verslags toelichting rapport Neva

Omschrijving	toelichting rapport Neva spoor 1,2 en 3 door 5.1.2f m.b.t. Citrix Netscaler incident
Vergaderdatum en -tijd	9 oktober 2025, 10:00 uur
Vergaderplaats	Gouda
Aanwezig	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 5.1.2e 5.1.2e , 5.1.2e 5.1.2e 5.1.2e , 5.1.2e 5. 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 (5.1.2f), 5.1.2e 5.1.2e (5.1.2f), 5.1.2e 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 , 5.1.2e 5.1.2e 5.1.2e , 5.1.2e 5.1.2e

Justitiële ICT Organisatie
Strategie en Bedrijfsvoering,
Bestuur en Strategie
IB&P

Contactpersoon
5.1.2e
5.1.2e

Datum
9 oktober 2025

Notulist
5.1.2e .1.2e 5.1.2e

5.1.2e en 5.1.2e openen het overleg.

5.1.2f geeft een toelichting op het eindrapport van het onderzoek naar de compromitatie van de citrix netscaler. Tijdens deze toelichting zijn er ook vragen gesteld die hieronder zijn weergegeven. De presentatie van 5.1.2f zal als aparte bijlage worden meegestuurd.

Vraag (Q) en antwoorden (A) bij de presentatie van 5.1.2f :

- Q: wat is er in de periode tussen de gevonden webshell en het starten van het onderzoek gebeurt?
  A: Er is contact geweest met Citrix over de resultaten van het script waaruit bleek dat er een webshell op de netscaler is aangetroffen. Citrix gaf het advies om de netscalers opnieuw op te bouwen, op te schonen (te wipen) en nieuw serviceaccounts te installeren, dat zou voldoende moeten zijn Dat is gebeurd.
- Q: is het SOC hierbij aangehaakt of is dit alleen door de technische mensen uitgevoerd?
  A: Het SOC is vanaf het begin betrokken geweest en heeft de triage gedaan in overleg met NCSC en Citrix.
- Hoe is de webshell ontdekt?
  A: er waren crashes van de netscaler, waarbij de crashdumps naar citrix zijn gestuurd om te onderzoeken wat de oorzaak was.
- Q: wat is er wel/niet gelogd?
  A: er is basale logging, 5.1.2h . Dat is nu sterk verbeterd met bijna 100% zichtbaarheid. Er is naast de logging ook gebruik gemaakt van de coredumps en backup images, 5.1.2h 5.1.2h De logging wordt nu ook doorgezet naar het SIEM.
- Q: Nu zijn de netscalers volledig onder monitoring, waarom niet eerder?
  A: Dat is niet bewust geweest maar historisch gegroeid door de keuze wat wel en niet te loggen met het oog op performance. Voortschrijdend inzicht laat zien dat het goed is om ook op de netscalers volledige monitoring te hebben
- Q: wat is de retentie van de logging?
  A: de retentie was 5.1.2h maar dit is nu 5.1.2h Voor de netscalers is dit nog niet precies uitgewerkt, deze data wordt nu nog bewaard. 5.1.2h
- Q: is het tijdverloop hetzelfde als bij het OM?
  A: er is contact geweest tussen JIO/Fox-IT en het OM, maar daar zijn geen details uitgewisseld. De tijdlijn van het incident matcht en er is overlap met gevonden IP-adressen. Het beeld is wel dat de tijdlijn ongeveer hetzelfde is.
- Q: Zit er een firewall tussen internet en de netscaler?
  A: ja, dat is normaal en die laat standaard connecties toe om thuiswerken te faciliteren.
- Q: hoe heeft JIO gehandeld naar de bredere groep die getroffen is toen bleek dat er naast de netscalers van JIO nog andere netscalers zichtbaar waren in de scans?
  A: Er is melding gedaan naar Solvinity (beheerder) en JenV (domein verantwoordelijke) over het openstaan van de omgeving. Hierop is actie

ondernomen om dit dicht te zetten. JIO heeft een extra pentest gedaan om te controleren of het nu dicht staat. Dat is het geval. JIO is verantwoordelijk voor de eigen omgeving. Solvinity en JenV moeten het incident buiten die omgeving oppakken. Er is een contact geweest met de 5.1.2e 5.1.2e zal dat nagaan.

- Q: is er alleen een webshell gevonden op de genoemde netscaler, niks op de overige?
  A: klopt. Alle andere netscalers in het JIO-domein zijn onderzocht en er is verder niks gevonden. Als er nieuwe scripts of IOC's zijn binnengekomen (van bv NCSC) dan is dit telkens opnieuw onderzocht.
- Q: hoe verhoudt het uitvoeren van scripts zich met het wissen van sporen door aanvallers?
  A: het script checkt vooral op aanwezigheid van IOC's (webshells en andere artefacten). Als deze kundig zijn verwijderd vindt het script niks. Je kunt dus nooit 100% zeker zijn dat er niets aanwezig is geweest.
- Q: Als het script niet alles detecteert kan het ook van andere netscalers afkomstig zijn?
- A: de gebruikte IP-adressen zijn in beeld en daar kunnen we acties en connecties uit herleiden. Deze netscalers zijn specifiek in beeld, de rest niet dus die zijn waarschijnlijk niet gebruikt door de aanvallers.
- Q: zijn de wachtwoorden versleuteld?
  A: De wachtwoorden zijn geobfusceerd. 5.1.2h 5.1.2h 5.1.2h Het onderzoek heeft gekeken naar verdachte verbindingen maar niks gevonden.
- Q: wat zijn die 2 rare pieken in het verkeer in die 3 maanden geweest?
  A: er is een piek in netwerkverbindingen, niet in de logs. Dit is niet goed te verklaren. Het zijn geen pieken (in grootte) die je verwacht bij een flinke dataexfiltratie
- Q: is de logging nu aangezet?
  A: ja de logging 5.1.2h is aangezet. Er vindt nu onderzoek plaats wat wel/niet moet worden bewaard op basis van usecases.
- Q: er zijn concrete aanwijzingen dat er sporen zijn gewist, kun je dat in project LoMe terugzien?
  A: Neva is een onderzoek geweest specifiek op de aangetroffen sporen, Lome is meer een algemeen onderzoek. Daar kan malware in aangetroffen worden. Het is lastig te zeggen wat er gevonden gaat worden. Hoe detecteer je semi-legitiem gedrag.
- Q: delen uit het rapport zie je niet terug in de dagelijkse sitraps
  A: communicatie tussen JIO, 5.1.2f en opdrachtgevers is niet eenduidig geweest, zit veel ruis in. Het contact met opdrachtgevers is niet altijd via de CISO-lijn geweest. (bijvoorbeeld over de continuiteitsplannen). Er moet afstemming komen over de communicatie tussen JIO en opdrachtgevers.
- Q: zaten er restricties op het verkeer van de netscaler naar de DWO?
  A: Ja, dat is uitvoerig onderzocht en die verbinding lijkt goed dicht te zitten.
- Q: is de toestemming voor inzage in de logs van de opdrachtgever nu geregeld?
  A: Ja. De inzage in de logging van de specifieke opdrachtgevers was tijdelijk. Wel is er nu inzicht in de logging die JenV doet aan de buitenkant.
- Q: wat is het verschil in aannemelijk, zeer aannemelijk en niet aannemelijk?
  A: in versie 1.1 zal een tabel moet toelichting hierop worden toegevoegd

168346405 0071 0200

- Q: hoelang duurt project lome?
  A: in de week van 13-10 zal de laatste data aanlevering zijn, daarna wordt de data geanalyseerd en dan een rapport opgeleverd. Zal ongeveer nog 2 maanden duren.
- Q: hoe aannemelijk is het dat iemand nu nog binnen zit (per opdrachtgever), kan er aan het bestuur worden gemeld dat we veilig zijn?
  A: daar kan 5.1.2f geen antwoord op geven, er is geen kennis van de interne processen.
- Q: de DIVD had al eerder info over een kwetsbaarheid van de citrix netscaler, is daar wat mee gedaan?
  A: waarschijnlijk is dit via een proactieve scan geweest op het moment van de patches en niet specifiek op deze kwetsbaarheid.
- Q: Waarom is er een scan gedaan op de sterkte van de wachtwoorden?
  A: dit is onderdeel geweest van spoor 3, als basis voor een risico-inschatting.
- Q: is de NTDS.dit gecompromitteerd?
  A: Nee, er zijn geen sporen van exfiltratie.
- Q: nu wordt specifiek de naam van de AP in het rapport vermeld, waarom?
  A: niet bewust, wordt veranderd in een algemene aanduiding.

Overige onderwerpen:
Er wordt ook nog gesproken over de hoeveelheid aan rapportages en bevindingen en hoe ermee om te gaan. 5.1.2e geeft aan om hier gezamenlijk in op te trekken en een zo groot mogelijk gemeenschappelijke deler proberen te vinden om tijdens de opdrachtgeversdag een gezamenlijk beeld richting bestuur te geven. 5.1.2e heeft ook aangegeven dat er een plan moet komen met extra acties ten opzichte van het bestaande actieplan als dat uit de analyse van de citrix crisis blijkt.

Het actieplan is indertijd opgesteld richting de bestuurders op basis van een bepaald beeld. Uit het rapport van 5.1.2f blijkt dat het dreigingsniveau anders is, hoger. Hieruit kan komen dat het actieplan anders moet worden ingekleurd. 5.1.2e geeft hierop aan dat JIO dit intern zal bespreken en erop terugkomt.

Acties:
1. JIO plant een vervolgoverleg in om ook nog een nadere toelichting te geven welke acties JIO heeft uitgezet tijdens en na deze crisis
2. JIO zorgt ervoor dat de antwoorden op vragen die in mails zijn gesteld in een integrale mail worden beantwoord
3. 5.1.2f komt met een versie 1.1 waarin diverse opmerkingen en aanpassingen zijn verwerkt
4. JIO zal nagaan welke acties er zijn uitgezet bij Solvinity n.a.v. het dichten in het gat van de firewall
5. JIO zal met de directeur actieplan bespreken of het rapport van 5.1.2f nog consequenties heeft voor de acties en richting van het actieplan.