CMT JIO

7 augustus 2025

Samenvatting nieuwe informatie

- Spoor 1: Er zijn geen nieuwe sporen van compromittering gevonden.
- Overleg geweest tussen de CISO van JIO en de CISO van J&V, er is gesproken over de voorwaarden en vorm voor mogelijke afschaling van de crisisorganisatie. Verwachting is dat we komende vrijdag zowel spoor 1 als spoor 2 hebben afgerond en daarmee starten met afschalen van de crisisorganisatie.
- Op spoor 3 wordt zowel de monitoring als het onderzoek parallel gelopen. Plan van aanpak is opgeleverd, opdracht verstrekt.
- Komende week wordt er een toelichting gestuurd naar alle opdrachtgevers met aanvullende duiding op de afschaling van de crisisorganisatie.

Situatie

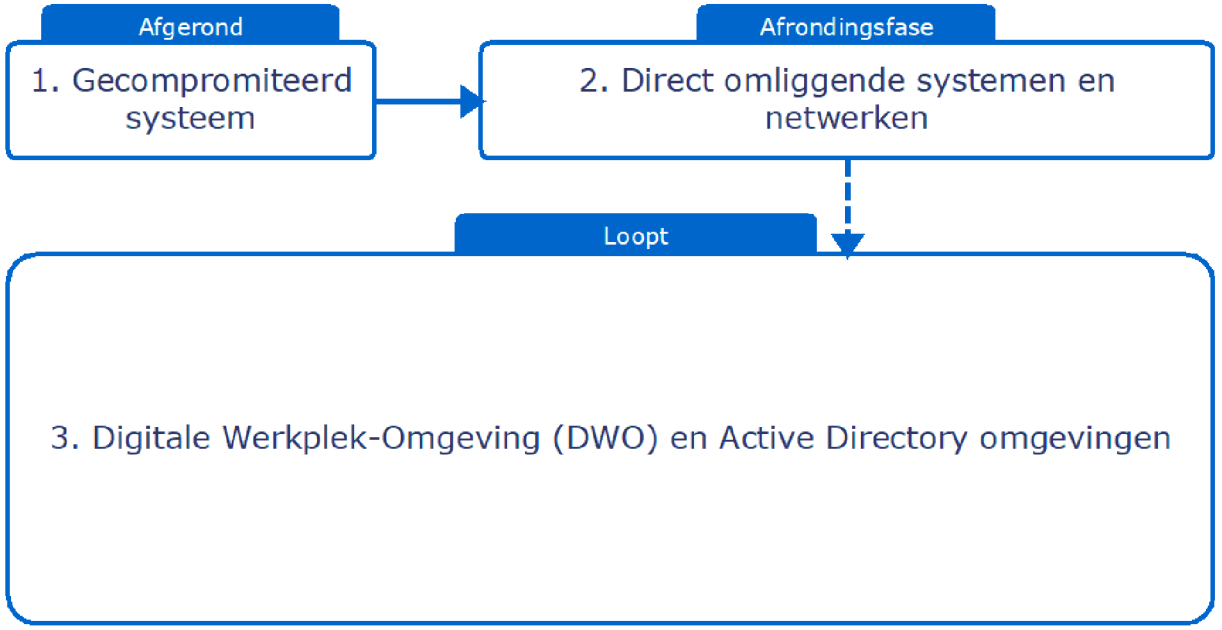
Op 26 mei 2025 om 03:56 UTC heeft een aanvaller middels een toen nog onbekende kwetsbaarheid toegang verkregen tot het voorportaal van het netwerk van JIO, waarmee toegang wordt aangeboden voor de digital werkplek-omgeving (DWO). Deze compromittatie kwam 17 juli aan het licht, waarna de interne crisis processen en een nog lopend incident onderzoek zijn opgestart.

Op basis van de huidige monitoring door JIO en JenV, en de voorlopige uitkomsten van het incident onderzoek zijn er geen signalen van verdere compromittatie waargenomen. Binnen de systemen (achter de firewall) nog geen verdachte activiteiten gevonden. Daarmee kan nog niet uitgesloten worden dat de digitale werkomgeving niet binnengedrongen is.

168346458 0119 0403

Technisch onderzoek

Het technische onderzoek is ingedeeld in een drietal onderzoekssporen. Hierbij is door de omvang van spoor 3 gekozen is voor het starten met spoor 1 en 2 middels het *"follow-the-evidence"* principe om de aanleiding voor het starten van het omvangrijke onderzoek voor spoor 3 goed te kunnen onderbouwen.



168346458 0119 0404

Maatregelen

Preventie

- Patching van inmiddels bekende kwetsbaarheid (uitgevoerd)
- Vernieuwen authenticatie middelen op Citrix Netscalers (uitgevoerd)
- Uitvraag aan opdrachtgevers voor handelingskader en impact bepaling bij een eventuele afsluiting van het internet (loopt, verwachting afronding 08-08-2025)
- Afsluiting DWO omgeving van internet (risico en impact analyse loopt, uitvoering bij directe aanleiding vanuit het technische onderzoek spoor 1 en 2)

Detectie

- 5.1.2h
- GAP analyse van huidige detectie middelen (loopt, wordt afgerond 08-08-2025)
- Beeld buiten eigen omgeving: direct contact met Politie & NCSC (loopt)
- SOC JenV en Solvinity zijn actief betrokken bij het incident en onderdeel van het onderzoeksteam

Respons

- Technisch onderzoek (loopt)
- Gefaseerde wachtwoord-resets in de DJI omgeving is uitgevoerd
- Gefaseerde wachtwoord-reset in de JIO en DTenV omgeving is uitgevoerd

168346458 0119 0405

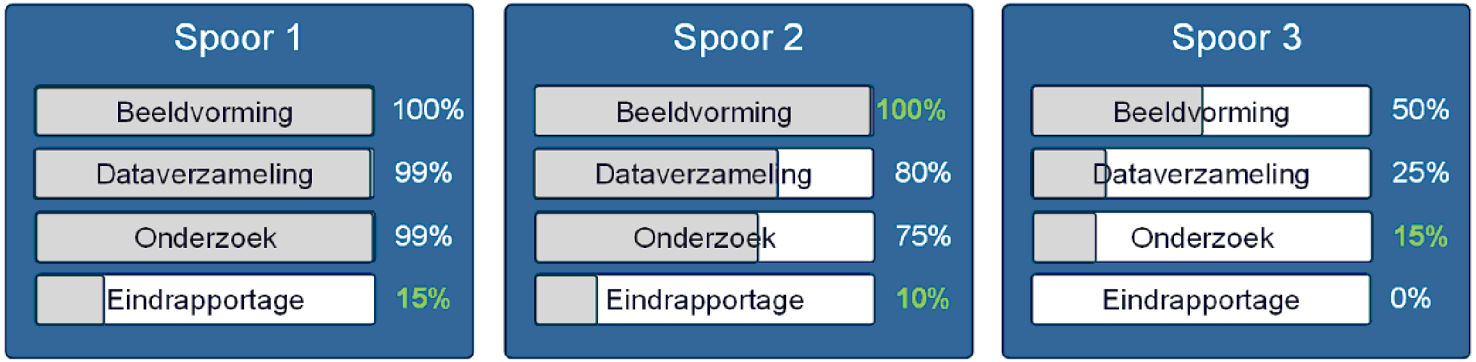
Risico’s

- Het technische onderzoek vindt plaats op basis van het follow-the-evidence principe. Hierbij is het onderzoek afhankelijk van logging en monitoring die niet volledig dekkend is. Hiermee is er een risico voor het missen van belangrijke aanvalssporen door blinde vlekken.
- Het resultaat van de uitgevoerde scans door het pentest team van JIO binnen spoor 2 laat zien dat er vanuit het voorportaal meer rijksonderdelen zichtbaar waren dan intieel verwacht. Solvinity heeft aanvullende maatregelen genomen.
- Toenemende vraag opdrachtgevers naar aanleiding van crisis met prioritering van dienstverlening tot gevolg.

168346458 0119 0406

Indicatie voortgang verschillende sporen

Voor de voortgang op de verschillende onderzoekssporen is hieronder een inschatting gemaakt. Dit is een momentopname van de huidige stand van zaken, uitkomsten van de beeldvorming kunnen de scope van een spoor nog vergroten of verkleinen, met hetzelfde effect op de percentuele voortgang.



168346458 0119 0407