# Afschalen Netscaler Crisis

## Maatregelen en risico's

7 augustus 2025

# Algemeen en Advies

tav afschalen van de crisisorganisatie zijn twee zaken met name van belang:
1. komt er niets uit de forensische analyse van spoor 1 en 2 (eind deze week afgerond)
2. is monitoring en detectie nu voldoende in place zodat wij mogelijke aanvallen of verdachte handeling kunnen waarnemen en hierop snel kunnen acteren

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 mitigeren van bestaande kwetsbaarheden is inmiddels afgerond en zorgt voor dekking op het gebied van logging en monitoring (SIEM aansluiting), dichtzetten van configuratiefouten en aanvullen van firewall logging.

**Op basis van het wegnemen van kwetsbaarheden, geen signaal van compromittering van het voorportaal en het ontbreken van verdacht verkeer, gekoppeld aan alle mitigerende maatregelen schatten we het risicoprofiel niet meer op crisisniveau in en ons voorstel is om de crisis per vrijdag 08-08-2025 af te schalen**.

# Sporen & scenario's

Spoor 1: Voorportaal gecompromitteerd

Spoor 2: Omliggende systemen en netwerken van het gecompromitteerde systeem

Spoor 3: Onderzoek Digitale Werk Omgeving (DWO)

5 scenario's zijn uitgewerkt om "afsluiten internet" nader te duiden (*Hierin zijn ook combinaties mogelijk)*

- Het inkomende internetverkeer richting de Connect dienst wordt beperkt
- Het inkomende internetverkeer richting de Connect dienst wordt volledig afgesloten
- Uitgaand internetverkeer wordt beperkt
- Uitgaand internet wordt volledig afgesloten
- Volledige quarantaine



168346305 0003 0015

# Mitigerende maatregelen Spoor 1: *Voorportaal gecompromitteerd*

Maatregelen uitgevoerd:

- Patching van inmiddels bekende kwetsbaarheid
- Vernieuwen authenticatie middelen op Citrix Netscalers
- Crash dumps kwetsbaarheid onderzocht (Citrix en externe partij)
- Indicators of compromise (IOC) toegepast, nieuwe IOC's vanuit contact NCSC, Politie en SOC J&V worden wanneer van toepassing toegepast
- Uitbreiden van detectiemaatregelen: EDR & Logging aan het SIEM

Bovenstaande maatregelen en forensisch onderzoek hebben geen verdere aanvalssporen of andere bevindingen opgeleverd

*Status: spoor 1 afgerond, wanneer nieuwe onderzoeksdata daar aanleiding toe geven wordt dit spoor weer onderzocht*



168346305 0003 0016

# Mitigerende maatregelen Spoor 2: *Omliggende systemen en netwerken van het gecompromitteerde systeem*

Maatregelen en status:

- 5.1.2i
- SOC JenV en Solvinity zijn actief betrokken bij het incident en onderdeel van het onderzoeksteam
- PEN test voorportaal door PEN testers JIO
- In overleg met Solvinity zijn mitigerende maatregelen getroffen binnen het voorportaal
- Gefaseerde wachtwoord-resets in de DJI omgeving is uitgevoerd
- Gefaseerde wachtwoord-reset in de JIO en DTenV omgeving is uitgevoerd
- Uitvraag aan opdrachtgevers voor handelingskader en impact bepaling bij een eventuele afsluiting van het internet

Status spoor 2: De omliggende systemen en netwerken vanuit de PEN test adviezen zijn aangepast en staan onder monitoring. We realiseren ons dat de logdata uit het verleden niet compleet dekkend is.



168346305 0003 0017

# Mitigerende maatregelen Spoor 3: Onderzoek Digitale Werk Omgeving (DWO)

Maatregelen en status:

- 5.1.2i
- 5.1.2h data onderzoek vanaf februari tot heden
  - Log data beschikbaar vanaf februari waardoor verkeersstromen binnen de DWO vóór de aanval kunnen worden gezien alsmede tijdens en na
  - Hiermee kan een baseline van verkeersstromen worden vastgesteld en eventuele afwijkingen worden gevonden in de log data

Status spoor 3: beeldvorming en dataverzameling in progress, nog niet afgerond en diepgaand data onderzoek nog niet gestart.



168346305 0003 0018

# Afschalen crisisorganisatie naar Projectorganisatie met hoge prioriteit






168346305 0003 0019

# Vervolg, parallel aan spoor 3

Spoor 3 heeft met name betrekking op (forensisch) onderzoek op de DWO omgeving. Daarnaast zijn er nog verschillende acties die binnen de projectorganisatie met verhoogde prioriteit worden uitvoerd:

1. Uitwerken van de handelingsperspectieven (samen met Opdrachtgevers)
2. Uitwerken van Business Continuity Plannen (BCP). Dit doet iedere organisatie zelf.
3. Password resets (op aangeven van Opdrachtgever)

Ook zijn er lopende acties die gereapporteerd worden via het actieplan, waaronder:

1. Verdere verbetering van detectie, logging en monitoring
2. Oplossen van eerdere Pentest bevindingen van begin dit jaar

Communicatie en rapportage:

Dit loopt zoveel mogelijk via de reguliere overleg en rapportagestructuren:

- Bestuurlijk overleg JIO met pSG
- Opdrachtgeversoverleg JIO – Opdrachtgevers
- CISO overleg JenV en CISO overleg JIO - Opdrachtgevers



168346305 0003 0020