To: 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 5.1.2e @dji.minjus.nl]; 5.1.2e , 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 5.1.2e @dji.minjus.nl]
From: 5.1.2e , 5.1.2e
Sent: Thur 7/24/2025 6:40:57 PM
Subject: Terugkoppeling CMT 24-07-2025 17:00 uur
Received: Thur 7/24/2025 6:42:16 PM

Aanwezigen: 5.1.2e 1 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e **en** 5.1.2e

- Stand van zaken:
  - Er is een externe partij die via NCSC is aangehaakt. 5.1.2h die ook een hack hebben gehad en waar we gelijke patronen zien. 5.1.2h We leren van hun cases. Wij doorzoeken onze servers en NetScaler op dezelfde patronen, er is nog niets zichtbaar.
  - Het lijkt een gecoördineerde aanval van een professioneel hackteam. Op 8 en 9 mei zijn de eerste sporen van verkenningen en pogingen zichtbaar. Op 26 mei was de poging geslaagd. Ze zijn binnengekomen via een Zero Day exploit, het is een lek wat bekend is bij de hackers en daar is nog geen oplossing (patch) voor. Door een van de andere organisaties is het CSIRT van de EU ook aangesloten.
  - Het spoor van NetScalers is nu redelijk klaar, alle onderzoeken die daarop zitten zijn redelijk afgerond. We kunnen niet met zekerheid vaststellen dat ze niet verder gekomen zijn, we moeten door met het onderzoek naar de andere sporen.
  - 5.1.2h Ze zijn de omgeving van de NetScalers in kaart aan het brengen, dit vergt enige tijd. Dit is veelomvattend. De Dc's zijn allemaal aangesloten op het SIEM en door het SOC bevestigd dat ze het zien. Voor het DWO lopen nu 3 testen, hopelijk morgen kunnen we richting de productieomgeving gaan. Waarna we gefaseerd over kunnen gaan.
  - We moeten melden aan de CISO's van de opdrachtgevers over het SIEM en onze (event)logging om een juist beeld over schetsen. 5.1.2h 5.1.2h
  - We zijn gebeld door het SOC dat er verdachte patronen te zien zijn op 5.1.2h Dit wordt momenteel onderzocht, maar er wordt ook gekeken of hij afgeschakeld kan worden.
- Bovenstaande wijzigt vooralsnog niets aan ons advies. Met name de check met de IP-adressen en de scan die bezig is (door de pentesters). Morgen zal een spannende dag zijn.
- We zijn aan het kijken wat we eventueel kunnen afsluiten of White listen. Als we willen opschalen qua maatregelen zijn we alvast aan het voorbereiden.
- Op de nota ook het "voortraject" meenemen. 5.1.2e deelt dat met 5.1.2e voegt deze toe.
- Handelingsperspectieven en wegingskader:
  - Vanmorgen op 2 vragen van DJI beantwoord.
  - Afkoppelen van internet (binnen-buiten), we willen een oudere White list gebruiken. Als deze ingezet worden, moeten we hierover gecommuniceerd worden met medewerkers.
  - PvA voor wachtwoord reset is verstuurd. DJI heeft aangegeven dat ze nog niet klaar zijn voor de wachtwoord reset, vanwege de mensen op vakantie. Mogelijk dat dit issue ook voor ons geld. Wij zijn geen voorstander voor het resetten van de serviceaccounts. Mogelijk dat dit wel kan voor de beheerdersaccounts (dit zijn de accounts met de hoogste rechten). 5.1.2e laat dit voorbereiden.
  - 5.1.2e doet DJI en 5.1.2e doet de andere opdrachtgevers bij het maken van het handelingsperspsectief.
- We hebben het contract van 5.1.2f opgehoogd. Alles wat we nu met 5.1.2f gaan doen is onrechtmatig. 5.1.2e gaat dit na bij 5.1.2e . We moeten via een document vastleggen waarom we onrechtmatig inkopen en dit aan het dossier hangen. 5.1.2e pakt deze actie op.
- Call gehad met 5.1.2f over de communicatiestrategie op de handelingsperspectieven. Vanmiddag al iemand gestart om zich

in te lezen. Morgen alvast een eerste gesprek.

- 5.1.2e is samen met de 5.1.2e een melding aan het voorbereiden voor bij de AP, dit op advies van het AP. Dit is een potentieel datalek. Mogelijk dat elke organisatie dat zelf kan doen, wij het voor allemaal kunnen doen of JenV het kan doen.

- 5.1.2e heeft 5.1.2e 5.1.2e gesproken, is de verbinding met 5.1.2e noodzakelijk of is deze lijn prima. 5.1.2e gaat dat na.

- Het advies n.a.v. ons uitgebreide logboek, volgt vanavond en is morgen te bespreken in het CMT. 5.1.2e schrijft ook een reactie voor het NCSC.

- 5.1.2e gaat na bij 5.1.2e of wij dienstverlening (evt. via Dienstencentrum) leveren aan NCSC en NCTV

Actiepunten

Alleen de openstaande acties zijn hierin opgenomen

Overleg	Actie	Wie
22-07 17:00	Nagaan waar wij mogelijk steken laten vallen vanwege deze situatie	5.1.2e en 5.1.2e
23-07 08:30	Handelingsperspectieven eigen organisatie x 5.1.2e en 5.1.2e	5.1.2e
23-07 17:00	Bespreken weekend inzet	5.1.2e
24-07 09:30	5.1.2e 5.1.2e vragen om een PvA schrijven van PvA voor wachtwoord reset	5.1.2e
24-07 17:00	We moeten via inkoop uitzoeken als dit nogmaals gebeurd moeten we voorbereid zijn (lange termijn, niet voor CMT)	5.1.2e
24-07 17:00	Nagaan of de inkoop onrechtmatig is, als dat zo is dan moet er een document voor opgesteld worden.	5.1.2e
24-07 17:00	Voorbereiden om een reset te doen voor de beheerdersaccount	5.1.2e
24-07 17:00	Nagaan dienstverlening aan NCSC en NCTV	5.1.2e

Met vriendelijke groet,

5. 5.1.2e) 5.1.2e
5.1.2e
.....
Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid
Stavorenweg 3 | 2803 PT | Gouda
Postbus 850 | 2800 AW | Gouda
.....
M 5.1.2e
E 5.1.2e @jio.nl
W http://www.jio.nl
.....
5.1.2e
Volg ons ook op: