Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

2184

Vragen van het lid **Verhoeven** (D66) aan de Minister van Justitie en Veiligheid over *de berichten «Universiteit Maastricht betaalde hackers losgeld» en «Verzekeraars zorgen voor toename van ransomware-aanvallen»* (ingezonden 23 januari 2020).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 23 maart 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 1721.

Vraag 1
Bent u bekend met de berichten ««Universiteit Maastricht betaalde hackers losgeld» en «Verzekeraars zorgen voor toename van ransomware-aanvallen»?[1] [2]

Antwoord 1
Ja.

Vraag 2
Hoeveel gevallen van (semi-)publieke instellingen, waaronder universiteiten en ziekenhuizen, die zijn getroffen door ransomware zijn er bij u bekend?

Antwoord 2
In 2019 zijn 188 meldingen en aangiftes gedaan van ransomware bij de politie. Het is niet mogelijk op korte termijn na te gaan hoeveel van deze meldingen/aangiftes afkomstig zijn van (semi-)publieke instellingen.

Vraag 3 en 4
In hoeveel gevallen is er gekozen voor de oplossing om ransomware te betalen in plaats van het terugzetten van back-ups? Kunt u de complexiteit van de afwegingen daarbij schetsen?
In hoeverre is het mogelijk om voor dergelijke beslissingen over het al dan niet betalen van losgeld eenduidig beleid te ontwikkelen? Ziet u additionele mogelijkheden voor beleid op het gebied van back-upbeleid?

[1] NRC, 2 januari 2020, «Universiteit Maastricht betaalde hackers losgeld» (https://www.nrc.nl/nieuws/2020/01/02/universiteit-maastricht-betaalde-hackers-losgeld-a3985528)
[2] Security.nl, 28 augustus 2019, https://www.security.nl/posting/622296#posting622383 Powered by TCPDF (www.tcpdf.org)

ah-tk-20192020-2184
ISSN 0921 - 7398
's-Gravenhage 2020

Antwoord 3 en 4
Ik heb geen informatie over het aantal gevallen waarin is gekozen ransomeware te betalen, danwel over de verschillende afwegingen die een rol spelen bij het overgaan tot betaling. Ik hecht eraan te benadrukken dat toegeven aan ransomware altijd onwenselijk is en dat het van belang is om altijd aangifte te doen. Door te betalen worden criminele activiteiten beloond en gestimuleerd. Daarnaast is de verwachting dat het betalen van losgeld leidt tot meer aanvallen van ransomware. Er wordt dan ook geen aanvullend beleid ontwikkeld met betrekking tot besluitvorming over het al dan niet betalen van losgeld.
Er bestaan geen algemene verplichtingen rond het maken van back-ups. Organisaties zijn zelf verantwoordelijk voor de cybersecurity binnen hun organisatie. Het is voor publieke en private organisaties van belang dat cybersecurity voldoende aandacht krijgt in de bedrijfsvoering. Via preventiecampagnes, advies en handelingsperspectieven wordt geprobeerd om burgers en bedrijven te informeren over veiligheid en internet, bijvoorbeeld via veiliginternetten.nl en het Digital Trust Center.[3] Het maken van back-ups wordt daarentegen wel actief onder de aandacht gebracht tijdens preventiecampagnes. Dit is een van de basisbeginselen om de schade van cybercrime te beperken.
Daarnaast adviseert het Nationaal Cyber Security Centrum (NCSC), de rijksoverheid en vitale aanbieders over cyberdreigingen en -incidenten. Het NCSC geeft ook voor het brede publiek toegankelijke adviezen op de website, waaronder ransomware. Onderdeel daarvan is het advies om regelmatig back-ups te maken.[4]

Vraag 5 en 6
Bent u het eens met de stelling dat het feit dat verzekeraars losgeld dat betaald wordt voor ransomware in sommige gevallen vergoeden, zorgt voor een toename in ransomware-aanvallen?
Zo ja, bent u van plan om stappen te nemen tegen, of eisen te stellen aan, het verzekeren van losgeld voor ransomware?

Antwoord 5 en 6
In beginsel is te verwachten dat het betalen van losgeld leidt tot meer aanvallen van ransomware. De politie verwacht dat losgeld dat betaald wordt door slachtoffers deels direct wordt ingezet om nieuwe aanvallen te bekostigen. Het vergoeden van losgeld door verzekeraars kan dit effect verder faciliteren.
Inzake het effect van de rol van verzekeraars op ransomware moet ook in acht worden genomen dat door middel van het stellen van cybersecurity eisen door verzekeraars het risico op ransomware kan afnemen. Bijvoorbeeld doordat verzekeraars eisen dat afnemers van een verzekering hun software up to date houden en dat back-ups worden gemaakt. Uiteraard heeft het daarbij de voorkeur dat de verzekeraar de geleden schade door het niet betalen van losgeld vergoedt, en niet het losgeld dat in handen van criminelen terecht komt.
Ik zal de onwenselijkheid om te betalen bij ransomware en de consequenties van betaling bij het Verbond van Verzekeraars onder de aandacht brengen.

Vraag 7
Welke andere stappen bent u van plan te nemen tegen ransomware-aanvallen?

Antwoord 7
De integrale aanpak cybercrime[5] benoemt maatregelen die tegen diverse vormen van cybercrime, waaronder ransomware, worden genomen. Zo wordt er onder andere ingezet op preventie, bijvoorbeeld via publiekscampagnes (zie antwoord vraag[6]. Daarnaast doen de politie en het Openbaar Ministerie onderzoek om daders aan te pakken en criminele werkwijzen tegen te gaan.

---

[3] https://digitaltrustcenter.nl/back-up
[4] https://www.ncsc.nl/actueel/nieuws/2019/september/5/ransomware-wat-kunt-u-doen
[5] Kamerstuk 28 684 nr. 564 en 28 684, nr. 522
[6] Security.nl, 28 augustus 2019, https://www.security.nl/posting/622296#posting622383

Het Regeerakkoord heeft een forse investering in de politie mogelijk gemaakt. Deze komt deels ten goede aan de opsporing van cybercrime en gedigitaliseerde criminaliteit.
Voor slachtoffers van ransomware heeft de politie samen met partners de site nomoreransom.org ontwikkeld. Deze site is een internationaal samenwerkingsverband tussen opsporingsdiensten en private partners. Hier worden, indien beschikbaar, ontsleutelcodes gratis ter beschikking gesteld. Ook wordt op de genoemde website voorlichting gegeven over het voorkomen van ransomware.
Tot slot kunnen burgers en organisaties zelf diverse maatregelen nemen om slachtofferschap van cybercrime te voorkómen of de schade te beperken. Via veilige hard- en software kan het risico worden beperkt dat ransomware zich verspreidt via kwetsbaarheden in software.[7] Daarnaast kan door het regelmatig maken van back-ups, het updaten van software en oplettendheid bij het ontvangen van berichten met hyperlinks van onbekende afzenders het risico om te maken te krijgen met ransomware beperkt worden. De regering ondersteunt activiteiten voor bewustwording over dergelijke mogelijkheden via bijvoorbeeld de campagnes «eerst checken, dan klikken» en «doe je updates».

[7] Voor initiatieven vanuit het kabinet inzake digitale veiligheid in het algemeen verwijs ik naar de Roadmap Veilige Hard en Software: Kamerstuk 26 643, nr. 535