**Terugkoppelingen OTC**

## End-of-Day 22-7-2026 16:00 tot 16:30

Aanwezigen: 5.1.2e 5.1.2f 5.1.2e 5.1.2f 5.1.2e 5.1.2f 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e en 5.1.2e 5.1.2e

**Voorlopige bevindingen**

- 26 mei gestart.
- 7 juli heeft Citrix informatie gegeven; daarin werd de backdoor genoemd.
- 8 juli zijn er mitigerende maatregelen genomen: patches, afgesloten sessies e.d.. Hierin had SOC betrokken moeten zijn en een fullblow incident response moeten plaatsvinden.

**Schematische weergave aanval**

Er zijn drie onderzoektracks bepaald:

1. Netscaler: sporen die we daar vinden, hopelijk concluderen 5.1.2e er ingebroken is.
2. Omliggende netwerk: het spoor van de 5.1.2e VLAN's: 5.1.2h 5.1.2h
3. DWO/AD: levert grotere scope en onderzoeksvragen op. Onderzoek duurt dan langer.

*Netscaler:*

- Backups 5.1.2e sturen aan 5.1.2f
- Ontvangen kopie AP en SF → 5.1.2e scan gedaan op file (staat daar iets malafide) geen bevindingen. Voorzichtige conclusies, er is niets geraakt, maar dubbel check met de back-ups.
- Firewall logs niet dekkend. Verbindingen die verwacht worden zijn er niet. Wordt er iets in de opslagketen weggefilterd? Hopelijk komen deze bovenwater. 5.1.2e van deze logs liggen bij SOC J&V en Solvinity.

--> Indien we niets zien kan dit betekenen: er is niets gebeurd of we weten het niet, er is nog een kans.

*Omliggend netwerk:*

- Pentesten JIO.
- Morgen hopelijk meer informatie over de planning/het tijdpad.

*DWO/AD*: wacht op bevindingen uit voorgaande tracks. Bij indicatie doorgaan van aanval of onvoldoende beeld.

- Toegang tot SIEM.
- Uitbreiden toezicht: 5.1.2h aanbrengen op dat wat niet in de scope is van de monitoring, om een beter gevoel te krijgen dat er niets aan de hand is.
- 5.1.2h onderzoeken. Hoeveel antivirus-meldingen gaan af op de omgeving.

**Overige punten**

- Betrokkenheid J&V, **zie actie 5.1.2e om SOC J&V te laten aansluiten bij Stand-up.** Indien meer externen bijgepraat moeten worden, staat 5.1.2f open voor een extra Stand-up met deze partijen.
- Onsite vertegenwoordiging is vanuit 5.1.2f als prettig ervaren. Dit gaat de hele week door.
- Weekend inzet: tijdig weten ook i.v.m. de planning → 5.1.2e **neemt dit mee naar het overall crisismanagement.**
- Budget: eind van de week is het budget op. Het is moeilijk in te schatten 5.1.2e we dan zijn. Forecast is niet te doen. → 5.1.2e 5.1.2e **neemt deze informatie mee naar het crisismanagement overleg.**

Vragen

- 5.1.2h 5.1.2h 5.1.2h ) wordt gepusht naar het SIEM. Dit kan deze week aangezet worden. 22 eventlogging is aangeleverd en wordt gecontroleerd op nut voor SIEM. 5.1.2e 5.1.2e gaat met 5.1.2f bespreken wat hiermee gedaan kan worden en of Detectielogica goed is ingeregeld, het SIEM moet aanslaan op bepaalde event.
- 5.1.2e **initiatief contact** 5.1.2e **wat kan** 5.1.2h **wel en niet, wat zou dit betekenen voor** 5.1.2h **Morgenochtend na standup.**
- Agents 5.1.2f wordt bedoeld realtime toezicht met 5.1.2h en 5.1.2h
- Wat zijn wensen van opdrachtgevers als vervolg? Er is voor DJI een wensen (kroonjuwelen) en handelinsperspectieven in concept. Is hiervoor een hulpvraag vanuit JIO aan 5.1.2f om te helpen informeren en aan zaken als threatmodeling te doen. Er is behoefte aan een handelingsperspectief bij verschillende scenario's. Bijv. ontkoppelen 5.1.2h → 5.1.2e **neemt dit aanbod mee naar het Crisismanagement overleg.**
- Agents van 5.1.2f uitrollen: de software is plug n play, uitrol via script. Kunnen we hiervoor een offerte krijgen om het rechtmatig in te kopen? De werkzaamheden nu zijn "onrechtmatig" ingekocht. In principe is de agents als onderdeel van de huidige dienst. 5.1.2e **koppelt dit wel terug aan de accountmanager.**

| Actiehouder | Actie | Nr |
|---|---|---|
| 5.1.2e 5.1.2e | 5.1.2e 5.1.2e & 5.1.2e 5.1.2e sluiten bij het operationeel crisisteam als Secretaris OCT | 1 |
| 5.1.2e 5.1.2e | Elke punt vanuit de actielijst is besproken met het operationeel crisisteam en de status is hiervoor bijgewerkt. | 2 |
| 5.1.2e 5.1.2e | SOC J&V wordt uitgenodigd voor aansluiting bij Stand-up. | 3 |
| 5.1.2e 5.1.2e | Er moeten techneuten komen op Opdrachtgevers vragen te beantwoorden. | 4 |
| 5.1.2e 5.1.2e | Budget is op, in crisismanagementovereleg bespreken hoe verder te gaan. | 5 |
| 5.1.2e 5.1.2e | Weekend inzet bespreken in crisismanagementoverleg. | 6 |
| 5.1.2e 5.1.2e | Bespreken of het aanbod van 5.1.2f om te ondersteunnen in communicatie op hoger (politiek) niveau gewenst is. | 7 |
| 5.1.2e 5.1.2e | Na de Stand Up van 23 juli wordt er contact opgenomen met 5.1.2e 5.1.2e om te bespreken wat 5.1.2h als agent allemaal kan. | 8 |
| 5.1.2e 5.1.2e | Terugkoppelen aan accountmanager dat er offertes | 9 |

**Voorlopige namenlijst deelnemers BVZ 23-07-2025 13:35**

5.1.2e 5.1.2e frontoffice
5.1.2e 5.1.2e (Tactisch beheer / telefonie)
5.1.2e 5.1.2e 5.1.2e 5.1.2e (webproxy, internetverkeer naar buiten)
5.1.2e 5.1.2e (DWO en endpoints)
5.1.2e 5.1.2e (DWO)
5.1.2e 5.1.2e (consultant endpoints)
5.1.2e 5.1.2e 5.1.2e (consultant DWO applicaties) volgende week terug van vakantie
5.1.2e 5.1.2e (platformen Windows)
5.1.2e 5.1.2e 5.1.2e AD specialist kennisdrager omgevingen
5.1.2e (architect kennisdrager probeer ik nog te bellen (vakantie).
5.1.2e 5.1.2e (netwerken)
5.1.2e 5.1.2e en of ondergetekende.

## End-of-Day 22-7-2026 16:00 tot 16:30

Aanwezigen: 5.1.2e 5.1.2f 5.1.2e 5.1.2f 5.1.2e 5.1.2f 5.1.2e 5.1.2e en 5.1.2e 5.1.2e

**Voorlopige bevindingen**

• De initieële toegang vond mogelijk plaats rond 26 mei 2025 03:56 UTC.
Periode 26 mei –7 juli 2025 (43 dagen/6 weken) – Track 1 en 2
Periode 26 mei – heden (57 dagen/8 weken ) – Track 2 en 3

**Onderzoeksaanpak: Netscaler-track**

Netscaler-track: Verder onderzoek op gecompromitteerd systeem en vergelijkbare

**Onderzoeksaanpak: Omliggende netwerk track**

Omliggende netwerk track: Onderzoek van direct omliggende systemen die een aanvaller had kunnen aanvallen (binnenkant, beheerkant en buitenkant)
Huidige status:
• Beeldvorming vorderd goed. Onderzoek in

**Onderzoeksaanpak: DWO/AD track**

DWO/AD track: Onderzoek op de digitale werkplek-omgeving die de aanvaller mogelijk had kunnen overnemen (DWO)
Huidige status:

**Overige punten:**

Samenwerking met het NCSC en de Politie is opgestart. Kostte 5.1.2f relatief veel tijd vandaag. Budget en weekend inzet moet besproken worden in het crisismanagementoverleg om 17:00

Uit de gesprekken tussen 5.1.2f en het OM blijkt dat

5.1.2f

Er wordt momenteel een scan uitgevoerd op de 5.1.2h VLAN's onder de hoofd netscaler 5.1.2h 5.1.2h Scan duurt onverwacht erg lang, probleem wordt besproken met Solvinity. Naast deze scan moet ook de koppelingen met deze systemen onderzocht worden.

Budget en inzet weekend moeten besproken worden. Verwachting 2e ronde budget moet besproken worden in het overleg om 17:00. Als alle severs onderzocht moeten worden zal de 2e ronde niet afdoende zijn.