Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

2822

Vragen van de leden **Mutluer** en **Kathmann** (beiden GroenLinks-PvdA) aan de Minister van Justitie en Veiligheid en de staatsecretaris van Binnenlandse Zaken en Koninkrijkrelaties over *de hackaanval op het Openbaar Ministerie* (ingezonden 28 juli 2025).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 12 augustus 2025)

Vraag 1
Bent u bekend met het bericht: «Digitale werkomgeving OM inderdaad gehackt, onderzoek moet uitwijzen welke informatie is gestolen»?[1]

Antwoord 1
Ja.

Vraag 2
Wat werd aangetroffen in de eerste scans van het Nationaal Cyber Security Centrum (NCSC) waaruit bleek dat onbevoegden de systemen van het Openbaar Ministerie (OM) zijn binnengedrongen?

Antwoord 2
Op 17 juli jl. berichtte ik u dat het OM uit voorzorg de interne systemen had losgekoppeld van het internet. Het NCSC heeft met gerichte scans gezocht naar kwetsbare of mogelijk gecompromitteerde systemen. Een analyse van de OM-omgevingen heeft reden gegeven om aan te nemen dat er gebruik is gemaakt van deze mogelijke kwetsbaarheid. Het NCSC heeft daarop het OM geïnformeerd en geadviseerd om nader onderzoek te verrichten. Inmiddels is een eerste technisch en forensisch onderzoek uitgevoerd.[2] Tot op heden zijn er geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald. Verder onderzoek vindt nog plaats.

[1] NRC, 22 juli 2025, «Digitale werkomgeving OM inderdaad gehackt, onderzoek moet uitwijzen welke informatie is gestolen», www.nrc.nl/nieuws/2025/07/22/digitale-werkomgeving-om-inderdaad-gehackt-onderzoek-moet-uitwijzen-welke-informatie-is-gestolen

[2] Kamerstukken II, 2024–2025, 26 643, nr. 1378.

ah-tk-20242025-2822
ISSN 0921 - 7398
's-Gravenhage 2025

Vraag 3 en 4
Bent u op de hoogte van het soort gegevens dat mogelijk is ingezien of buitgemaakt door onbevoegden? Heeft u gericht maatregelen genomen op basis van deze informatie?
Zijn er aanwijzingen dat persoonsgegevens van medewerkers, zoals e-mailadressen, inloggegevens, telefoonnummers of privéadressen, zijn buitgemaakt of ingezien door onbevoegden?

Antwoord 3 en 4
Zoals aangegeven in de beantwoording van vraag 2 is zijn er tot op heden geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald. Er wordt nog nader onderzoek gedaan. Over het lopende strafrechtelijk onderzoek kan ik u gedurende dat onderzoek geen mededelingen doen.

Vraag 5 en 6
Wordt er onderzocht welke gevolgen deze hackaanval kunnen hebben voor de digitale en fysieke veiligheid van OM-medewerkers, met name zij die betrokken zijn bij zware strafzaken ten aanzien van ondermijnende criminaliteit? Zo nee, bent u bereid dit wel te doen?
Zijn er aanwijzingen dat persoonsgegevens van getuigen of slachtoffers zijn buitgemaakt of ingezien door onbevoegden? Wat doet u om hun veiligheid te waarborgen?

Antwoord 5 en 6
Tot op heden zijn er geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald. Verder onderzoek vindt nog plaats.

Vraag 7
Is er een (voorlopige) risicoanalyse gemaakt en worden er op basis daarvan al maatregelen genomen om kwetsbaarheden af te dekken, naast het offline halen van het OM?

Antwoord 7
Er zijn maatregelen genomen om kwetsbaarheden af te dekken. Inmiddels gaat het OM stapsgewijs weer online. Dit proces moet zorgvuldig worden ingericht, met versterkte monitoring en detectie, omdat misbruik nooit helemaal kan worden uitgesloten.[3]

Vraag 8 en 9
Welke overheidsorganisaties maken nog meer gebruik van Citrix-software die dezelfde kwetsbaarheid bevat? Welke maatregelen nemen zij om mogelijke hackaanvallen te onderzoeken en zo nodig hun systemen veilig te stellen, gezien u in de brief van 23 juli j.l. schrijft dat het NCSC heeft geadviseerd dat alle organisaties die deze software gebruiken mogelijk misbruik moeten onderzoeken (Kamerstuk 26 643, nr. 1377)?
Hoe wordt actuele en relevante informatie uit het onderzoek van het OM gedeeld met andere organisaties die mogelijk ook zijn getroffen door een hackaanval? Bent u bereid deze informatie ook proactief met commerciële partijen te delen?

Antwoord 8 en 9
Het NCSC heeft alle organisaties die Citrix NetScaler ADC en Citrix NetScaler Getaway gebruiken opgeroepen om onderzoek te doen naar mogelijk gebruik en misbruik van de kwetsbaarheden, ook als de kwetsbaarheden reeds zijn verholpen middels de update. CIO Rijk heeft deze casuïstiek en het handelingsperspectief van het NCSC bij alle departementen middels meerdere CISO-briefings onder de aandacht gebracht, met het dringende advies dit op te volgen.
Het NCSC vervult een coördinerende rol in de informatie-uitwisseling door continu informatie samen te brengen en te delen, zodat organisaties zelf in staat zijn aanvullend onderzoek te verrichten. Binnen de juridische kaders verstrekt het NCSC informatie als duiding, handelingsperspectieven en

[3] Kamerstukken II, 2024–2025, nr. 1378.

beveiligingsadviezen via verschillende netwerken en (openbare) kanalen aan zowel publieke als private organisaties.
Ik kan alleen ingaan op de organisaties die onder mijn departement vallen en verwijs daarvoor onder meer naar de Kamerbrieven van 17 juli jl.[4] en van 12 augustus jl.[5]

Vraag 10
Hoe worden ketenpartners waar de systemen van het OM mee zijn geïntegreerd betrokken bij deze operatie? Ontvangen zij ook steun voor het onderzoeken van eigen systemen of om belemmeringen in hun werk te voorkomen?

Antwoord 10
De gehele afsluiting van het OM van het internet had impact op het OM zelf en alle samenwerkingspartners. Door alle betrokkenen is dagelijks hard gewerkt om de ontstane knelpunten en effecten zoveel mogelijk op te lossen, met als doel de impact zoveel mogelijk beperken en de mogelijke risico's mitigeren. Over de impact op de strafrechtketen heb ik u op 12 augustus jl. geïnformeerd.[6]

Vraag 11
Is het mogelijk om het herstel van de OM-systemen sneller te laten verlopen dan de verwachte wekenlange operatie? Zo ja, bent u bereid capaciteit vrij te maken om dit te versnellen?

Antwoord 11
Op basis van de onderzoeksresultaten van het technisch en forensisch onderzoek – en het naarmate het offline zijn van het OM langer duurt, steeds zwaarwegender belang van het goed functioneren van de strafrechtketen en de impact daarvan op de maatschappij – heeft het College van procureurs-generaal het besluit genomen dat het verantwoord en wenselijk is om het OM weer in fasen online te laten gaan. Over deze stapsgewijze livegang van het OM heb ik uw Kamer op 4 augustus geïnformeerd.[7]

Vraag 12
Wat zijn de praktische gevolgen van het offline halen van de systemen voor OM-medewerkers en lopende strafzaken? Is de organisatie voldoende uitgerust om taken analoog of met back-up systemen volwaardig op te pakken?

Antwoord 12
Medewerkers van het OM konden alleen inloggen op kantoorlocaties, waren niet per mail bereikbaar en er was sprake van een beperkte functionaliteit van de systemen.[8] In de periode dat het OM geheel offline was kon er geen enkele digitale informatie van en naar het OM worden gestuurd. Dit raakten alle ketenpartners in en rondom de strafrechtketen. Het OM en ketenpartners stelden werkprocessen vast om proces(stukken) per post, fysiek of door andere organisaties dan het OM aan te leveren. Daarnaast had het OM speciale aandacht voor het informeren van slachtoffers en hun gemachtigden. Dit toont de inventiviteit, enorme inzet en bereidheid om samen te werken in de strafrechtketen. Over de verdere impact op de organisaties in en rondom de strafrechtketen heb ik u op X augustus geïnformeerd.[9]

Vraag 13
Worden verdachten, advocaten, rechters en andere betrokkenen in de keten actief geïnformeerd over de gevolgen die zij mogelijk ondervinden?

---

[4] Kamerstukken II, 2024–2025, 26 643, nr. 1376,
[5] Kamerstukken II, 2024–2025, 26643, nr. XXX
[6] Kamerstukken II, 2024–2025, 26643, nr. XXX
[7] Kamerstukken II, 2024–2025, 26 643, nr. 1378.
[8] Kamerstukken II, 2024–2025, 26 643, nr. 1377.
[9] Kamerstukken II, 2024–2025, 26643, nr. XXX

Antwoord 13
Het OM heeft Q&A's geplaatst op de eigen website met daarin de veelgestelde vragen op een rij voor de advocatuur, inclusief een apart overzicht voor slachtofferadvocatuur en daarnaast voor slachtoffers. Ook is informatie over de telefonische bereikbaarheid van het OM opgenomen.[10] Deze overzichten worden steeds bijgewerkt. Ook op de website van de Rechtspraak is een overzicht met veelgestelde vragen te vinden over de invloed die de IT-problemen bij het OM kunnen hebben op lopende strafzaken.[11] Het CJIB en Slachtofferhulp Nederland (SHN) geven op hun websites aan dat de situatie bij het OM gevolgen heeft voor de eigen werkzaamheden en dat – ook met de gegeven alternatieve oplossingen – als gevolg daarvan slachtoffers in bepaalde gevallen mogelijk minder goed geïnformeerd en/of proactief ondersteund kunnen worden.[12]

Vraag 14 en 15
Wanneer is er sprake van genoeg zekerheid om (delen van) het interne systeem weer online te brengen? Hoe voorkomt u dat er uit haast onvoldoende voorzorg wordt genomen, zolang niet precies bekend is wat de ernst van de hack is?
Hoe draagt u bij aan het zo snel mogelijk inzicht krijgen van de gevolgen en het veilig online brengen van de het interne OM-netwerk? Stelt u hiervoor extra capaciteit beschikbaar?

Antwoord 14 en 15
Zoals reeds aan uw Kamer gemeld, zijn er tot op heden er geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald. Op 4 augustus jl. heb ik u geïnformeerd over het stapsgewijs weer online gaan van de systemen van het OM.[13] Dit proces wordt zorgvuldig ingericht met versterkte monitoring en detectie. Ik heb het OM verzocht om bij deze gefaseerde livegang in afstemming met de keten te bezien welke essentiële processen met prioriteit weer gedigitaliseerd doorgang moeten vinden.

Vraag 16
Is de Autoriteit Persoonsgegevens betrokken bij deze operatie? Kunt u hen nauw betrekken zodat er snel gehandeld kan worden als blijkt dat persoonsgegevens ingezien of buitgemaakt zijn?

Antwoord 16
De Autoriteit Persoonsgegevens is reeds door het OM en JIO ingelicht over de situatie. Waar nodig wordt vanzelfsprekend nauw contact onderhouden met de Autoriteit Persoonsgegevens.

Vraag 17
Heeft u contact gehad met Citrix over de kwetsbaarheid in hun software? Kan de leverancier bijdragen aan een oplossing voor het OM?

Antwoord 17
Ja, met Citrix is regelmatig contact over de kwetsbaarheden en oplossingen hiervoor.

Vraag 18
Kunt u, zo nodig vertrouwelijk, de Kamer informeren over de interne toelichting die is gegeven aan het OM en bekend is bij het NRC?

---

[10] https://www.om.nl/onderwerpen/inbreuk-om-ict
[11] https://www.rechtspraak.nl/Voor-advocaten-en-juristen/Reglementen-procedures-en-formulieren/Strafrecht/Paginas/IT-problemen-bij-OM.aspx
[12] https://www.cjib.nl/nieuws/om-langzaam-weer-online-informatie-uitwisseling-met-cjib-nog-niet-normaal
https://www.slachtofferhulp.nl/nieuws/2025/situatie-om-raakt-ook-het-werk-van-slachtofferhulp-nederland-beperkt/
[13] Kamerstukken II, 2024–2025, 26 643, nr. 1378.

Antwoord 18
Ik acht het niet opportuun om in te gaan op mediaberichtgeving over interne communicatie binnen het OM. Het is aan het OM om daar al dan niet op te reageren. Voor het overige verwijs ik naar de Kamerbrieven die uw Kamer over dit onderwerp zijn toegestuurd.

Vraag 19
Kunt u deze vragen afzonderlijk van elkaar en spoedig beantwoorden, en indien mogelijk betrekken bij de eerstvolgende update over de situatie?

Antwoord 19
Waar relevant zijn antwoorden samengevoegd om herhaling te voorkomen.