Verslag Update Citrix/Netscaler 29-7-2025

Aanwezig: 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). 5.1.2e , 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

Opening

Slide Deck wordt gedeeld na de bijeenkomst. 5.1.2e van 5.1.2f presenteert.

Slide 1

Spoor 1 gaat over onderzoek Netscaler zelf. Spoor 2 onderzoek omliggende netwerken, daar zijn we heel erg afhankelijk van de uitkomst van de beeldvorming. De beeldvorming veranderd de scope van het onderzoek en daarmee de voortgang. Spoor 3 is informeel gestart om quick wins op te halen, zoals bijv. logging domain controllers. Er zij nog geen harde indicaties gevonden om naar spoor 3 over te stappen. Er wordt een voorstel hiervoor voor gemaakt aan JIO momenteel door 5.1.2f 2f .

- 5.1.2e heeft begrepen dat spoor 1 was afgerond. 5.1.2e geeft aan dat dit het geval is, dat het vooral gaat om kleine laatste puntjes op de i.
- 5.1.2e : 20% van de beeldvorming ontbreekt, zit daarin nog missende informatie van SOC J&V. Dat klopt deels. Dit helpt om de verder beeld te krijgen van de betekenis van de gaten die er zijn.

Slide 2

Een tijdlijn wordt voornamelijk in de rapportage uitgewerkt, maar is nu alvast gedaan omdat het prettig is voor iedereen om hier een beeld bij te hebben. De doorlooptijd is groot, dit maakt forensisch onderzoek lastiger. Het is veel data dat moet worden doorgenomen en er kan een hoop gebeurd zijn m.b.t. de sporen.

- 5.1.2e 5.1.2e Is er tussen 26 mei en 17 juni niets gebeurd? Dit wordt nu onderzocht. Er is via track 1 niets gevonden. De logging over welke netwerkverbindingen van Netscaler opgezet, daar wachten we nu op. Het akkoord van alle CISO's is nodig om goedkeuring te geven aan SOC J&V om deze gegevens te delen met JIO/Fox IT.
- 5.1.2e :

  1. Tijdslijn staat tot 29 juli. Wanneer verwachten jullie dit af te ronden? Het is moeilijk om te weten wanneer het onderzoek klaar is. Voor track 3 staat de beeldvorming nog maar op 5 procent. Track 2 uitkomsten beïnvloeden. Gaat het nog dagen of maanden duren. Voorzichtige impact is enkele weken voor track 2, track 3 is groots, daar valt geen tijd aan te koppelen.
  2. Waarom heeft de monitoring niet aangestaan zodat het in het begin van de tijdslijn het incident zou zijn opgevallen? 5.1.2f 2f heeft logging om door te nemen. Verder zijn zij niet degene die antwoord kunnen geven op deze vraag. → 5.1.2e gaat deze vraag mee terugnemen naar het CMT JIO om te beantwoorden.
- 5.1.2e : De aanvaller verwijderd zijn sporen. Daar wordt door 5.1.2f rekening mee gehouden, in de modus operandi van de aanvaller.

Slide 3

De vraag voor toestemming voor inkijk in verbindingen bij Solvinity is echt belangrijk om dit deel van het onderzoek goed te kunnen doen.

- 5.1.2e : kun je hier nog spreken over een goed ingerichte DMZ? 5.1.2f 2f wordt vaker gevraagd om een firewall e.d. te analyseren. Het is aan de business om de keuze te maken. 5.1.2f vindt het een opvallend iets, maar weet niet waarom Solvinity dit zo heeft ingericht. Dit is een reden tot evaluatie met Solvinity en zorg, aldus 5.1.2e .

- 5.1.2e : Zijn de BC alleen read-only of ook schrijfbaar? Momenteel weten wij dit niet. Dit zou verder onderzocht moeten worden en iemand moet eigenaarschap hierop pakken, 5.1.2f werkt nu voor JIO enkel.

Vragen

- 5.1.2e : Nieuwsuur staat om 16:00 uur voor de deur om een update over OM en DJI. We willen graag een woordvoerderslijn hierin krijgen, graag voor 14:00.
- 5.1.2e : 5.1.2e is woordvoerder vanuit J&V. Onderliggende organisaties doen geen eigen woordvoering/uitspraken.
- 5.1.2e : Is een ZBO dus valt niet helemaal onder J&V. Zeker met het nieuws vanuit DJI (DJI heeft vanochtend om 10:52 geplaatst (dji.nl/nieuws) moet een eenduidig reactie te komen. Deze reactie is waarschijnlijk niet met 5.1.2e afgesproken, dat gaat 5.1.2e uitzoeken. 5.1.2e gaat zijn directeur laten bellen met 5.1.2e om een persboodschap af te stemmen.
- 5.1.2e : Gisteren heeft 5.1.2e begrepen dat er een voorstelbericht vanuit JIO zou komen om te communiceren naar de buitenwereld. Dat is niet wat 5.1.2e bedoelde, die bedoelde dat er een verhaal zou komen over de tijdlijn en de acties/stand van zaken voor de duidelijkheid bij alle partijen in het CISO-overleg. 5.1.2e geeft ook aan dat voor JIO de communicatie via J&V 5.1.2e loopt. 5.1.2e neemt eventueel voor meer informatie contact op met 5.1.2e .

Morgen zelfde tijd wederom overleg.

Rondvraag

- 5.1.2e deelt informatie NSCS ook met andere CISO's n.a.v. vraag 5.1.2e .
- 5.1.2e : het advies van afkoppelen door NSCS was gisteren niet bekend bij JIO. Dit bericht is minder zwart wit dan in eerste instantie geplaatst, 5.1.2e geeft aan dat hier nog reactie op komt.
- 5.1.2e : In DMZ staan een hoop andere systemen waar zou kunnen zijn toegeslagen. Gaat Solvinity hiernaar kijken? De informatie is gedeeld met CISO J&V en die gaat contact opnemen om met de betreffende CISO's om verdere stappen te zetten. 5.1.2f probeert in ieder geval zoveel mogelijk in kaart te brengen welke verbindingen er gemaakt zijn vanuit de Netscaler.
- 5.1.2e : Appje van 5.1.2e over scenario's eiland modus.
- 5.1.2e : Er is behoefte aan een overzicht welke systemen uit de lucht gaat indien we van het internet afgaan. Deze vraag wordt meegenomen naar CMT JIO.
- 5.1.2e : DJI heeft in lijn met JIO melding bij AP gedaan.

Acties

1. Behoefte aan een overzicht van de systemen die offline gaan bij afkoppeling met internet. 5.1.2e gaat dit bespreken in het CMT van JIO.
2. Antwoord op de vraag: waarom heeft de monitoring niet eerder de intrusie opgepikt. 5.1.2e gaat deze vraag uitzetten ter beantwoording middels het CMT van JIO.