Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

1383

Vragen van het lid **Van Raak** (SP) aan de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie en Veiligheid over *het bericht dat er losgeld is gevraagd om gehackte gemeentedata terug te krijgen* (ingezonden 9 december 2020).

Antwoord van Staatssecretaris **Knops** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Minister van Justitie en Veiligheid (ontvangen 20 januari 2021).

Vraag 1
Bent u het eens met de weigering van de burgemeester om losgeld te betalen om gehackte gemeentedata weer terug te krijgen? Zo nee, waarom niet?[1]

Antwoord 1
Ja. Het betalen van losgeld is zeer onwenselijk, omdat dit het crimineel verdienmodel ondersteunt. De politie ziet bovendien dat losgeld door criminelen direct wordt geïnvesteerd in nieuwe ransomware-aanvallen. Het advies is daarom om altijd aangifte te doen bij de politie en geen losgeld te betalen.

Vraag 2
Is dit vaker voorgekomen bij publieke instellingen? In hoeveel gevallen is er eventueel losgeld betaald? Kunt u hier een overzicht van geven?

Antwoord 2
De politie registreert niet apart of er sprake is van een publieke instelling. Daarom is het, zoals is aangegeven bij de beantwoording op schriftelijke Kamervragen over de ransomware-aanval op de Universiteit Maastricht, bij meldingen en aangiften op korte termijn niet te zeggen of er sprake is van een publieke instelling.[2] Uit een analyse van de politie blijkt dat in de jaren 2018, 2019 en 2020 (tot half december) er respectievelijk 180, 188 en 186 meldingen en aangiften van ransomware-aanvallen bij de politie zijn gedaan. In zijn algemeenheid is bekend dat bij cybercrimedelicten de aangifte- of

[1] Tubantia, 7 december 2020 (https://www.tubantia.nl/tech/toch-losgeld-geeist-na-cyberaanval-op-gemeente-hof-van-twente-hackers-eisen-750-duizend-euro~a1f61c76/)
[2] Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 2184.

ah-tk-20202021-1383
ISSN 0921 - 7398
's-Gravenhage 2021

meldingsbereidheid laag is. Dit geldt ook voor aangiften van ransomware. Er is geen volledig beeld van gevallen waarbij er door publieke instellingen losgeld is betaald.

Vraag 3
Hoe wordt voorkomen dat andere gemeenten slachtoffer worden van dit soort afpersing? Worden door u extra maatregelen getroffen naar aanleiding van deze zaak?

Antwoord 3
Gemeenten werken aan constante verbetering van de digitale weerbaarheid, waarbij de Informatiebeveiligingsdienst (IBD) alle gemeenten ondersteunt als Computer Emergency Response Team (CERT). Daarmee wordt de kans op een succesvolle aanval verminderd.
De IBD heeft de rol van CERT in het kader van de Wet Beveiliging Netwerk- en Informatiesystemen (Wet BNI) en vormt de verbindende schakel tussen het Nationaal Cybersecurity Centrum (NCSC) en gemeenten. Vanuit deze rol ondersteunt de IBD de gemeente Hof van Twente en informeert waar nodig andere gemeenten.
Verder biedt de door de Vereniging van Nederlandse Gemeenten (VNG) opgestelde gemeentelijke Agenda Digitale Veiligheid 2020–2024[3] handelingsperspectief aan alle gemeenten. De hoofdonderwerpen van deze agenda zijn: bewustwording, governance, risicogericht handelen en werken als één overheid. De Agenda biedt ook handvatten bij het voorkomen en oplossen van cyberincidenten.
Gemeenten gebruiken voor hun informatiebeveiliging de Baseline Informatiebeveiliging Overheid (BIO), welke geldt als basisnormenkader voor informatiebeveiliging bij de gehele overheid. Het Ministerie van BZK voert onderhoud op de BIO[4] in samenspraak met de bestuurslagen Rijk, provincies, gemeenten en waterschappen.
Om alle overheden ook te laten oefenen met cybersecurity-incidenten, organiseert het Ministerie van BZK sinds 2019 een Overheidsbrede Cyberoefening[5] welke jaarlijks plaatsvindt, met in het programma een prominente plek voor een gesimuleerde hackaanval. Het Rijk, provincies, gemeenten en waterschappen oefenen aan de hand van een zo realistisch mogelijk scenario. Tijdens de Overheidsbrede Cyberoefening van 2021 zal het thema ransomware prominent op de agenda staan en worden de geleerde lessen overheidsbreed gedeeld. Dit naar aanleiding van de gebeurtenis bij de gemeente Hof van Twente.
Verder is met subsidie vanuit het Ministerie van BZK begin 2020 een drietal gemeentelijke cyberoefenpakketten[6] ontwikkeld en gratis beschikbaar gesteld aan alle gemeenten. De cyberoefenpakketten zijn tot stand gekomen in nauwe samenwerking met het Instituut voor Veiligheids- en Crisismanagement (het COT). De cyberoefenpakketten bieden alle gemeenten op diverse niveaus van de organisatie handelingsperspectief ten aanzien van crisismanagement.
De bovengenoemde activiteiten leveren een bijdrage aan een verhoogde digitale weerbaarheid bij de overheid. Zodoende worden er geen extra maatregelen getroffen naar aanleiding van de gebeurtenis bij de gemeente Hof van Twente, met uitzondering van het delen van de geleerde lessen tijdens de Overheidsbrede Cyberoefening 2021. Cybersecurity-incidenten zijn lastig te voorspellen en te voorkomen. Het permanent oefenen is van groot belang voor het overheidsbrede samenspel met relevante private partijen. Op die manier kan er al aan de voorkant beter op elkaar worden ingespeeld.

---

[3] De Agenda Digitale Veiligheid van de VNG is te vinden op https://vng.nl/publicaties/agenda-digitale-veiligheid-2020–2024

[4] De BIO is gepubliceerd in de Staatscourant, te vinden op https://zoek.officielebekendmakingen.nl/stcrt-2020–7857.html

[5] Nadere informatie over de Overheidsbrede Cyberoefening is te vinden op www.weerbaredigitaleoverheid.nl

[6] De drie cyberoefenpakketten zijn te vinden op de website van de IBD: https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/

Vraag 4
Hoeveel afpersers van soortgelijke gevallen (publiek of privaat) zijn er in de afgelopen tien jaar veroordeeld? Hoe gaat u de pakkans van deze criminelen vergroten?

Antwoord 4
Ransomware is geen apart delict en wordt niet als zodanig geregistreerd door het OM en de Rechtspraak. De tenlastelegging van ransomware bestaat uit een combinatie van verschillende strafbare feiten, zoals computervredebreuk en afpersing. Per zaak kan de samenstelling van deze strafbare feiten verschillen. Het is daarom niet bekend hoeveel veroordelingen voor ransomware hebben plaatsgevonden. Wel blijkt dat er sinds 2015 in Nederland enkele zaken zijn geweest met een veroordeling voor een combinatie van afpersing (317 Sr) met computervredebreuk (138ab Sr), het gebruik van een technisch hulpmiddel (139d Sr) of opzettelijke computersabotage (350a Sr), dan wel poging daartoe. Het gaat hierbij om veroordelingen in eerste aanleg. De wetsartikelen 138a, 139d en 350a zijn in 2015 in hun huidige vorm in werking getreden.
De opsporing in het digitale domein kent verschillende uitdagingen. De grenzeloosheid van het internet zorgt dat daders vaak zelf niet in het land aanwezig zijn waar zij slachtoffers maken, of dat het land van waaruit de dader zijn activiteiten uitvoert zeer lastig te achterhalen is. Ransomware wordt gepleegd door verschillende typen daders. Zware cybercriminele organisaties richten ransomware-aanvallen op grote bedrijven en organisaties. Daarnaast zijn er individuele daders die ransomware-as-a-service van criminele dienstverleners afnemen en meer ongericht middelgrote tot kleine organisaties aanvallen. Al deze dadercategorieën kennen een sterke internationale component.
De investeringen in de politie en de strafrechtketen uit het Regeerakkoord hebben een versterking van de capaciteit voor de aanpak van cybercrime mogelijk gemaakt. Zo beschikt elke regionale eenheid inmiddels over een cybercrimeteam. Daarnaast bestrijdt het Team High Tech Crime (THTC) ransomware in het segment van zware, georganiseerde cybercrime met een internationale component. In het kader van de EU en de Raad van Europa wordt gewerkt aan het verbeteren van de internationale mogelijkheden voor de opsporing. Tot slot is het van belang preventieve maatregelen te nemen, zoals het verhogen van de digitale weerbaarheid. Hierbij is het van belang dat organisaties basismaatregelen nemen, zoals het patchen van systemen.