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

225

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht dat het Ministerie van Justitie en Veiligheid de mogelijkheden onderzoekt om verzekeraars te verbieden om losgeld te vergoeden bij slachtoffers van een ransomware-aanval* (ingezonden 21 september 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 7 oktober 2021).

Vraag 1
Bent u bekend met het artikel «Overheid in actie tegen betalen van losgeld aan ransomware-criminelen»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat op dit moment de mogelijkheden worden onderzocht om verzekeraars te verbieden om losgeld te vergoeden bij slachtoffers van een ransomware-aanval? Zo ja, hoe verklaart u dit verschil in beleid ten opzichte van wel en niet verzekerde bedrijven? Welke mogelijkheden worden er nog meer onderzocht om te kijken of het aantal losgeldbetalingen verminderd kan worden?

Antwoord 2
Ja, een verbod op het vergoeden van betaald losgeld aan cybercriminelen na een ransomware-aanval door verzekeraars wordt momenteel onderzocht. Hierbij worden de voor- en nadelen en de juridische mogelijkheden geïnventariseerd. Er is geen besluit over genomen. Daarnaast wordt gekeken naar hoe overheden om moeten gaan met ransomware, waaronder losgeldbetalingen. De meest wenselijke wijze van het beperken van losgeldbetalingen ligt echter in het voorkomen dat personen en organisaties überhaupt slachtoffer worden van ransomware.

[1] NOS, 19 september 2021, «Overheid in actie tegen betalen van losgeld aan ransomware-criminelen», https://nos.nl/artikel/2398399-overheid-in-actie-tegen-betalen-van-losgeld-aan-ransomware-criminelen

ah-tk-20212022-225
ISSN 0921 - 7398
's-Gravenhage 2021

Vraag 3
Bent u het ermee eens dat het betalen van losgeld bij ransomware aanvallen onwenselijk is en dat bedrijven zich tegelijkertijd soms genoodzaakt voelen losgeld te betalen op korte termijn, omdat anders de continuïteit van bedrijfsprocessen in gevaar komt? Zo ja, hoe beoordeelt u dan een algeheel verbod op het betalen van losgeld? Zo nee, waarom niet? En bent u het ermee eens dat er daarom ingezet moet worden op het dringende advies om niet te betalen? Zo nee, waarom niet?

Antwoord 3
Het dringende advies vanuit het Kabinet blijft om geen losgeld te betalen na een ransomware-aanval, aangezien dit het crimineel verdienmodel in stand houdt. De politie stelt vast dat een relevant deel van het door slachtoffers betaalde losgeld rechtstreeks wordt geïnvesteerd in nieuwe aanvalsinfrastructuren.[2] Ik heb begrip voor de moeilijke positie waarin slachtoffers van ransomware zich soms bevinden. Een algemeen verbod op het betalen van losgeld kan leiden tot minder losgeldbetalingen, maar kan ook grote nadelige effecten hebben. Op dit moment is er geen voornemen om losgeldbetalingen wettelijk te verbieden.

Vraag 4
Bent u het ermee eens dat ondernemers en organisaties vooral slachtoffer zijn bij een ransomware-aanval? Zo nee, waarom niet?

Antwoord 4
Ja.

Vraag 5
Bent u zich ervan bewust dat het niet betalen van losgeld kan leiden tot een situatie waarin systemen weer vanaf de grond opnieuw moeten worden opgebouwd wat vaak langer duurt en meer geld kost dan het betalen van losgeld?

Antwoord 5
Ja. Criminelen die ransomware-aanvallen uitvoeren maken een zorgvuldige calculatie bij het stellen van de losgeldeis. Indien er geen losgeld wordt betaald en er geen back-up beschikbaar is, kan dit tot gevolg hebben dat de versleutelde data verloren gaat en de ICT-infrastructuur opnieuw moet worden opgebouwd. Ook kan een aanval leiden tot openbaarmaking van gestolen informatie en gegevens. De totale kosten voor een organisatie om een ransomware-aanval te boven te komen, zoals gevolgschade of het verlies van kostbare informatie, zijn vaak groter dan het geëiste losgeldbedrag.[3] Ook indien er wel losgeld wordt betaald en de sleutel door criminelen wordt verstrekt, leidt dit niet gegarandeerd tot succes. Zo kan de sleutel niet goed functioneren waardoor de toegang tot data en systemen niet wordt hersteld. Verder zal in veel gevallen de hele ICT-infrastructuur alsnog opnieuw moeten worden opgebouwd, aangezien deze als gecompromitteerd moet worden beschouwd. Omdat doorgaans na een ransomwarebesmetting de integriteit van de ICT-infrastructuur niet meer kan worden gewaarborgd en een organisatie zijn systemen dus niet meer kan vertrouwen, zal deze dus ook bij betaling vaak vervangen moeten worden. Bovendien blijven kwaadwillenden beschikken over eventuele buitgemaakte data en kan er opnieuw een losgeld geëist worden om publicatie daarvan te voorkomen.

Vraag 6
Bent u zich ervan bewust dat een algemeen verbod op het betalen van losgeld zelfs kan leiden tot het faillissement van een getroffen bedrijf? Zo ja, bent u het ermee eens dat dit een zeer onwenselijk scenario is voor getroffen bedrijven en dat een verbod op het betalen van losgeld het probleem van ransomware aanvallen op bedrijven niet oplost? Zo nee, waarom niet?

---

[2] Cybersecuritybeeld Nederland (CSBN) 2021, p.29
[3] CSBN 2021, p. 30

Antwoord 6
Ja. Een ransomware-aanval kan grote impact hebben op slachtoffers, maar ook op diens klanten en gebruikers. In uiterste gevallen kan dit leiden tot een faillissement. De nadelige gevolgen van een algemeen verbod op het betalen van losgeld kunnen daarom zeer groot zijn. Op dit moment is er geen voornemen om losgeldbetalingen wettelijk te verbieden. Zoals gemeld in het antwoord op vraag 2 wordt de mogelijkheid van een verbod op het vergoeden van losgeldbetalingen door verzekeraars wel onderzocht.

Vraag 7
Bent u het ermee eens dat de oplossing moet worden gezocht in ransomware aanvallen in eerste instantie voorkomen door te focussen op preventieve maatregelen en de digitale basishygiëne van bedrijven vergroten? Zo ja, welke mogelijkheden ziet u hiertoe? Zo nee, waarom niet?

Antwoord 7
De meest wenselijke wijze van het beperken van losgeldbetalingen ligt in het voorkomen dat personen en organisaties slachtoffer worden van ransomware. Preventie vormt een belangrijk onderdeel bij het tegengaan van cybercrime, waaronder ook ransomware. Het beeld is dat bij veel succesvolle ransomware-aanvallen de basismaatregelen onvoldoende getroffen zijn. Om de cyberweerbaarheid te vergroten biedt het Digital Trust Center (DTC) van het Ministerie van EZK verschillende kennisproducten aan met adviezen voor ondernemers om een besmetting met ransomware te voorkomen en adequaat te reageren als het toch gebeurt. Daarnaast biedt het DTC mogelijkheden om de cyberweerbaarheid van een bedrijf te testen middels een basisscan. Ook het NCSC biedt voor diens achterban diensten en producten aan om de cyberweerbaarheid te verhogen. Veel informatie en adviezen zijn voor het brede publiek beschikbaar op de website van het NCSC. Verder wordt in het kader van het convenant voor preventie van cybercrime met private partijen samengewerkt aan de verbreding van het gebruik van twee-factor authenticatie.[4] De politie geeft aan dat dit al aanzienlijk kan helpen bij het tegengaan van ransomware. Het verhogen van de cyberweerbaarheid van burgers, bedrijven en organisaties vraagt blijvende inspanning.

[4] Kamerstuk 26 643, nr. 768, p. 3