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

1599

Vragen van het lid **Faber** (PVV) aan de Staatssecretaris van Justitie en Veiligheid over *hackers hadden vijf maanden toegang tot gegevens DJI-medewerkers* (ingezonden 4 maart 2026).

Antwoord van Staatssecretaris **Van Bruggen** (Justitie en Veiligheid) (ontvangen 13 april 2026). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 1422.

Vraag 1
Bent u bekend met het bericht «Hackers hadden vijf maanden toegang tot gegevens DJI-medewerkers»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat met spoed onderzocht moet worden tot welke gegevens de hackers toegang hebben/hadden?

Antwoord 2
Ja, deze mening deel ik en dit onderzoek wordt momenteel uitgevoerd. Het Nationaal Cyber Security Centrum (NCSC) is op 29 januari jl. door Ivanti op de hoogte gesteld van kwetsbaarheden in Ivanti Endpoint Manager Mobile (EPMM) en doet technisch onderzoek[2]. Ivanti EPMM is een softwareplatform dat door verschillende organisaties wordt gebruikt om mobiele apparaten centraal te beheren en te beveiligen. Uw Kamer is op 27 februari 2026 geïnformeerd omtrent de organisaties die door de kwetsbaarheid in Ivanti EPMM zijn getroffen.[3] De Justitiële ICT Organisatie (JIO), de IT-leverancier van de Dienst Justitiële Inrichtingen (DJI), heeft een extern expertisebureau de opdracht gegeven technisch/forensisch onderzoek uit te voeren. Waar nodig doen zij dit met specialistische adviespartijen.
De uitkomsten van de onderzoeken zijn nog niet bekend. Indien sprake is van relevante ontwikkelingen zal de Kamer worden geïnformeerd.

---

[1] NOS, 28 februari 2026, «Hackers hadden vijf maanden toegang tot gegevens DJI-medewerkers» (https://nos.nl/artikel/2604180-hackers-hadden-vijf-maanden-toegang-tot-gegevens-dji-medewerkers).
[2] Kamerstukken II, 2025–26, 26 643, nr. 1462
[3] Kamerstukken II, 2025–26, 26 643, nr. 1492

ah-tk-20252026-1599
ISSN 0921 - 7398
's-Gravenhage 2026

Vraag 3
Hoe kan het dan zo zijn dat de u aangeeft dat het geen reden is om aan te nemen dat medewerkers onveilig zouden zijn, terwijl ook voormalig gevangenisdirecteur Klaas Brandsma aangeeft dat medewerkers van Dienst Justitiële Inrichtingen (DJI) lopen extra risico op chantage en afpersing?

Antwoord 3
De informatie waar toegang tot is verkregen betreft persoonsgegevens van medewerkers zoals namen, emailadressen, telefoonnummers en locatiegegevens. In algemene zin geldt dat de aard van de werkzaamheden van DJI maakt dat medewerkers mogelijk een aanvullend risico lopen op chantage en afpersing indien dergelijke gegevens bij derden bekend raken. Vanwege dit risico vind ik het dan ook erg belangrijk dat waar nodig veiligheidsmaatregelen zijn getroffen. Dit alles heeft uiteraard impact op de medewerkers van DJI. DJI houdt samen met JIO alsmede met partners uit de keten nauwlettend in de gaten welke eventuele gevolgen de onbevoegde toegang heeft voor de DJI-medewerkers. Daaruit volgt dat er op dit moment geen signalen zijn dat er sprake is van eventuele gevolgen voor de veiligheid van de DJI medewerkers.
Op basis van de voorlopige uitkomsten van het forensisch onderzoek heeft het NCSC een handelingsperspectief opgesteld dat op 16 februari 2026 is gedeeld met DJI. DJI heeft hierop in samenwerking met JIO en NCSC direct maatregelen getroffen die zowel zien op de techniek als op de monitoring van (cyber)dreigingen. Daarover communiceert DJI periodiek naar alle medewerkers. Daarnaast heeft DJI de medewerkers voorzien van een handelingskader, waaronder een oproep tot extra alertheid en instructies hoe om te gaan locatiegegevens.

Vraag 4
Zijn DJI-medewerkers van de Extra Beveiligde Inrichting (EBI) ook getroffen?

Antwoord 4
Zoals in de beantwoording van vraag één is aangegeven, wordt er momenteel onderzoek gedaan naar de precieze omvang van de daadwerkelijke onbevoegde toegang tot devices die draaien op Ivanti. Vanuit het oogpunt van de veiligheid van de medewerkers kan ik niet verder ingaan op welke medewerkers dit onderzoek ziet. Uit voorzorg heeft DJI breed alle medewerkers van een handelingskader voorzien.

Vraag 5
Bent u van mening dat het datalek mogelijk invloed kan hebben op behoud van het huidige personeel en de aanwerving van nieuw personeel? Welke maatregelen gaat u nemen om het getroffen personeel tegemoet te komen?

Antwoord 5
Ik ben me zeer bewust van welke impact deze situatie kan hebben op de medewerkers van DJI. De effecten hiervan op de werving van nieuw personeel zijn onvoorspelbaar. Dergelijke onbevoegd toegang tot systemen heeft impact op medewerkers, met name op hen die al werkzaam zijn voor DJI. Het kan tot vragen leiden over het uitvoeren van de werkzaamheden en mogelijk ook tot gevoelens van onzekerheid, met name over de veiligheid. Daarom is het van belang dat er maatregelen zijn genomen zoals het periodiek informeren van de medewerkers. Ten aanzien van de maatregelen verwijs ik u naar de beantwoording bij vraag drie.

Vraag 6
Welke extra maatregelen gaat u nemen om dergelijke scenario's in de toekomst te voorkomen?

Antwoord 6
De eerste prioriteit ligt bij de veiligheid van de medewerkers en het afronden van het onderzoek. Nadat het onderzoek is afgerond zal een evaluatie en oorzakenanalyse plaatsvinden om te komen tot potentiële verbeteringen.
Ik kan niet vooruitlopen op de uitkomsten van de onderzoeken die op dit moment lopen. Zoals bij de beantwoording van vraag drie is aangegeven houdt DJI samen met partners uit de keten nauwlettend in de gaten welke

eventuele gevolgen de onbevoegde toegang heeft voor de DJI medewerkers. Indien nodig worden aanvullende maatregelen getroffen.