 2023 een *whitepaper* over data-exfiltratie bij een ransomware-aanval uitgebracht. Ook hierin adviseert het Nationaal Cyber Security Centrum om naast het melden van de ransomware-aanval bij het Centrum aangifte bij de politie te doen.[12]

Vraag 9
Hoe reflecteert u op het gegeven uit het rapport «The State of Data Security» waaruit blijkt dat van de deelnemende bedrijven in Nederland slechts 9 procent in staat is om alle data te herstellen na betaling van cybercriminelen? Ondanks deze zorgelijke cijfers betaalt driekwart van de bedrijven losgeld bij een ransomware-aanval.[13]

Antwoord 9
Het rapport bevestigt dat de grootste winst valt te behalen door te investeren in risicomanagement en preventieve maatregelen. Er is geen enkele garantie dat de sleutel (decryptor) of het wachtwoord wordt overhandigd nadat het gevraagde losgeld is betaald. Hierdoor blijft het risico bestaan dat de nieuwe of herstelde bestanden versleuteld worden en de afpersing nogmaals plaats zal vinden. Bovendien kan de gestolen data later alsnog door de cybercriminelen worden verhandeld. Het veilig herstellen van de data is in veel gevallen onmogelijk of bijna onmogelijk. Het Nationaal Cyber Security Centrum biedt in het incidentresponseplan diverse handvatten voor organisaties om preventieve maatregelen te treffen.

Vraag 10
Wat vindt u van het gegeven uit hetzelfde rapport dat slechts 58 procent van de deelnemende organisaties een crisisplan voor cyberaanvallen opstelt? Ziet u een rol voor uzelf om dit percentage te verhogen. Zo ja, welke rol?

Antwoord 10
Ik deel de zorg dat nog te weinig organisaties crisisplannen hebben voor cyberincidenten. Dit kabinet stimuleert het schrijven van deze plannen door via verschillende wegen organisaties te adviseren crisisprocessen in te

---

[12] https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf.
[13] Techzine, 18 april 2023, Organisaties verliezen bijna altijd data bij ransomware-aanval (www.techzine.nl/nieuws/security/521910/organisaties-verliezen-bijna-altijd-data-bij-ransomware-aanval/).

richten en vast te leggen, en door oefeningen zoals ISIDOOR te organiseren en een goede voorbereiding bij de deelnemers te benadrukken.
Onder de NIS2 wordt het voor organisaties die onder de richtlijn vallen verplicht om maatregelen te hebben voor bedrijfscontinuïteit en crisisbeheersing. Het is de verwachting dat daardoor meer organisaties voorbereidingen voor cyberincidenten treffen en vastleggen.
Voor zelfstandigen zonder personeel, kleine organisaties en midden- en kleinbedrijven biedt het Digital Trust Centre op haar website een leidraad om een incidentresponseplan op te stellen. Daarnaast voorziet de Cyberveilig Check van het Digital Trust Centre in meerdere maatregelen die zowel preventief werken als de schade van een cyberincident beperken.

Vraag 11
Hoeveel financiële middelen worden er in totaal de komende jaren per jaar uitgetrokken om het bedrijfsleven beter te faciliteren om beschermd te zijn tegen ransomware-aanvallen?

Antwoord 11
Het budget voor de uitvoering van de Nederlandse Cybersecurity Strategie betreft een bedrag oplopend tot 111 miljoen euro per jaar structureel. Dit bedrag komt ten goede aan de cybersecurity van Nederland, wat de weerbaarheid tegen onder meer ransomware-aanvallen versterkt. De middelen zijn onderverdeeld bij de departementen en uitvoeringsorganisaties, met een eigen verantwoordelijkheid voor de toekenning van voldoende capaciteit en financiële middelen om de in de Nederlandse Cybersecuritystrategie en het actieplan vastgelegde beleidsdoelen en acties te realiseren. Daarnaast ondersteunen het Nationaal Cyber Security Centrum, het Digital Trust Centre, het Openbaar Ministerie, de politie en andere partners binnen en buiten de (Rijks)overheid doorlopend op verschillende manieren het bedrijfsleven en andere organisaties in het verhogen van de cyberweerbaarheid tegen onder andere ransomware.

Vraag 12
MiND (meldpunt internet discriminatie) kan een belangrijke rol spelen in het tegengaan van hate-speech en discriminatie online, maar uit de cijfers (339 meldingen vorig jaar) blijkt dat het meldpunt onvoldoende wordt gevonden. Welke stappen onderneemt u om het meldpunt beter onder de aandacht te brengen, en kunt u specifiek ingaan op hoe u de doelgroep jongeren hier attent op wilt maken?

Antwoord 12
Ik vind het van groot belang dat het Meldpunt Internetdiscriminatie goed gevonden wordt. Op dit moment is dat onvoldoende het geval. Mijn ministerie verstrekt jaarlijks subsidie aan Meldpunt. Met het Meldpunt is afgesproken dat zij zich de komende tijd sterk inzetten om een betere naamsbekendheid te genereren. Als resultaat van een herpositionering zal het meldpunt deze zomer een nieuwe merknaam introduceren met bijbehorende communicatie(uitingen). Door middel van (online) campagnes worden doelgroepen, waaronder jongeren, bereikt om hen te informeren over het meldpunt en de oproep tot het melden van online discriminatie.