To: 5.1.2e, 5.1.2e 5.1.2e @dji.minjus.nl]
From: 5.1.2e
Sent: Wed 7/30/2025 2:06:49 PM
Subject: RE: Slides CISO overleg
Received: Wed 7/30/2025 2:06:50 PM

Hi 5.1.2e,
Hierbij de notulen inclusief de inhoud van de presentatie van ons vorige overleg:

Update citrix / netscaler 30-07-2025

Updates vanuit het lopenende onderzoek
- Samenwerking 5.1.2f SOC JIO & SOC JenV
- Beeldvorming van de AD structuur
- Vragen containment maatregelen > eerste analyse bekende kwetsbaarheden voor quick-wins
- NCSC gaat opnieuw een analyse doen met alle data die ze van 5.1.2f en andere partijen hebben ontvangen

Informatie-uitwisseling NCSC & JIO over rapporten 5.1.2f is besproken. 5.1.2f en JIO heeft geen problemen om deze resultaten te bespreken maar NCSC wilt de end-of-day rapportages ontvangen waarbij vermeld is dat dit geen probleem is maar wel met de voorwaarde dat de partijen bij de end-of-day overleggen aansluiten om ook de context mee te krijgen.
Het is belangrijk om te vermelden wat de doeleinde zijn van de informatie die het NCSC wilt ontvangen en dat deze informatie niet zomaar verspreid wordt.

Samenwerking SOC JenV: connectie logs
Er lopen drie trajects waar 5.1.2f mee bezig is. De DMZ, omliggende netwerken en DWO. Vanuit 5.1.2f zien wij voornamelijk het verkeer binnen deze drie levels in de logs (Van DMZ naar de omliggende netwerken en/of DWO) maar we zien niet het verkeer die binnen deze delen plaatsvinden (Binnen DMZ). Er moet besloten worden wie verantwoordelijk is voor de opvolging van de pentest resultaten die buiten het onderzoek van 5.1.2f lopen.

Indicatie voortgang verschillende sporen
Voor de voortgang op de verschillende onderzoekssporen is hieronder een inschatting gemaakt. Dit is een momentopname van de huidige stand van zaken, uitkomsten van de beeldvorming kunnen de scope van een spoor nog vergroten of verkleinen, met hetzelfde effect op de percentuele voortgang. Beeldvorming en dataverzameling van Spoor 1 is verder ontwikkeld en de beeldvorming van spoor 3 is ook vergroot.

JIO is bezig om 5 scenario's op te stellen in het geval zij nodig zullen zijn tijdens deze situatie. Per scenario wordt uitgeschreven wat er gedaan wordt en wat de gevolgen hiervan zijn.
1. He tinkomende internverkeer richting de Connect dienst wordt beperkt
2. Het inkomende internetverkeer richting de Connect dienst wordt volledig afgesloten
3. Uitgaand internetverkeer wordt beperkt
4. Uitgaand internet wordt volledig afgesloten
5. Volledige quarantaine

Het zou prettig zijn om de voortgang van de vijf scenario's te bespreken in het CMT. Op dit moment worden gesprekken gevoerd met verschillende partijen om deze scenario's en bijbehorende acties in kaart te brengen. Deze en volgende week wordt hieraan gewerkt. Naar verwachting zal het eerste scenario volgende week afgerond zijn. De uitwerking is sterk afhankelijk van externe partijen. De klantenteams moeten aangeven hoe zij hiermee om willen gaan en of zij hierin een rol willen nemen.

Daarnaast is onduidelijk wat precies wordt bedoeld met het volledig herstel van de dienstverlening van het OM. De herstelwerkzaamheden worden dit weekend gefaseerd uitgevoerd. Het is nog niet duidelijk of het onderzoek van invloed heeft op het herstel van de dienstverlening. Dit onderzoek staat los van de herstelacties vanuit het OM.

Met vriendelijke groet,
5.1.2e 5.1.2e
5.1.2e

Afdeling Kwaliteit, Planning & Control

Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid
Stavorenweg 3 | 2803 PT | Gouda |
Postbus 850 | 2800 AW | Gouda
.....
5.1.2e

T: 5.1.2e
E: 5.1.2e @dji.minjus.nl
W: www.justitieleictorganisatie.nl

Van: 5.1.2e , 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
Verzonden: woensdag 30 juli 2025 15:43
Aan: 5.1.2e < 5.1.2e @dji.minjus.nl>
Onderwerp: FW: Slides CISO overleg
Van: 5.1.2e 5.1.2e : 5.1.2e @fox-it.com>
Verzonden: woensdag 30 juli 2025 15:07
Aan: 5.1.2e , 5.1.2e 5.1.2e 5.1.2e @dji.minjus.nl>
Onderwerp: Slides CISO overleg

Zoals besproken, hierbij de slides.
Groet,
5.1.2e