CMT JIO

30 juli 2025

Samenvatting nieuwe informatie

- Afspraken met opdrachtgevers inzake (technische) handelingsperspectieven zijn allemaal ingepland en de eerste conceptuitwerkingen zijn gedeeld.
- Logbronnen vanuit SOC JenV zijn beschikbaar gesteld na toestemming van opdrachtgevers. Vandaag op locatie in Gouda gestart aan een gezamenlijk onderzoek met externe leveranciers (o.a. Solvinity, SOC JenV, SOC JIO) naar de logging vanuit Spoor 2 (omliggende netwerk track) op locatie in Gouda.
  - Output is identificatie te onderzoeken en uit te sluiten systemen

168346466 0124 0436

Situatie

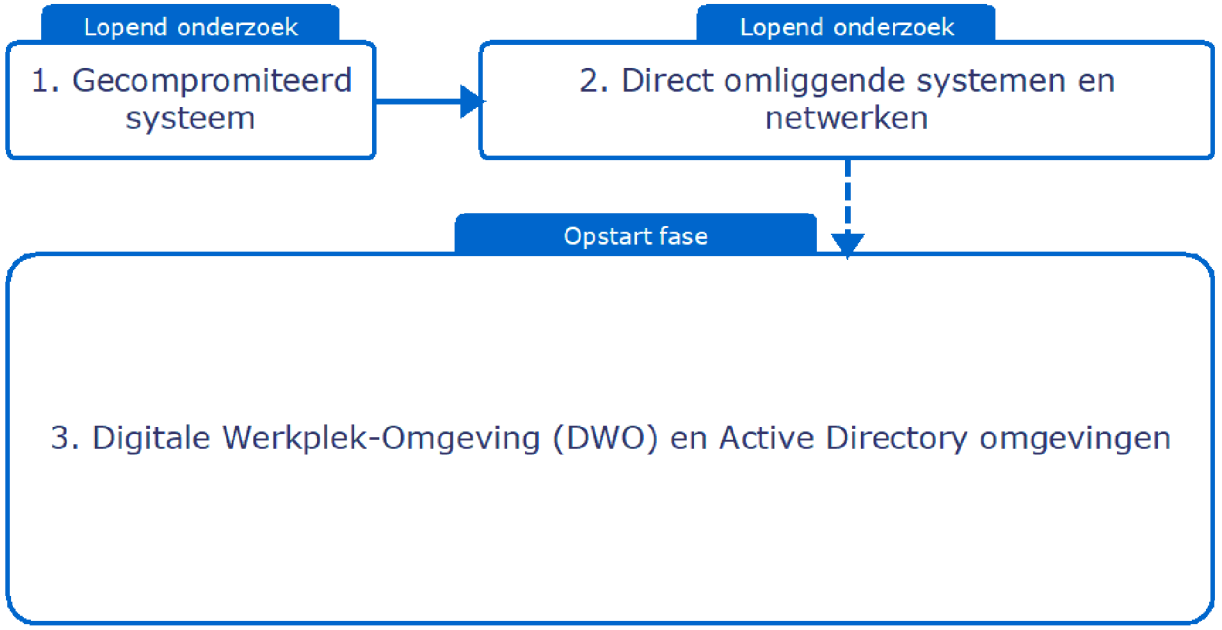
Op 26 mei 2025 om 03:56 UTC heeft een aanvaller middels een toen nog onbekende kwetsbaarheid toegang verkregen tot het voorportaal van het netwerk van JIO, waarmee toegang wordt aangeboden voor de digital werkplek-omgeving (DWO). Deze compromittatie kwam 17 juli aan het licht, waarna de interne crisis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

168346466 0124 0437

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.



168346466 0124 0438

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 input 01-08-2025)
- Afsluiting DWO omgeving van internet (risico en impact analyse loopt, uitvoering bij directe aanleiding vanuit het technische onderzoek spoor 1 en 2)

Detectie

- 5.1.2i
- GAP analyse van huidige detectie middelen (loopt, verwachting 31-07-2025)
- 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 op 26-7 uitgevoerd
- Gefaseerde wachtwoord-reset in de JIO en DTenV omgeving staat gepland op 31-7

168346466 0124 0439

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.
- Gedeelde verantwoordelijkheid tussen JIO en opdrachtgevers onderling voor de systemen en dienstverlening verhoogt de complexiteit in de besluitvorming (zoals het stekkermandaat).
  - In de huidige situatie geeft JIO hierover een advies en de opdrachtgever(s) neemt (in overleg met de eigenaar en de CIO JenV) zelf het besluit hierover.
- Het resutaat van de uitgevoerde scans door het pentest team van JIO binnen spoor 2 laat zien dat er vanuit het voorportaal meer rijksonderdelen zichtbaar zijn dan intieel verwacht. Hier wordt ism Solvinity en externe leveranciers verder onderzoek naar gedaan.

168346466 0124 0440

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.



168346466 0124 0441