Vragen aan JIO

- Wij constateren dat kwaadwillende actoren in de zomer van 2025 hebben kunnen binnendringen bij JIO via een kwetsbaarheid in de Citrix Netscaler. Wat is daarop uw reactie?
- Op welke datum vond het eerste misbruik van deze kwetsbaarheid bij JIO plaats?
- Op welke datum constateerde JIO dat aanvallers misbruik hadden gemaakt van deze kwetsbaarheid bij JIO?
- Wij constateren dat door een configuratiefout in de firewall (die wordt beheerd door Solvinity) de monitoring en logging van de firewall uitstond. Hierdoor konden de indringers vanuit de demilitarized zone (DMZ) onopgemerkt doordringen tot de ICT-systemen van JIO en de klanten / opdrachtgevers van JIO. Wat is daarop uw reactie?
- Hoe kan het dat JIO niet doorhad dat de firewall verkeerd was geconfigureerd?
- Hoe lang stond die firewall al verkeerd geconfigureerd?
- Wat is het beleid van JIO ten aanzien van monitoring en logging? Voert JIO periodieke controles uit op de firewalls en andere vergelijkbare security-systemen?
- Wat weet JIO over de identiteit van de indringers? Klopt het dat de veiligheidsdiensten hebben gewaarschuwd dat het waarschijnlijk gaat om een statelijke actor?
  Over de identiteit van de indringers doet Justitiële ICT Organisatie geen uitspraken.
- Welke informatie heeft JIO over deze ICT-inbreuk gedeeld met haar opdrachtgevers?
- Wat heeft JIO gedaan om te voorkomen dat gevoelige data gelekt zouden worden?
- Verschillende betrokkenen hebben gewaarschuwd voor de risico's van de hack en hebben JIO geadviseerd de ICT-systemen offline te halen. Wij constateren dat JIO dit niet heeft gedaan. Waarom heeft JIO dit advies niet opgevolgd?
- Verschillende bronnen wijzen op het risico dat enkelbanden niet meer (volledig) zouden functioneren als JIO offline zou gaan. Erkent u dit risico? Welke rol speelde dit risico in het besluit om de organisatie niet offline te halen? Weet u inmiddels of de enkelbanden in zo'n geval inderdaad niet meer (volledig) zouden functioneren?
- 5.1.2f heeft onderzoek gedaan naar aanleiding van de hack. Klopt het dat het (concept)rapport van 5.1.2f met u gedeeld is? Waarom is er nog geen definitief rapport? Waarom zijn de resultaten niet met de Tweede Kamer gedeeld?
- Wij concluderen dat de indringers die via het Citrix-lek zijn binnengekomen mogelijk nog steeds mee kunnen kijken in de systemen van JIO en de klanten van JIO. Kunt u uitsluiten dat de indringers nog steeds mee kunnen kijken?
- Uit onze bronnen blijkt dat 5.1.2e 5.1.2e 5.1.2e per 1 maart vertrokken is bij JIO. Waarom is hij vertrokken? Houdt zijn vertrek verband met de tekortschietende informatiebeveiliging van JIO?