Justitiële ICT Organisatie
Ministerie van Justitie en Veiligheid

Directie Justitiële ICT Organisatie (DJIO)

Justitiële ICT Organisatie
Strategie en Bedrijfsvoering

Stavorenweg 3
2803 PT Gouda
Postbus 850
2800 AW Gouda
www.justitieleictorganisatie.nl

Contactpersoon
5.1.2e 5.1.2e
5.1.2e

Datum
16 april 2026

Ons kenmerk
n.v.t.

nota

Opvolging conclusies en aanbevelingen evaluatie Berenschot van crisisorganisatie Citrix Netscaler 2025

Inleiding

In de zomerperiode van 2025 is het crisismanagementteam (CMT) van de Justitiële ICT Organisatie (JIO) actief geweest. De aanleiding hiervoor was de ontstane situatie nadat bleek dat een kwetsbaarheid in de Citrix Netscalers die JIO gebruikt was geëxploiteerd.

Om te leren van de gebeurtenissen, heeft JIO aan Berenschot de opdracht gegeven een evaluatie te organiseren die zich richt zich op het functioneren van de interne crisisorganisatie van JIO, lopend in de periode 21 juli t/m 8 augustus 2025. Daarnaast is bij de evaluatie aandacht geschonken voor hoe de opdrachtgevers van JIO de crisisaanpak van JIO hebben ervaren.

Voor JIO is het van cruciaal belang lessen te trekken uit de aanpak van de crisisorganisatie ter verbetering hiervan. Door te leren van ervaringen uit het verleden worden wij in staat gesteld om onze crisisaanpak verder te professionaliseren en onze organisatie (en mensen) gericht te ontwikkelen en te trainen. Evaluatie is wat ons betreft een essentieel instrument om continu te verbeteren en crisismanagement in de organisatie beter te borgen.

Op dinsdag 9 december 2025 heeft Berenschot haar bevindingen gedeeld in een rapport. De bedoeling was om het rapport begin januari 2026 te delen en toe te lichten in een sessie maar helaas is dit door capaciteitsproblematiek en de focus op de 5.1.2h blijven liggen. In de bijlage is het rapport toegevoegd. In deze nota gaan wij in op de belangrijkste conclusies en aanbevelingen van het Berenschot-onderzoek en lichten wij toe op welke wijze opvolging is gegeven aan het rapport.

Onderzoeksvragen en -aanpak

Voor de uitvoering van de evaluatie heeft Berenschot een drietal vragen opgesteld waarop in het rapport een antwoord wordt gegeven:

1 Wat kan de crisisorganisatie van JIO leren van haar inzet tijden het incident met Citrix Netscaler in 2025?
2 In welke mate heeft de crisisorganisatie van JIO het crisismanagementplan gevolgd tijdens de crisis reactie?
3 Hoe hebben opdrachtgevers van JIO de crisisreactie van JIO ervaren?

Om antwoord te geven op deze onderzoeksvragen heeft Berenschot een aantal activiteiten verricht. Op 16 oktober 2025 een evaluatiebijeenkomst georganiseerd met het crisisteam van JIO. Tijdens deze bijeenkomst hebben leden van de crisisorganisatie gezamenlijk het gesprek gevoerd over de leerpunten die uit dit incident naar voren komen. Daarnaast heeft Berenschot de door JIO beschikbare crisisdocumentatie bestudeerd, en gesproken met drie opdrachtgevers van JIO, DJI, DT&V en de AP, om op die manier in kaart te brengen wat hoe zij de crisisreactie van JIO ervaren hebben.

Dit rapport wordt ook aangeboden aan de opdrachtgevers die betrokken zijn geweest tijdens de Citrix Netscaler Crisis en zal in een sessie worden toegelicht om verbeterpunten en procesafspraken te maken. Deze sessie zal worden ingepland als ook de resultaten van de (interne) evaluatie van de 5.1.2h bekend zijn. (planning sessie juni 2026)

Conclusies

De conclusies en aanbevelingen zijn gebaseerd op de uitkomsten van de gesprekken met het CMT, de opdrachtgevers van JIO en de documentstudie. De conclusies geven op hoofdlijnen weer welke punten het belangrijkst zijn in deze evaluatie. De aanbevelingen hierbij zijn voor een deel één op één aan een conclusie te verbinden, andere zijn meer generiek van aard.

Conclusie 1: het duurde te lang voordat JIO opschaalde naar de formele crisisstructuur.
Het handboek crisismanagement is in het directieoverleg (JIO) van 14 juli 2025 vastgesteld. De crisisstructuur was daarmee nieuw en nog in ontwikkeling. Hierdoor was het in beginsel zoeken hoe het crisismanagementteam opgestart moest worden en welke personen in de beginfase van de crisis betrokken moesten zijn, ook omdat het een vakantieperiode was. Bovendien was de impact van de crisis niet direct duidelijk. Het incident is hierdoor in eerste instantie langs de reguliere incident management lijn opgepakt. Hierbij is in de pre-fase van een potentiële crisis periodiek de vraag of opschaling naar een crisisstructuur noodzakelijk is.

Conclusie 2: het besluit om systemen niet preventief offline te halen is genomen voorafgaand aan de opschaling van de crisisorganisatie. De afweging van JIO is daarna niet meer gewijzigd.
In de verslaglegging is niet duidelijk benoemd of en zo ja op welke wijze het besluit om niet preventief offline te gaan is heroverwogen. Ook is niet duidelijk welke overwegingen JIO hierbij had.

JIO heeft direct na ontdekking van de compromitatie contact gezocht met het NCSC en de vraag voorgelegd of we preventief offline moesten gaan. Hierop is door het NCSC voorgesteld om eerst een compromis assessment te doen door een externe incident respons partij om meer duidelijkheid te krijgen. Het preventief offline gaan van JIO betekent een enorme impact voor alle opdrachtgevers van JIO. De aanpak van het compromis assessment is gedaan volgens het 'follow the evidence' principe, zoals voorgesteld door 5.1.2f. Een heroverweging om offline te gaan zou afhangen van de resultaten van de bevindingen, in overweging met de 5.1.2e JenV.

Conclusie 3: JIO heeft een vast ritme en een vaste vorm gehanteerd voor het informeren van opdrachtgevers en andere stakeholders, namelijk in de vorm van sitraps en dagelijkse overleggen. Ondanks deze inspanningen kon JIO niet voldoen aan de informatiebehoefte van opdrachtgevers.
Dagelijks organiseerde JIO een informatiebijeenkomst voor de CISO's van opdrachtgevers, hierbij sloot 5.1.2f (forensisch onderzoeker) aan. JIO was ten tijde van deze bijeenkomsten niet altijd in staat alle vragen te beantwoorden en had meer tijd nodig voor onderzoek en analyse. Vanuit de opdrachtgevers ontstond hierdoor het beeld dat JIO niet altijd transparant was en werd handelingsperspectief gemist. Daarnaast heeft JIO in een tweetal sessies met alle intern betrokkenen van JIO alle openstaande schriftelijke vragen van de opdrachtgevers besproken en beantwoord.

Conclusie 4: tijdens de crisis was het actuele informatiebeeld niet centraal beschikbaar, wat de informatieoverdracht buiten het CMT bemoeilijkte.
Het CMT had een actueel beeld van de situatie, echter het ontbrak in het CMT aan een dedicated informatiecoördinator. Dit had met name te maken vanwege het feit dat de informatiecoördinator een gecombineerde rol was met de rol van adviseur crisisbeheersing. Deze combinatie is een te hoge belasting voor één persoon gebleken.

Conclusie 5: richting opdrachtgevers en stakeholders is gekozen om op punten terughoudend te zijn met het delen van informatie die mogelijk vertrouwelijk of gevoelig was.
Het CMT heeft vooropgesteld de intentie gehad om te allen tijde transparant te zijn, maar heeft echter ook geworsteld met de mate van informatievoorziening. Dit had met name te maken gevoeligheden van bepaalde informatie en de mogelijke effecten van het delen hiervan met stakeholders. Het betrof met name informatie over de technische infrastructuur die alleen op basis van het 'need-to-know' principe gedeeld kan worden om de security risico's zo laag mogelijk te houden. De afwegingen bij informatiedeling zijn zo zorgvuldig als mogelijk genomen, en niet lichtvaardig opgevat.

Conclusie 6: het proces van crisiscommunicatie heeft tijdens deze crisis geen solide vorm gekregen.
Tijdens het uitbreken van de crisis was er geen communicatieadviseur aanwezig. Crisiscommunicatie was hierdoor ad hoc georganiseerd. Met het aantrekken van een senior communicatieadviseur en het opzetten van een crisiscommunicatieteam hebben we dit nu sterker georganiseerd.

Conclusie 7: het inrichten van een hoog-prioriteit projectorganisatie in de nafase heeft gezorgd voor een goede overdracht van crisisorganisatie naar de reguliere organisatie.
Op 8 augustus 2025 schaalde JIO weloverwogen de crisisorganisatie af. Dit hing samen met de afschaling van het DCC van het ministerie van JenV. De openstaande acties en taken zijn toen overgedragen en in de nafase uitgevoerd door een resultaatgerichte hoog-prioriteit projectorganisatie. Met het afronden van de openstaande acties en het opleveren van het rapport LOME is de projectorganisatie opgeheven.

Aanbevelingen en vervolg
Naast conclusies heeft Berenschot – zoals eerder in deze nota aangegeven – aanbevelingen geformuleerd. Daar zijn hieronder benoemd alsmede die concrete verbeteractie daarbij.

1 *Versterk de overlegstructuur tijdens crisis, zodat de besluitvorming gestructureerd plaatsvindt en gebaseerd is op sterkere oordeelsvorming op basis van de feiten.*

Op 9 december 2025 heeft een basistraining crisismanagement plaatsgevonden met collega's met een rol in de crisismanagementstructuur. Daarbij is expliciet geoefend met het gebruiken van de zogenoemde BOB-methodiek om bewuste keuzes en afwegingen te maken voordat een besluit wordt genomen. Hier gaan we in 2026 mee verder. Opleiden, Trainen en Oefenen zijn een vast onderdeel van onze werkwijze geworden.

2 *Versterk de rolinvulling van de informatiecoördinator.*

Binnen de organisatie is een flexibele pool van informatiecoördinatoren (ICO's) opgebouwd met 8 collega's. Hiermee wordt voorkomen dat er een dubbelrol ontstaat met de adviseur crisisbeheersing en kan de informatiecoördinator zich volledig richten op het verzamelen van actuele informatie, en het opstellen en behouden van een actueel beeld. In juni 2026 staat een training voor alle ICO's gepland.

3 *Versterk de positie van crisiscommunicatie in het CMT door middel van concrete invulling van de rol van strategisch adviseur crisiscommunicatie.*

JIO heeft de organisatie versterkt op het gebied van strategische communicatie. De communicatieadviseur draagt bij aan het duiden van gestructureerd en eenduidig communiceren naar interne- en externe doelgroepen. Daarbij wordt de communicatieadviseur vanuit het CMT waar nodig inhoudelijk ondersteunt om de technische inhoud te duiden voor een juiste communicatieboodschap.

4 *Werk nader uit op welke manier opdrachtgevers tijdens een crisis betrokken worden.*

Om in de koude fase verwachtingen en informatielijnen ten tijde van crisissituaties met opdrachtgevers af te stemmen is de adviseur crisisbeheersing gestart met een gespreksronde langs diverse opdrachtgevers. Er is gesproken met medewerkers die zich bezig houden met crisisbeheersing en BCM van opdrachtgevers Justis en DJI over de processen, ketenafhankelijkheden, afstemmen en samenwerking. De komende periode worden verder gesprekken gepland met overige opdrachtgevers, waaronder DT&V, RvdK en de AP.

5 *Update het handboek crisismanagement Berenschot gaat bij het updaten van het handboek in op een drietal punten:*
- *Maak expliciet welke functies binnen JIO aangesloten moeten worden bij de crisisorganisatie en wie direct geïnformeerd wordt over een crisissituatie.*

- *Werk uit hoe de aansluiting van de crisisorganisatie van JIO op de JenV crisisstructuur in elkaar zit. Denk hierbij aan de informatielijnen van JenV, de invulling van de rol van liaison en de afstemming met de opdrachtgevers van JIO die ook onder JenV vallen*
- *Werk de rol van informatiecoördinator verder uit.*

Op de bovenstaande onderdelen wordt het crisishandboek aangepast waarbij ook leerpunten uit 5.1.2h worden meengenomen. Het nieuwe handboek kan dan worden vastgesteld in het directieoverleg JIO. (planning eind mei 2026)

6 *Werk een jaarplan uit voor opleiden, trainen en oefenen en zorg dat leden van de crisisorganisatie kunnen oefenen in hun rollen*

In 2026 willen wij de crisismanagementstructuur en werkwijze meer eigen gaan maken door middel van opleiden, trainen en oefenen van/met de betrokken collega's. In samenwerking met Berenschot hebben we een kalender opgesteld met deze activiteiten. De kalender is vastgesteld in het directieoverleg van 9 maart 2026

Ter afsluiting
De conclusies en aanbevelingen van het Berenschot evaluatie omvatten voor ons belangrijke nieuwe inzichten en concrete aanknopingspunten om onze crisisaanpak te versterken. Dit is een belangrijke basis om onze crisisaanpak in het geheel verder te professionaliseren. De aanbevelingen vanuit Berenschot nemen wij over en worden in 2026 verder uitgewerkt zoals hierboven beschreven.

Tegelijkertijd heeft in 2026 zich opnieuw een crisissituatie voorgedaan waardoor het CMT was ingesteld. De aanvraag voor een interne evaluatie hiervan is recentelijk opgestart. De bevindingen, conclusies en aanbevelingen daarvan worden eind mei gepubliceerd.