Q&A Netscaler Citrix – JIO

VRAAG: Waarom is niet besloten om de IT-omgeving los te koppelen van het internet?

ANTWOORD: Omdat uit extern onderzoek is gebleken dat de hackers niet zijn doorgedrongen tot de achterliggende IT-omgevingen. En omdat Netscaler gepatched was en er aanvullende veiligheidsmaatregelen getroffen zijn.

VRAAG: Klopt het dat de firewalls niet goed functioneerden?
ANTWOORD: De firewalls functioneerden zoals beoogd en beschikten tijdens deze periode over logging van alle gebeurtenissen. Deze logging is door het externe onderzoeksbureau gebruikt bij hun onderzoek.

VRAAG: Waarom geven bronnen bij Argos aan dat de logging niet compleet is?
ANTWOORD: De Netscaler heeft ook interne logging, door beperkingen van dit systeem is dit echter beperkt tot enkele uren. De logging van de firewalls en van het netwerkverkeer is wel beschikbaar.

VRAAG: Was het onduidelijk of de enkelbanden nog zouden werken?

ANTWOORD: Er lag een scenario klaar voor het continueren van onder andere Elektronische Monitoring als de overige systemen van het internet afgeschakeld zouden worden.

VRAAG: Is de Justitiële ICT Organisatie gehacked?
ANTWOORD: in de Netscaler zijn sporen van inbraak aangetroffen. Er is gebruik gemaakt van de kwetsbaarheid en dus sprake van een hack. In de achterliggende IT-omgevingen zijn geen sporen aangetroffen.

VRAAG: Was de impact groot geweest als de IT-diensten afgeschakeld werden van het internet?
ANTWOORD: Ja, zonder aanvullende maatregelen had dit een grote impact gehad op de dienstverlening van de J en V-onderdelen.

VRAAG: Is een advies om de systemen offline te halen niet opgevolgd?
ANTWOORD: Er waren scenario's uitgewerkt om de impact voor de vitale processen te minimaliseren, zoals het (gedeeltelijk) afschakelen van het internet.

VRAAG: Houd het vertrek van de algemeen directeur van Justitiële ICT Organisatie verband met de status van de informatiebeveiliging?
ANTWOORD: Nee.

VRAAG: Is er een verband tussen de kwetsbaarheden van Citrix Netscaler en 5.1.2h EPMM?

ANTWOORD: Nee, uit extern onderzoek naar de kwetsbaarheid van 5.1.2h EPMM is geen verband naar voren gekomen.

VRAAG: Was de interne firewall door een configuratiefout uitgeschakeld?

ANTWOORD: Nee. Wel lieten deze meer verkeer door dan voor reguliere werking strikt noodzakelijk is.

VRAAG: Was er toegang tot andere IT-omgevingen?
ANTWOORD: Dit is onderzocht. Er werd vanuit de Citrix Netscaler meer verkeer toegelaten dan strikt noodzakelijk is dan de reguliere werking van het systeem.