

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

335

Vragen van het lid **Eerdmans** (JA21) aan de Minister van Justitie en Veiligheid over *het datalek bij het Openbaar Ministerie* (ingezonden 25 augustus 2025).

Antwoord van Minister **Van Oosten** (Justitie en Veiligheid) (ontvangen 4 november 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 3103.

Vraag 1

Kunt u toelichten welke herstelstappen sinds de hack zijn gezet om herhaling te voorkomen en hoe u de effectiviteit van deze maatregelen verifieert, specifiek met het oog op bescherming van gevoelige categorieën informatie, zoals adressen van Blijf-van-mijn-lijf-huizen en andere beschermde opvanglocaties, gegevens over kroongetuigen en hun naasten, dossiers over zware georganiseerde misdaad en terrorisme, interne HR-dossiers die officieren van justitie en andere functionarissen mogelijk chantabel of afpersbaar maken?

Antwoord 1

Er zijn sinds de ontdekking van de ICT-inbreuk meerdere herstelstappen gezet. Hierover is uw Kamer per brief op 23 juli, 4 augustus, 12 augustus en 3 september geïnformeerd.¹ Het OM voldoet aan de kaders en richtlijnen voor informatiebeveiliging die door het Rijk en het Ministerie van Justitie en Veiligheid worden voorgeschreven. Het OM is dit verplicht als zelfstandige organisatie binnen het justitiedomein. Dit zal voor de toekomst ongewijzigd blijven en langs deze kaders en richtlijnen zijn de herstelwerkzaamheden ook verder uitgevoerd.

De livegang van de systemen van het OM vond stapsgewijs plaats zodat per stap extra monitoring en detectie kon plaatsvinden. Elk systeem dient zeker te worden gesteld voordat het weer live kan gaan. Die fasering heeft te maken met de volgorde waarin systemen moeten worden opgestart; die volgorde voorkomt dat werkprocessen met en tussen ketenpartners worden verstoord als informatie uit de verschillende systemen niet in de goede volgorde wordt ingeladen. Over de impact op de strafrechtketen naar aanleiding van de offline-gang van het Openbaar Ministerie (OM) is uw Kamer reeds geïnformeerd.² Ook is uw Kamer geïnformeerd over het besluit dat samen met het

¹ Kamerstuk 26 643, 2025–2026, nrs. 1377, 1378, 1379, 190.

² Kamerstuk 26 643, nr. 1379, vergaderjaar 2025–2026

OM is genomen om onderzoek te doen over de ICT-inbreuk.³ Dat onderzoek zal zich onder andere moeten richten op de wijze waarop incidenten in de informatiebeveiliging in de toekomst voorkomen kunnen worden.

Vraag 2 t/m 5

In hoeverre kan technisch of forensisch worden vastgesteld of adressen van Blijf-van-mijn-lijf-huizen en andere beschermde opvanglocaties, gegevens over kroongetuigen en hun naasten of dossiers over zware georganiseerde misdaad en terrorisme, daadwerkelijk zijn ingezien of buitgemaakt?

Welke specifieke maatregelen zijn genomen om te achterhalen of HR-dossiers van medewerkers, inclusief aanklagers en officieren van justitie, mogelijk in handen van kwaadwillenden zijn gekomen en hen kwetsbaar maken voor chantage en/of afpersing?

Zijn er signalen of indicaties dat met mogelijk buitgemaakte informatie al pogingen zijn gedaan om procespartijen, getuigen of medewerkers van het Openbaar Ministerie (OM) te beïnvloeden of te intimideren?

Betekent, dat u stelt dat er geen aanwijzingen zijn voor datamanipulatie, ook kunt u uitsluiten dat gevoelige gegevens zijn gekopieerd of op termijn kunnen worden misbruikt? Zo nee, welke voorzorgsmaatregelen zijn getroffen tegen langdurig sluimerend misbruik?⁴

Antwoord 2 t/m 5

Inmiddels is een eerste technisch en forensisch onderzoek uitgevoerd. Tot op heden zijn er geen aanwijzingen dat data (strafvorderlijk of anderszins) is gemanipuleerd of weggehaald. Er wordt nog nader strafrechtelijk onderzoek gedaan. Over het lopende strafrechtelijke onderzoek kan ik geen mededelingen doen.

Er zijn maatregelen genomen om risico's zoals hernieuwd misbruik van systemen en het risico op datamanipulatie te mitigeren. Inmiddels is het OM weer online.

Vraag 6

Kunt u uiteenzetten hoe het OM en het ministerie ervoor zorgen dat ook ketenpartners zoals politie, rechtspraak en opvanginstellingen volledig op de hoogte zijn van de mogelijke risico's, zodat zij preventief maatregelen kunnen nemen?

Antwoord 6

De gehele afsluiting van het OM van het internet had impact op het OM zelf en op alle samenwerkingspartners. De samenwerkingspartners werden goed geïnformeerd door het OM. 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 bent u op 12 augustus jl. geïnformeerd.⁵

Vraag 7

Acht u het zinvol en noodzakelijk om, naar analogie van de kritische financiële sector, zo snel mogelijk de eis neer te leggen dat bij organisaties met een essentiële rol in de rechtsstaat, zoals het OM, een onafhankelijke risicofunctie wordt belegd, met specifieke focus op cyberveiligheid en integriteitsbescherming?

Antwoord 7

Ik acht het zinvol dat het OM hier op in blijft zetten, vanwege de (digitale) weerbaarheid van deze kritische organisatie binnen de rechtsstaat. Dit vraagt continu aandacht gezien de toenemende dreiging van verschillende actoren. Grotendeels wordt dit vormgegeven door het CIO-stelsel Rijk⁶ en de compliance structuren die daaruit volgen. Voorbeelden hiervan waar het OM

³ Kamerstuk 26 643, nr. 1390, vergaderjaar 2025–2026

⁴ Kamerstuk 26 643, nr. 1378

⁵ Kamerstukken II, 2025–2026, 26 643, nr. 1379.

⁶ Stelsel van Chief Information Officers.

gebruik van maakt zijn de Baseline Informatiebeveiliging Overheid (BIO) en het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI). Zoals ik onder mijn antwoord op vraag 1 ook heb vermeld, zal ik samen met het OM een onderzoek laten uitvoeren naar de ICT-inbreuk. Hiervoor zal een onafhankelijke commissie van nog aan te stellen deskundigen op het gebied van onder meer cybersecurity, IT en informatievoorziening worden ingesteld. Een deel van het onderzoek zal zich richten op het versterken van de weerbaarheid van de IT en informatievoorziening van het OM, mede in relatie tot de ketenorganisaties. Over de planning en resultaten van het onderzoek zal ik u op een later moment verder informeren.

Vraag 8

Bent u bereid de Kamer periodiek en vertrouwelijk te informeren over de stand van zaken, ook als er geen nieuwe incidenten worden ontdekt, om het vertrouwen in de veiligheid van het OM te herstellen en te behouden?

Antwoord 8

Ik informeer de Kamer al regelmatig over de stand van zaken.