Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

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

## 1558

Vragen van de leden **Kathmann** en **Mutluer** (beiden GroenLinks-PvdA) aan de Staatssecretaris van Economische Zaken en Klimaat en de Minister van Justitie en Veiligheid over *het bericht «Hackers persen Odido af na datalek en eisen een miljoen euro losgeld»* (ingezonden 27 februari 2026).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) en de Staatssecretaris van Economische Zaken en Klimaat (ontvangen 8 april 2026).

Vraag 1
Bent u bekend met het bericht «Hackers persen Odido af na datalek en eisen een miljoen euro losgeld»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat het verdienmodel van cybercriminelen voor een groot deel draait op het afpersen van slachtoffers, onder dreiging van het publiceren van gestolen data of het voor eeuwig versleutelen van systemen?

Antwoord 2
De modus operandi van cybercriminelen waarbij slachtoffers worden afgeperst onder dreiging van het publiceren van gestolen data of versleuteling is bekend.[2]

Vraag 3
Vindt u dat het toegeven aan dit soort afpersing het verdienmodel van cybercriminelen in stand houdt? Hoe verhoudt dit zich volgens u tot de bescherming van slachtoffers, die hun persoonlijke data in handen van criminelen zien verdwijnen als een getroffen organisatie niet betaalt?

Antwoord 3
Slachtoffer worden van ransomware en dit soort afpersing kan veel impact hebben. De schade kan enorm oplopen en plaatst een getroffen bedrijf in een moeilijke positie, ook richting klanten. Zeker in dit geval waar het aantal

[1] Nu.nl, 24 februari 2026
[2] CSBN 2021

ah-tk-20252026-1558
ISSN 0921 - 7398
's-Gravenhage 2026

gestolen gegevens zo omvangrijk is. De uiteindelijke afweging is aan de getroffen organisatie, maar het dringende advies vanuit de overheid blijft: geen losgeld betalen. Het betalen van losgeld biedt geen garantie dat criminelen systemen weer toegankelijk maken of gestolen data niet doorverkopen aan andere criminelen. Het uitbetalen van losgeld houdt bovendien het verdienmodel van criminelen in stand. En lokt daarmee mogelijk nieuwe aanvallen op Nederlandse organisaties uit.
Er kan zich spanning voordoen tussen het belang van een individueel slachtoffer om op de korte termijn schade te beperken en het bredere maatschappelijke belang om het totaal aantal (potentiële) slachtoffers te verminderen en het verdienmodel van criminelen niet in stand te houden. Het is vooral belangrijk dat getroffen personen informatie krijgen over de risico's die zij lopen en wat zij daartegen kunnen doen. Mensen die vermoeden dat ze slachtoffer zijn geworden van de diefstal van hun gegevens, kunnen op de site van de politie controleren[3] of hun data in handen van criminelen is gevallen.

Vraag 4
Klopt het dat het voor een getroffen organisatie logisch kan lijken om losgeld te betalen (op basis van de belofte van daders dat gestolen data niet gepubliceerd worden of versleutelde systemen worden vrijgegeven), maar dat dit de samenleving als geheel juist meer kan kosten, omdat het verdienmodel van cybercriminelen in stand gehouden wordt? Zo nee, waarom niet? Zo ja, op welke manier kan de samenleving volgens u dit dilemma oplossen?

Antwoord 4
Slachtoffer worden van dergelijke afperspraktijken kan veel impact hebben. De schade kan enorm oplopen en plaatst een getroffen bedrijf in een moeilijke positie, ook richting hun klanten. Zeker in dit geval waar het aantal gestolen gegevens zo omvangrijk is. De uiteindelijke afweging ligt bij de getroffen organisatie, maar het dringende advies van de overheid blijft om geen losgeld te betalen. Betaling van losgeld biedt geen garantie dat criminelen systemen herstellen, gestolen data verwijderen of ervan afzien deze openbaar te maken of door te verkopen aan andere criminelen. Daarnaast houdt het betalen van losgeld het verdienmodel van cybercriminelen in stand. De opbrengsten worden veelal ingezet voor verdere, geavanceerde cyberaanvallen, waarmee nieuwe slachtoffers worden gemaakt. Dit kan bovendien nieuwe aanvallen op Nederlandse organisaties uitlokken.

Vraag 5
Staat u nog steeds achter het advies van de overheid aan organisaties om geen losgeld aan hackers te betalen? Op welke expertkennis baseert u dat advies?

Antwoord 5
Ja, zie de antwoorden op de voorgaande vragen. Dit sluit aan bij het inzicht en advies van de politie en het OM.

Vraag 6
Zou een verbod op het betalen van losgeld aan hackers de samenleving als geheel ten goede kunnen komen? Zo ja, waarom? Zo nee, waarom niet? Wat zijn volgens u de voor- en nadelen van een dergelijk verbod?

Antwoord 6
We willen organisaties die slachtoffer zijn geworden van een ransomware aanval niet criminaliseren. Er kan zich spanning voordoen tussen het belang van een individueel slachtoffer om op de korte termijn schade te beperken en het bredere maatschappelijke belang om het totaal aantal (potentiële) slachtoffers te verminderen en het verdienmodel van criminelen niet in stand te houden. Zolang die spanning niet eenduidig kan worden opgelost wordt – net als in de meeste EU landen – dringend geadviseerd om geen losgeld te betalen, in plaats van een wettelijk verbod. Daarnaast wordt ingezet op

[3] https://www.politie.nl/nieuws/2026/maart/2/checkjehack-aangevuld-met-odido.html

preventie, meldplichten bij toezichthouders en gerichte informatie aan individuen wier gegevens zijn getroffen.

Vraag 7
Kan een verbod op het betalen van losgeld ook dienen als extra prikkel voor organisaties om extra werk te maken van cyberweerbaarheid? Zo nee, waarom niet?

Antwoord 7
Het huidige wettelijke kader (Telecommunicatiewet, Wbni, de AVG en de aankomende Cyberbeveiligingswet) verplicht organisaties om serieus werk te maken van cyberweerbaarheid. Zoals uiteengezet in het antwoord op vraag 2 is daarbij het dringende advies om geen losgeld te betalen. Er kunnen situaties voorkomen waarbij toch een andere afweging wordt gemaakt door een organisatie. Om deze reden achten wij een volledig wettelijk verbod onwenselijk.

Vraag 8
Welke extra prikkels en instrumenten kunt u inzetten om ervoor te zorgen dat organisaties te dwingen hun cyberweerbaarheid serieus te nemen? Denkt u dat boetes hier een effectief middel voor kunnen zijn? Zo ja, op welke manier? Zo nee, waarom niet?

Antwoord 8
Het huidige wettelijke kader (Telecommunicatiewet, Wbni en AVG) biedt de nodige handhavende bevoegdheden om in te grijpen bij vastgestelde onregelmatigheden. Ingrijpen kan bijvoorbeeld door het bevestigen van normen, het geven van waarschuwingen, stilleggen van verwerkingen van persoonsgegevens of het opleggen van boetes. Onder de zorgplicht van de Telecommunicatiewet moeten organisaties passende technische en organisatorische maatregelen nemen om beveiligingsrisico's te beheersen. Hieronder vallen ook risico's met betrekking tot diensten zoals een klantsysteem. De Rijksinspectie Digitale Infrastructuur houdt toezicht op de Telecomwet en de Autoriteit Persoonsgegevens houdt toezicht op de AVG.
Daarnaast wordt met de aankomende implementatie van de Cyberbeveiligingswet (Cbw) een impuls gegeven aan de wettelijke verplichtingen voor essentiële en belangrijke entiteiten om maatregelen te nemen die bijdragen aan hun eigen cyberweerbaarheid. Ook is er sprake van een meldplicht bij significante incidenten. De verplichtingen uit de Cbw worden gehandhaafd door de bevoegde toezichthouders/autoriteiten. Organisaties worden onderworpen aan een beveiligingsscan en audit, en kunnen een aanwijzing, de verplichting tot het openbaar maken van een overtreding, een last onder bestuursdwang, een last onder dwangsom en een bestuurlijke boete opgelegd krijgen.

Vraag 9
Kunt u deze vragen afzonderlijk van elkaar en binnen de gestelde termijn beantwoorden?

Antwoord 9
ja.