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

2823

Vragen van de leden **Buijsse** en **Michon-Derkzen** (beiden VVD) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie en Veiligheid over *de brief van de Minister van Justitie en Veiligheid «Informatiebeveiliging OM»*.[1] (ingezonden 21 juli 2025).

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

Vraag 1
Bent u van mening dat het loskoppelen van de interne digitale omgeving van het Openbaar Ministerie (OM) een zware maatregel is?

Antwoord 1
Het loskoppelen van het OM van het internet is inderdaad een zware maatregel. Het OM heeft mij echter laten weten dat die in dit geval onvermijdelijk werd geacht.

Vraag 2
Kunt u uitleggen waarom dit uit voorzorg gedaan is? Welke gebeurtenissen of risico's gaven daar aanleiding toe?

Antwoord 2
Op 17 juli jl. berichtte ik u dat het OM uit voorzorg de interne systemen heeft losgekoppeld van het internet vanwege signalen van een mogelijke kwetsbaarheid in de Citrix-systemen.[2] Op basis van het technisch en forensisch onderzoek is vastgesteld dat er inderdaad gebruik is gemaakt van de kwetsbaarheden in die systemen. Tot op heden zijn er echter geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald. Verder forensisch en strafrechtelijk onderzoek vindt nog plaats. Inmiddels heeft het College van procureurs-generaal besloten om het OM stapsgewijs weer aan te laten sluiten op het internet. Hierover heb ik u op 4 augustus jl. geïnformeerd.[3]

[1] Kamerstuk 26 643, nr. 1376.
[2] Kamerstukken II, 2024–2025, 26 643, nr. 1376.
[3] Kamerstukken II, 2024–2025, 26 643, nr. 1378.

ah-tk-20242025-2823
ISSN 0921 - 7398
's-Gravenhage 2025

Vraag 3
Zijn er mogelijk vertrouwelijke gegevens ingezien of gestolen?

Antwoord 3
Zoals reeds gemeld in de brief van 4 augustus jl. zijn er tot op heden geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald.

Vraag 4
Zijn de back-ups van dossiers geborgd?

Antwoord 4
Ja.

Vraag 5
Bestaat het risico op vertraging of vormfouten in lopende strafzaken door het misbruik van deze kwetsbaarheid bij het OM? Of zijn er andere operationele risico's?

Antwoord 5
In algemene zin had de gehele afsluiting van het OM van het internet 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. Het OM en alle ketenpartners hebben intensief samengewerkt. Het doorgaan van zittingen en behandelen van strafzaken hebben prioriteit gekregen en voor spoedeisende processen zijn afspraken gemaakt met ketenpartners.
Tegelijkertijd leidt de situatie tot verstoringen en vertragingen in de operationele werkprocessen met ketenpartners. Om deze operationele uitdagingen zoveel als mogelijk te mitigeren, zijn er verschillende maatregelen geïmplementeerd. Over de meest recente situatie, inclusief de knelpunten en effecten, heb ik uw Kamer op 12 augustus jl. geïnformeerd.[4]

Vraag 6
Zijn er maatregelen genomen om de bestaande, bekende kwetsbaarheden te verminderen?

Antwoord 6
In de periode vanaf juni 2025 tot aan 23 juli 2025 zijn er meerdere kwetsbaarheden bekend geworden van Citrix-systemen. Het NCSC heeft alle organisaties die Citrix NetScaler ADC en Citrix NetScaler Getaway gebruiken opgeroepen om onderzoek te doen naar mogelijk gebruik van de kwetsbaarheden, ook als de kwetsbaarheden reeds waren verholpen middels de update. Het NCSC heeft hier verschillende beveiligingsadviezen voor uitgebracht.
Het OM heeft naar aanleiding hiervan verscheidene maatregelen genomen, waaronder het loskoppelen van de systemen van het internet, en het bijwerken onder meer van de software waardoor de kwetsbaarheid is ontstaan om het veiligheidslek te dichten. Ook loopt er een strafrechtelijk onderzoek. Daarnaast heeft het OM onderzoek gedaan om gebruik van de systemen te kunnen onderkennen of uit te kunnen sluiten. Er zijn tot op heden geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald.
De livegang van de systemen van het OM dient stapsgewijs plaats te vinden, onder meer omdat deze zorgvuldig moet worden ingericht, met versterkte monitoring en detectie, omdat misbruik nooit helemaal kan worden uitgesloten.

Vraag 7
Welke maatregelen worden getroffen om te voorkomen dat rechters structureel door voorzorgsmaatregelen worden gehinderd in hun werkzaamheden, in het geval er toch een kwetsbaarheid aan het licht komt?

---

[4] Kamerstukken II, 2024–2025, 26643, nr. XXX

Antwoord 7
Met uitzondering van de (super) snelrechtzittingen hebben de zittingen voor het overgrote deel doorgang kunnen vinden. Wel zijn er alternatieve oplossingen bedacht voor werkprocessen om doorgang te kunnen waarborgen. Zo kon de advocatuur (proces)stukken die kort voor de behandeling van de zitting aangeleverd dienen te worden, sturen naar de Rechtspraak, die de processtukken vervolgens heeft verspreid naar de procespartijen. Daarnaast is er voor spoedeisende beslissingen geregeld dat de Rechtspraak – in plaats van het OM – deze naar het CJIB (Centraal Justitieel Incassobureau) stuurt. Het CJIB legt de beslissingen vervolgens op gebruikelijke en juiste wijze ten uitvoer. De focus ligt nu op de livegang van het OM. Het is nog te vroeg om te beoordelen of het nodig is om structurele maatregelen te treffen.

Vraag 8, 9 en 10
Zijn er redenen waarom de beschikbare, uitgebrachte patch niet kon voorkomen dat deze kwetsbaarheid is gemitigeerd?
Wanneer heeft het OM de patch geïmplementeerd?
Was de implementatietijd van de patch voldoende om de systemen te beschermen tegen de hack?

Antwoord 8, 9 en 10
Het moment waarop gebruik is gemaakt van de kwetsbaarheid in relatie tot het moment van patchen hangt samen met onderdelen uit het strafrechtelijk onderzoek. Ik wil niet op de uitkomsten daarvan vooruitlopen.

Vraag 11, 12 en 13
Is er binnen het huidige audit- en screeningbeleid voldoende en tijdige aandacht geweest voor deze kwetsbaarheid? Geldt dit ook voor de leverancier van Citrix Netscaler?
Heeft het OM tijdig en adequaat gereageerd op de waarschuwingen van het Nationaal Cyber Security Centrum (NCSC)?
Wat zijn de protocollen voor het omgaan met dergelijke waarschuwingen en zijn deze gevolgd?

Antwoord 11, 12 en 13
Het NCSC heeft op verschillende momenten beveiligingsadviezen uitgebracht aan alle organisaties over de kwetsbaarheden in de Citrix-systemen, en heeft het OM naar aanleiding daarvan verschillende stappen gezet. Het OM volgt standaard operationele procedures om zo adequaat mogelijk te reageren op waarschuwingen. Er loopt nog nader onderzoek naar de omvang van het eventuele gebruik, de preventieve maatregelen die zijn genomen en de effecten daarvan.

Vraag 14
Kunt u deze vragen een voor een beantwoorden?

Antwoord 14
De vragen zijn waar relevant in samenhang beantwoord ter voorkoming van herhaling.