From: 5.1.2e
Sent: Fri 8/1/2025 1:33:05 PM
Subject: Terugkoppeling CMT 31.07.2025 13:30 uur
Received: Fri 8/1/2025 1:33:04 PM

Van: 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl> **Namens**
Verzonden: donderdag 31 juli 2025 16:42
Aan: 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @jio.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e, 5.1.2e < 5.1.2e @dji.minjus.nl>; 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
CC: 5.1.2e 5.1.2e < 5.1.2e @dji.minjus.nl>
Onderwerp: Terugkoppeling CMT 31.07.2025 13:30 uur

Crisisoverleg CMT 31-07-2025 13.30
Aanwezig: 5.1.2e 1 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. 5.1.2f 5.1.2e 5.1.2e 5.1.2e
Afwezig: 5.1.2e

Bespreekpunten

- Bevinding pentestteam DMZ: Er is uitgebreid gesproken met Solvinity over bevinding DMZ. Solvinity heeft preventieve maatregelen genomen. Solvinity gaat dit op papier zetten en dan komt het ter bespreking in dit CMT. In dit CMT bekijken hoe we hiermee verder gaan.
  Meerdere organisaties nemen de connect-dienst af, maar doen hun eigen infra. Dit is niet in scope van het huidige forensisch onderzoek. Hierdoor is er onduidelijkheid onder deze organisaties of zij hun eigen forensische onderzoek.
  Besluit: Advies JIO is om CISO JenV om advies te vragen.
- 5.1.2h Het is van belang om hier oog te hebben voor de scope van het onderzoek in spoor 2.
- Oplevering impactanalyse: De oplevering van de impactanalyse spoor 2 gaat langer duren dan 1 augustus. Dit is opgenomen in de sitrap van 31/7.
- Aansluiting op SIEM: Er is nu veel meer aangesloten op het SIEM. Alle informatie die hier uit komt, is bruikbaar. Vanuit 5.1.2h geen zorgelijke meldingen op het netwerk. Als we melding krijgen, is dat te verklaren of te achterhalen. Complimenten aan het SOC voor de realiseren hiervan.
- Aanvullend spoor compromittering: Uit onderzoek van 5.1.2f is een tweede webshell gevonden. Dit is in dezelfde tijdspanne en op dezelfde netscaler. Het gaat om dezelfde compromittering, maar nu is dit door 5.1.2f gevonden in de back-up. De eerste webshell komt uit de dump van Citrix.
- Sessie met SOC JenV: 5.1.2f heeft de sessie met SOC JenV erg positief ervaren. Men was heel behulpzaam bij het inzichtelijk maken van de connecties. Hierdoor heeft 5.1.2f goed kunnen verifiëren dat ze over de juiste data beschikken.
- 5.1.2h is mogelijk een zeer interessante bron voor het SOC. Hiermee kunnen ze teruggaan naar begin dit jaar (dus voor de aanval).
- Advies wachtwoord reset: Vanuit CISO-overleg is de vraag of het verstandig is om een wachtwoord reset te doen. Besluit: JIO adviseert opdrachtgevers om een wachtwoord reset te doen.
- CISO-overleg: Wederom werd er door CISO JenV om de voortgang van de handelingsperspectieven gevraagd. De boodschap dat de opdrachtgevers zelf verantwoordelijk zijn voor hun eigen handelingsperspectief lijkt niet goed door te komen. We blijven dit communiceren. Voor de voortgang kan de CISO JenV dus terecht bij de opdrachtgevers zelf.
- Sitrap 31-7-2025: De sitrap is besproken. Tekstuele wijzigingen zijn tijdens het overleg doorgevoerd en verstuurd naar de CMT-leden. De sitrap wordt conform afspraken verder verspreid naar CISO's, DCC, CIO's, en secretaris CMT JIO.
- CMT weekend 2-3 augustus: CMT gaat in deze vorm door komend weekend.

Actiepunten – Niet besproken
Alleen de openstaande acties zijn hierin opgenomen

Overleg	#	Actie	Wie	Status
22-07 17:00	1	Nagaan waar mogelijk afspraken niet nagekomen kunnen worden vanwege deze situatie	5.1.2e en 5.1.2e	28-07 13:30: Loopt 29-07 13:30: Loopt 30-07 13:30: Loopt

23-07 08:30	2	Handelingsperspectieven eigen organisatie è 5.1.2e en 5.1.2e	5.1.2e	28-07 13:30: Vanmiddag kick-off handelingsperspectieven 5.1.2e doet DJI, 5.1.2e de rest, inclusief JIO. 29-07 13:30: Loopt 30-07 13:30: Loopt
24-07 09:30	3	5.1.2 5.1.2e vragen om een PvA schrijven van PvA voor wachtwoord reset	5.1.2e	28-07 13:30: PvA DJI is afgerond. DT&V en JIO nog wel doen. 29-07 13:30: PvA DT&V en JIO is klaar. Uit te voeren op 31-07.
24-07 17:00	4	We moeten via inkoop uitzoeken als dit nogmaals gebeurd moeten we voorbereid zijn (lange termijn, niet voor CMT)	5.1.2e	28-07 13:30: Lange termijn
24-07 17:00	5	Voorbereiden om een reset te doen voor de beheerdersaccount (5.1.2e *heeft 26.07 per mail laten weten dat voorbereiding heeft plaatsgevonden.* 5.1.2e *heeft ingestemd om dat maandag (28.07) uit te voeren)*	5.1.2e	28-07 13:30: Besluit CMT: Op woensdag 30-07 uitvoeren van de reset 29-07 13:30: Wordt 30-7 in gang gezet 30-07 13:30: Is in gang gezet. Dit wordt morgen afgerond.
24-07 17:00	6	Nagaan dienstverlening aan NCSC en NCTV	5.1.2e	5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2e 5.1.2h Afgerond
25-07 17:00	7	5.1.2e vraagt 5.1.2e na te gaan wat er onder de dienstverlening van 5.1.2f valt binnen hun overeenkomst met het Rijk	5.1.2e	28-07 13:30: Nog geen antwoord. 29-07 13:30: Nog niks gevonden. 30-07 13:30: 5.1.2e heeft uitvraag 5.1.2f met 5.1.2e gedeeld. Nog geen antwoord.
28-07 13:30	11	Lijst met dekking monitoring 5.1.1b voor CISO's opstellen	5.1.2e	28/7 13:30: actie 5.1.2e, in overleg met 5.1.2e en 5.1.2e 5.1.2e en 5.1.2e kijken mee 29/7 13:30: Loopt 30-07 13:30: Mapping is op dienstniveau. Dit loopt.
29-07 13:30	14	Voorzet kosten en tijd uitbreiden hardware	5.1.2e	30-07 13:30: Loopt
29-07	15	Verzamelen van de vragen die	5.1.2e	30-07 13:30: Loopt. Actie allen: Input

13:30		bij opdrachtgevers e.a. leven en maken een startset met antwoorden		leveren.
30-07 13:30	16	Inventariseren wens ww reset andere opdrachtgevers + toelichten van het nut hiervan in CISO-overleg	5.1.2e	