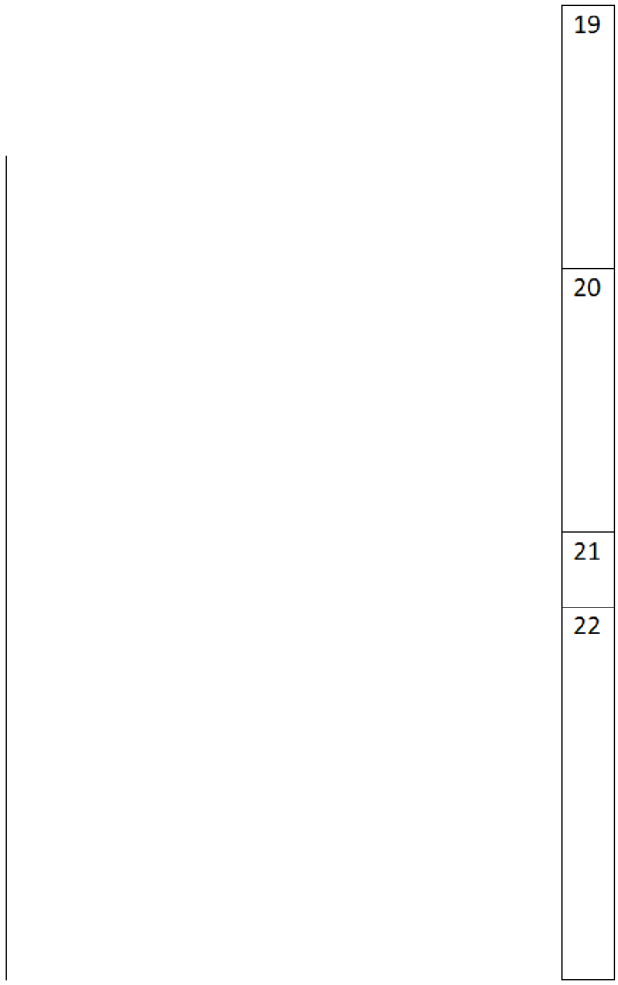
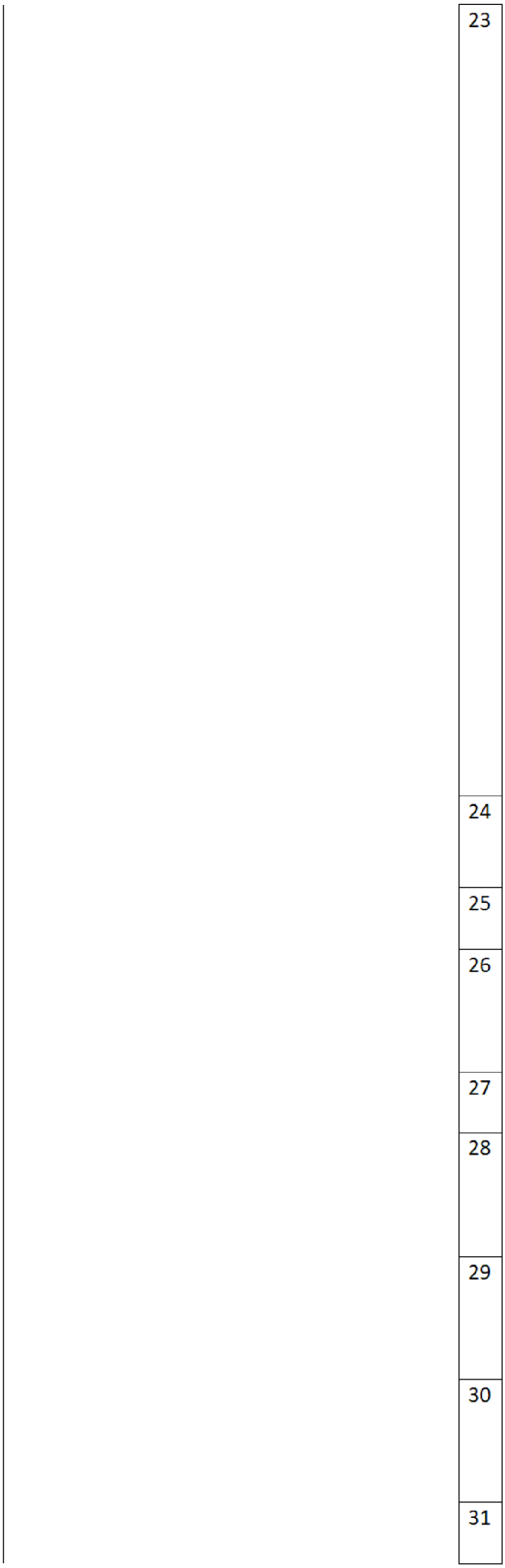
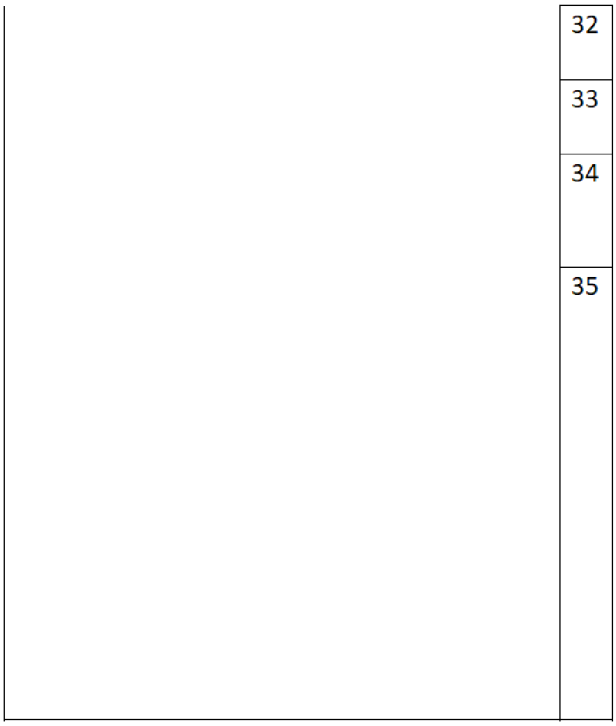
Bron	
CISO DT&V - 21-08-2025	1
	2
	3
	4
	5
	6
	7
	8
	9
	10
AP - wo 8-10-2025 16:17	12
	13
	14
	15
	16
	17
	18


19
20
21
22


23
24
25
26
27
28
29
30
31


32
33
34
35

Vraag
Welke beheerprocessen (instellingen zoals load balancing rules, content switching policies of authentication-methodes worden gewijzigd zonder logische verklaring of zonder dat een beheerder dit heeft aangepast), **beheeractiviteiten** (zoals verhoogde CPU-belasting- of geheugenbelasting) **en dataverkeer** (communicatie via ongebruikelijke poorten) **worden in de DMZ door JIO gelogd?**
Zijn infrastructurele loggings in de logbestanden aanwezig?
Welke infrastructurele loggings zijn plotseling afwezig in de logbestanden / logboeken? (logbestanden zijn incompleet, missen cruciale gegevens of tonen onrealistische inlogtijdstippen)
Vanaf welke datum kan JIO garanderen dat de back-up van ons primair processysteem ISTV en BO 100% volledig is?
Vanaf welke datum kan JIO garanderen dat de back-up van ons e-mail-omgeving 100% volledig is?
Vanaf welke datum kan JIO garanderen dat de back-up van ons DWO Productie-omgeving 100% volledig is?
Wanneer is de laatste back-up en restore test in relatie tot dienstverlening DTenV geweest en wat was het resultaat?
Rapportage Spoor 1: Gecompromitteerd systeem, wanneer is de verwachting dat deze met DTenV wordt gedeeld?
Rapportage Spoor 2: Direct omliggende sysrtemen en netwerken, wanneer is de verwachting dat deze met DTenV wordt gedeeld?
Rapportage Spoor 3: DWO en AD-omgevingen DTenV en DJI en JIO, wanneer is de verwachting dat deze met DTenV wordt gedeeld?
Op 7 juli bevestigt Citrix dat de Netscalers gecompromitteerd zijn. Het heeft tot 17 juli geduurd voordat er een expertiseteam is ingehuurd (5.1.2f) en tot 20 juli voordat het onderzoeksproces daadwerkelijk is gestart. Wat is de reden voor deze vertraging? Heeft JIO de potentiële risico's onderschat?
In de introductie van het rapport wordt de AP genoemd, maar er wordt nergens in het rapport naar de specifieke situatie van de AP verwezen. Zo is het bekend dat er verbindingen zijn opgezet richting de systemen (netscalers) van de AP. Wat is hier het gevolg van geweest?
Pagina 8 - alinea 4: JIO geeft aan dat de Netscalers direct gepatcht zijn bij het vrijgeven van de patches door Citrix. Is dit een geautomatiseerd of handmatig proces geweest? Is hier bewijsmateriaal van opgeleverd?
Pagina 9 - alinea 1: 5.1.2f geeft aan dat er geen sluitend advies te geven is over het offline halen van de services. JIO kiest ervoor om de services niet te onderbreken. Op basis waarvan is dit gebeurd?
Pagina 9 - alinea 1: Overkoepelende vraag voor het hele onderzoekstraject: Is er een besluitenlijst opgesteld waarin wordt geduid of en waarom adviezen van opdrachtgevers, 5.1.2f en partijen als Citrix zijn opgevolgd of juist niet zijn opgevolgd inclusief de overweging?
Pagina 12 - 2.1.2. - alinea 4: Gedurende het incident is additionele toegang verkregen tot informatie binnen het SIEM van het SOC van JenV voor zowel 5.1.2f als het SOC van JIO. Hoelang blijft deze toegang nog bestaan of is die inmiddels verwijderd?
Pagina 15 - alinea 1 / 5: Een herhaaldelijke conclusie van 5.1.2f in het rapport is dat er te weinig bewijsmateriaal werd of wordt verzameld binnen de gehele infrastructuur. Is dit het resultaat van een risico-afweging door JIO? Zo ja, wat is deze risicoafweging geweest? Zo nee, wat is de reden dat dit risico aan de aandacht van JIO is ontsnapt?

Pagina 16 - alinea 6: 5.1.2f heeft Opdrachtgever vanaf begin bewust gemaakt van de mogelijke noodzaak tot uitvoeren van een onderzoek op een groot deel van het interne netwerk. Reden hiervoor is dat dit onderzoek (project Neva) mogelijk onvoldoende antwoord kan geven in verband met onderzoeksbeperkingen. Welke afweging heeft JIO gemaakt om niet direct / simultaan te starten met een spoor 3 onderzoek, als 5.1.2f vanaf de start van het project al duidelijk heeft gemaakt dat er zeer waarschijnlijk geen resultaten zouden volgen uit onderzoeksspoor 1 en 2. Hiermee is potentieel kostbare tijd verloren gegaan.
Pagina 17 - alinea 3: 5.1.2f geeft aan dat er dringend zaken verbeterd moeten worden (spoed-verbetertraject). Wat is de afweging geweest van JIO om 5.1.2f niet bij dit verbetertraject te betrekken om dit traject te bespoedigen? Bij schrijven zijn nog (steeds) niet alle systemen onder monitoring en is de effectiviteit hiervan voor zover de AP weet niet getest. En wat is de status nu van die verbeteringen.
Pagina 18 - tabel 1: Data in de tabel kloppen niet. De firmwareversies zijn respectievelijk 25 juni en 17 juli beschikbaar gemaakt door Citrix.
Pagina 19 - tabel 3: Zijn de alle genoemde maatregelen uitgevoerd én getest en daarmee afgerond?

Pagina 21 en 22: Er zijn non-conformiteiten ontdekt door 5.1.2f. De AP verwacht van JIO een verklaring van deze non-conformities inclusief een mitigatieplanning en -rapport.
Pagina 23 - figuur 2: In dit schema is duidelijk dat de DTV Netscalers ook verbindingen heeft op kunnen zetten met 'andere deelnemers die gebruik maken van 5.1.2h. Wat is het potentiële gevolg voor deze 'deelnemers'? Waar in deze afbeelding bevindt de AP zich en wat zijn de gevolgen voor de AP?
Pagina 24 - tabel 5: Data in de tabel kloppen niet. De firmwareversies zijn respectievelijk 25 juni en 17 juli beschikbaar gemaakt door Citrix.
Pagina 25 - alinea 2: De systeemuitval is gecategoriseerd als technische storing. Is het ontbreken van monitoring hier cruciaal geweest?
Pagina 27 - alinea 3: Het is best-practice om op alle configuratiebestanden detectie van wijzigingen geïmplementeerd te hebben. Is dit het geval geweest? En zo niet, wat is hierbij de risicoafweging geweest?
Pagina 29 - alinea 4: *Het advies van Citrix om een onderzoek in te stellen, of om een intern of extern securityteam te betrekken, lijkt niet direct te zijn opgevolgd. Toen* 5.1.2f *gecontacteerd werd op zaterdag 19 juli 2025 was het securityteam van Opdrachtgever sinds 17 juli 2025 op de hoogte van de compromittatie.* Graag een verklaring van JIO.
Pagina 31 - alinea 5: Wat zijn de verantwoordelijkheden en plichten van JIO en Solvinity voor de juiste configuratie van de DMZ? Wie controleert wie?
Pagina 36 - alinea 2: Wat betekent een maximale risicoscore van 5.1.2h Zijn er verbetermaatregelen doorgevoerd en zo ja, welke? En geldt dit ook voor de AP?
Pagina 36 - alinea 3: 5.1.2f merkt op dat het ontbreekt aan een gelaagde beveiliging. Wat is het verbeterplan van JIO? En wat is de planning?

Pagina 36 - alinea 4: Er wordt gesproken over EoL-versies. Maakt de AP ook gebruik van EoL-producten? Wat is het verbeterplan en -planning hiervoor?
Pagina 36 - alinea 4: 5.1.2f geeft aan dat er sprake is van mogelijke compommitering van sessies, wat zijn de gevolgen hiervan? Wat betekent dit voor de opdrachtgevers?
Pagina 36 - alinea 6: 5.1.2f wijst op mogelijke 5.1.2h die kan leiden tot privilege escalatie. Is deze situatie opgelost? Zo niet, wat is het verbeterplan en de -planning?
Pagina 38 - statement: *Daarnaast acht* 5.1.2f *de kans zeer aannemelijk dat de aanvaller met de verkregen toegang op de NetScalers ook de sessies van actieve gebruikers kon overnemen. Zodoende acht* 5.1.2f *het zeer aannemelijk dat alle sessies van gebruikersaccounts tussen 26 mei en 7 juli 2025 een risico hebben gelopen op overname door de aanvaller.* Dit is voor de AP nieuwe informatie en werpt de vraag op of de schorsing van services ten onrechte is afgewezen door JIO. Wat is het standpunt van JIO hierin? En van 5.1.2f 5.1.2? Wat zijn de implicaties van deze mogelijke sessiehijacking? Geldt dit scenario potentieel ook voor de AP?

De DMZ wordt beheerd door Solvinity en wij hebben geen toegang tot infrastructurele logging binnen de DMZ. Wij hebben wel toegang tot 5.1.2h en daarmee zicht op de firewalls in de DMZ, we hebben applicatieve logging van de applicaties die in de DMZ staan en de Netscalers zijn sinds deze zomer aangesloten op logging (SIEM).
Ja, in onze eigen omgeving zijn logbestanden beschikbaar met dataverkeer en routering.
Ja, ten tijde van deze problematiek ontbraken er loggegevens door het ontbreken van een aansluiting van onze Netscalers op het SIEM of door het uitgeschakeld zijn van logging. Sindsdien deze zomer zijn de Netscalers aangesloten op het SIEM en is de logging compleet.
De back-up van de data wordt conform de afspraken in de NOK uitgevoerd.
De back-up van de e-mail data wordt conform de afspraken in de NOK uitgevoerd
5.1.2h
Voor DTenV is geen hersteltest uitgevoerd. Met het klantenteam kan een afspraak gemaakt worden voor het gezamenlijk uitvoeren van een restore-test.
De rapportage spoor 1 is opgenomen in het Neva rapport van 5.1.2f en is eerder verspreid.
De rapportage spoor 2 is opgenomen in het Neva rapport van 5.1.2f en is eerder verspreid.
De rapportage spoor 3 is opgenomen in het Neva rapport van 5.1.2f en is eerder verspreid.
Op 7 juli kregen wij advies van Citrix. Vanaf diezelfde dag is ons SOC betrokken bij de aanpak. In de dagen na 7 juli zijn in overleg met Citrix diverse aanvullende maatregelen genomen zoals verwoord op pagina 18/19 van het rapport van 5.1.2f.
De omgeving van de getroffen Netscaler is onderzocht. Er zijn pogingen ondernomen om verbindingen op te starten met de Netscaler van AP. Deze is verder onderzocht, maar er zijn geen sporen aangetroffen op de Netscaler van de AP.
Wij hebben een tool waarmee wij de Citrix omgeving patchen. Deze tool starten wij handmatig, de patch wordt vervolgens automatisch uitgevoerd.
Het uitschakelen/afschakelen van kroonjuweelsystemen heeft een grote impact op de continuïteit van de bedrijfsvoering van onze opdrachtgevers. Vanwege de koppelingen tussen diverse andere systemen zou deze impact vele malen groter zijn voor de hele JenV keten. Een besluit of een systeem uit te schakelen moet in het bredere perspectief op JenV niveau genomen moeten worden. Wij waren hier over in gesprek met de CIO JenV.
Na het intern activeren van de crisisstructuur zijn besluiten in logboeken opgenomen. Als lessons learned uit deze crisis nemen wij mee dat we bij het activeren van de crisisstructuur met terugwerkende kracht de logboeken aan te vullen met de besluiten die hieraan voorafgaand zijn genomen.
Deze accounts, en dus de toegang, zijn verwijderd na afronding van het onderzoek Neva.
De Netscalers waren niet aangesloten op het SIEM. De retentie van de lokale Netscalers heeft te maken met de beperkte opslagmogelijkheden op de lokale Netscaler. Inmiddels wordt de logdata van alle Netscalers naar het SIEM gestuurd. Deze waren niet eerder aan het SIEM toegevoegd door een tekort aan opslag / capaciteit. Deze is inmiddels uitgebreid.

5.1.2f heeft geadviseerd om niet meteen spoor 3 op te starten omdat eerst spoor 1 moest worden onderzocht. Wij hebben in deze het advies van 5.1.2f gevolgd.
Wij hebben naar aanleiding van het 5.1.2f onderzoek diverse verbeteringen, conform de adviezen, onder hoge druk uitgevoerd. Het betrekken van 5.1.2f hierbij had niet tot een snellere oplossing geleid, omdat de werkzaamheden uitgevoerd worden door onze eigen interne medewerkers. We hebben de expertise van 5.1.2f gevraagd bij het vervolg traject LoMe. De aansluiting van systemen op het SIEM is nog niet afgerond, mede door de hiervoor benodigde uitbreiding van de hardware. De effectiviteit zal in 2026 door middel van een pentest en red teaming test worden beproefd.
Deze data zijn door 5.1.2f aangepast in het rapport (versie 1.1).
1) Opdrachtgever start gefaseerd met de wachtwoordwijziging voor gebruikers van het 5.1.2h 5.1.2h : dit is uitgevoerd
5.1.2h
3) Opdrachtgever neemt de NetScaler logdata op in het SIEM: dit is uitgevoerd.
4) Opdrachtgever deelt handelingsperspectief met deelnemers en start inventarisatie van gewenste mitigerende acties: dit is uitgevoerd.
5) Opdrachtgever en Solvinity (leverancier 5.1.2h) hebben een 5.1.2h configuratie aangepast: dit is uitgevoerd.

1. De Netscaler logdata was niet aanwezig in het SIEM, dit is inmiddels wel aanwezig.

5.1.2h

3. Deze kwetsbaarheid is door onze pentesters zichtbaar gemaakt. Vervolgens heeft Solvinity dit aangepast.
4. Er zijn betere werkafspraken gemaakt tussen SOC JIO en SOC JenV.
5. Hierbij geldt hetzelfde als bij punt 1 - het gaat hier om de interne Netscalers.
6. Momenteel wordt nog onderzocht om de 5.1.2h toe te voegen aan het SIEM. Wat hier in meespeelt is de omvang van deze dataset.
7. Het is niet mogelijk om in de logging een verschil te zien tussen een bedrijfssysteem en een BYOD-device. Dit kan alleen opgelost worden door in het beleid BYOD uit te sluiten - dit heeft echter een grote impact.
8. Zie hetzelfde antwoord voor punt 1.
9. Het opnieuw inspoelen is één van de maatregelen om ervoor te zorgen dat een aanvaller geen persistentie kan creeëren op het systeem. Het draagt daarmee bij aan een veilig systeem. Het nadeel is dat hiermee ook dat eventuele sporen van aanvallers verwijderd worden. Het opnieuw inspoelen van de systemen, wordt gezien als goede maatregel ondanks de onderzoeksbeperking.

5.1.2h

11. Zie het antwoord voor punt 10.
12. Dit punt is inmiddels verbeterd, door de uitrol van 5.1.2h op alle OS-en.
13. Zie het antwoord voor punt 7.

De Netscalers van AP zijn onderzocht en er zijn geen sporen aangetroffen, daarmee zijn er ook geen gevolgen.

Deze data zijn door 5.1.2f aangepast in het rapport (versie 1.1).

De instabiliteit van de Netscalers zijn initieel beoordeeld als een technische storing, waarbij hulp en ondersteuning van de leverancier is gevraagd. Omdat het om een zero-day kwetsbaarheid ging was de leverancier niet op de hoogte van een kwetsbaarheid. Het ontbreken van monitoring heeft geen invloed op gehad.

Nee dit was ten tijde van de crisis niet geïmplementeerd, maar inmiddels wel.

Op 7 juli krijgen wij het advies/comprommitatie melding van Citrix. Vanaf diezelfde dag is ons SOC betrokken bij het probleem. In de dagen na 7 juli zijn in overleg met Citrix diverse aanvullende maatregelen genomen zoals verwoord op pagina 18/19 van het rapport.

Onze internetverbindingen (5.1.2h) en de " 5.1.2h " zijn in beheer bij Solvinity. JenV/DI&I is de opdrachtgever. Als wij wijzigingen willen doorvoeren dan vragen wij die aan bij Solvinity, deze aanvragen worden zowel bij ons als bij Solvinity gecontroleerd. Alle betrokken partijen kunnen wijzigingen voorstellen aan hun eigen systemen.

5.1.2h 5.1.2h 5.1.2h

5.1.2h 5.1.2h

5.1.2h

5.1.2h

Nee.

Op de Netscalers van AP zijn geen sporen van compromitatie aangetroffen. Voor DTenV, DJI en JIO heeft is er een wachtwoordreset bij alle gebruikers uitgevoerd.

5.1.2h

Dit scenario geldt niet voor AP. De Netscalers van AP waren niet gecompromiteerd.

Wij hebben naar aanleiding van de adviezen, de gebruikers van de organisatie afgedwongen de wachtwoorden te wijzigen. Voor DJI zijn de wachtwoorden na 25 juli gefaseerd gereset, voor DTenV zijn de wachtwoorden op 31 juli gefaseerd gereset en voor JIO zijn de wachtwoorden op 31 juli 2025 om 13:00 uur gereset.

Het uitschakelen/afschakelen van kroonjuweelsystemen heeft een grote impact op de continuïteit van de bedrijfsvoering van onze opdrachtgevers. Vanwege de koppelingen tussen diverse andere systemen zou deze impact vele malen groter zijn voor de hele JenV keten. Een besluit of een systeem uit te schakelen moet in het bredere perspectief op JenV niveau genomen moeten worden. Wij waren hier over in gesprek met de CIO JenV.