Auditdienst Rijk
Ministerie van Financiën

Rapport van bevindingen gebruikers CIOT 2018 NVWA-IOD, ILT-IOD, Rijksrecherche

Definitief

Colofon

Titel	Rapport van bevindingen gebruikers CIS 2018 NVWA-IOD, ILT-IOD, Rijksrecherche
Uitgebracht aan	Mw. mr. J.G. Vegter
Datum	1 Oktober 2019
Kenmerk	2019-0000148025

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

De minister van Justitie en Veiligheid is conform artikel 8 tweede lid van het Besluit Verstrekking Gegevens Telecommunicatie gehouden "jaarlijks een verslag op te stellen van een audit naar de goede uitvoering van het besluit door aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het Informatiepunt, de arrondissementsparketten en de politiekorpsen, of andere opsporingsdiensten."

De Auditdienst Rijk (ADR) is gevraagd over 2018 een onderzoek uit te voeren naar de maatregelen die afnemers hebben getroffen om tegemoet te komen aan de gemaakte afspraken in de DNO[1] en DAP[2], waaronder de rechtmatigheid van de bevragingen bij drie (bijzondere) opsporingsdiensten. De opsporingsdiensten zijn gebruiker van het geautomatiseerde CIOT informatiesysteem (CIS). Het onderzoek is uitgevoerd bij: de Nederlandse Voedsel en Warenautoriteit (NVWA), de Inspectie Leefomgeving Transport (ILT) en de Rijksrecherche (RR). De rijksrecherche is een opsporingsdienst in de zin van de politiewet 2012. De NVWA en ILT zijn bijzondere opsporingsdiensten in de zin van artikel 2, onderdeel b, van de Wet bijzondere opsporingsdiensten.

De opdrachtgever is de directeur-generaal Rechtspleging en Rechtshandhaving, mw. mr J.G. Vegter. De gedelegeerd opdrachtgever en dagelijks contactpersoon bij DGRR is de heer J. Dobbelaar van de Directie Rechtshandhaving en Criminaliteitsbestrijding (DRC).
Opdrachtnemer namens de ADR is de accountdirecteur BZK/JenV.

De gemaakte afspraken in de DNO en DAP zijn opgenomen in een normenkader (bijlage 2). Het normenkader is voorafgaand aan het onderzoek met de opdrachtgever afgestemd. De normen stellen eisen aan de bij de diensten getroffen maatregelen.

Leeswijzer:
In de vier hoofdstukken die hierna volgen zijn de feitelijke bevindingen van ons onderzoek die niet herleidbaar naar de diensten is beschreven. Hoofdstuk 1 beschrijft de bevindingen van de normen die betrekking hebben op de rechtmatigheid van de bevraging. In hoofdstuk 2 staan de bevindingen voor de (toegangs) beveiliging, hoofdstuk 3 bevat de bevindingen over beheer en monitoring en hoofdstuk 4 beschrijft bevindingen van (geformaliseerde) processen. De verantwoording van het onderzoek volgt in hoofdstuk 5. Hierna is de ondertekening in hoofdstuk 6 en zijn 3 bijlagen opgenomen: de reactie van de opdrachtgever, het normenkader en een overzicht van de geïnterviewden.

[1] Dienstniveau overeenkomst
[2] Dossier Afspraken en Procedures

1 Rechtmatigheid van de CIOT bevragingen moet beter

1.1 Aanwijzing van gebruikers door bevoegd gezag niet expliciet

De norm eist dat alle gebruikers (zowel lokale beheerder als bevrager) door bevoegd gezag zijn aangewezen.

Wij hebben de volgende bevindingen:
Bij één van de drie diensten is beschreven dat gebruikers van het CIS worden aangewezen. Bij deze dienst is voor één van de vier geautoriseerden in 2018 de aanwijzing aanwezig in de vorm van het aanvraagformulier dat door de portefeuillehouder is getekend.

Bij één van de drie diensten is een specifieke functiegroep aangewezen als gebruiker van het CIS. Deze maatregel is niet opgenomen in de handleiding en blijkt ook niet uit MT besluitvorming. Tijdens het locatiebezoek hebben we van een aantal geautoriseerden vastgesteld dat zij tot deze functiegroep behoren.

Bij één dienst zijn geen maatregelen voor de aanwijzing van medewerkers getroffen.

1.2 Externen hebben geen toegang tot CIS, alle gebruikers hebben een passende opleiding gevolgd, BOB middel niet door bevrager opgemaakt

De norm eist dat externen die in aanraking komen met het CIS moeten zijn gescreend. En dat gebruikers van het CIS moeten een daartoe passende opleiding hebben gevolgd en als hij/zij het BOB middel opmaken aangewezen zijn als OA of BOA.

Wij hebben de volgende bevindingen:
Bij geen van de diensten hebben externen toegang tot CIS. Toegang is voorbehouden aan medewerkers in dienst. Bij alle drie de diensten worden potentiële gebruikers of beheerders aangemeld voor de opleiding bij IBO[3]. Het account met een geldig certificaat wordt na de opleiding aangevraagd. Bij geen van de drie diensten wordt het BOB[4] middel door de CIS bevrager opgemaakt.

1.3 5 van de 54 bevragingen in de deelwaarneming voldoen niet aan alle criteria van rechtmatigheid

De norm eist dat een bevraging rechtmatig is als deze door een geautoriseerde gebruiker is uitgevoerd en een bevel in de vorm van een proces-verbaal aanwezig is, getekend door een bevoegde autoriteit op basis van een geldige grondslag (wetsartikel en periode).

Wij hebben een deelwaarneming uitgevoerd op totaal 54 CIS bevragingen in de periode van 1-1-2018 tot 31-12-2018. Bij één dienst zijn in 2018 vier bevragingen gedaan. Bij deze dienst hebben we alle bevragingen in de deelwaarneming betrokken. Bij de andere twee zijn conform de opdrachtbevestiging 25 willekeurige bevragingen gekozen.
Wij hebben de volgende bevindingen:

- alle bevragingen zijn uitgevoerd door geautoriseerde medewerkers;
- bij vijf bevragingen kon de rechtmatigheid van de bevraging niet worden aangetoond:

[3] Informatiepunt Bijzondere Opsporingsonderzoeken
[4] Bijzondere Opsporingsbevoegdheden

- in twee gevallen komt de handtekening niet overeen met de naam van de Officier van Justitie op het document, en is de naam en functie van de ondertekenaar niet bekend;
- in één geval was de geldigheidstermijn van het proces-verbaal verstreken;
- in één geval kon geen getekend proces-verbaal worden getoond;
- in één geval komt de registratie van het strafvorderlijk artikel opgenomen in CIS niet overeen met de onderliggende vordering.

Alle drie de diensten geven aan dat voorafgaand aan de bevraging een controle wordt uitgevoerd. Bij één van de drie is de controle aantoonbaar doordat de dienst een checklist gebruikt waarop de verschillende aspecten en de uitgevoerde controle zijn vastgelegd. De andere twee leggen de controle niet vast.

1.4 Ondertekening op processen-verbaal is niet altijd herleidbaar naar een bevoegde autoriteit

Eén van de eisen voor een geldig proces-verbaal is dat het bevel door een daartoe bevoegde autoriteit is.

Wij hebben de volgende bevindingen:
In onze deelwaarneming zijn we bij 3 van de 25 bevragingen verschillende wijze van ondertekening van het proces-verbaal tegen gekomen. In één geval kon de handtekening door de medewerkers worden herleid naar een daartoe bevoegde autoriteit. De twee andere bevragingen zijn aangemerkt als niet aantoonbaar rechtmatig (zie 1.3) De voorkomende varianten zijn:

1. Getekend 'voor deze' zonder vermelding van de functies van de ondertekenaar;
2. Een handtekening die niet overeenkomt met de naam die staat vermeld, zonder een vermelding in welke hoedanigheid het document wordt getekend;
3. Getekend door iemand waarvan de naam niet te herleiden is.

1.5 Bij twee diensten kan de vastlegging en dossiervorming van de bevragingen beter

De norm eist dat een bevraging herleidbaar is naar het onderliggende (straf)dossier op basis van een identificerend kenmerk. En dat de geautoriseerde ambtenaar een dossier houdt, zodat te allen tijde de rechtmatigheid van de uitgevoerde bevraging tot op dossierniveau kan worden aangetoond.

Wij hebben de volgende bevindingen:
Bij alle drie de diensten wordt een identificerend kenmerk gebruikt die wordt opgenomen in het CIS. Bij één dienst was de gehanteerde systematiek niet eenduidig. Dit bemoeilijkt het leggen van een relatie tussen dossier en bevraging en daarmee dus ook de controle. Het ophalen van de onderliggende bevelen heeft hier ook meer tijd gekost dan bij de twee andere diensten.

Bij alle drie de diensten worden de onderliggende documenten voor de uitgevoerde bevraging bewaard. Twee van de drie hebben dit beschreven.
Bij één dienst zijn voor alle 25 bevragingen de onderliggende documenten conform de werkwijze in Summit [5] opgenomen.

Bij de deelwaarneming komen bij 2 van de 3 diensten de onderliggende documenten in tegenstelling tot de gemaakte afspraken van meerdere digitale locaties.
Bij één kwam dit voor bij 8 van de 25 bevragingen. Hier was de dossiervorming reeds in 2018 onderkend als verbeterpunt en heeft men in werkoverleggen aandacht besteed aan het maken van afspraken voor het dossier van de bevragingen. Bij de andere dienst kwam dit voor bij 2 van de 4 bevragingen.

[5] systeem dat diensten gebruiken voor de opsporing

1.6 Periodieke controle wordt deels uitgevoerd, de aanpak en de wijze van vastlegging varieert

De norm eist dat de beheerder periodiek en aantoonbaar controleert dt de uitgevoerde bevragingen alleen door de juiste personen met een rechtmatige vordering toegang hebben tot het CIS en hierover aan het bevoegd gezag en IBO rapporteert.

Wij hebben de volgende bevindingen:
Bij één dienst is in 2018 het merendeel van de bevragingen door de beheerder zelf uitgevoerd. Een controle achteraf heeft daarom niet plaatsgevonden over 2018. Bij deze dienst is de controle voorafgaand aan het doen van de bevraging vastgelegd in een checklist.

Bij de tweede dienst konden we inzicht krijgen in de door de beheerder uitgevoerde controle over 2018. We konden dit vaststellen omdat naar aanleiding van de controle notities waren vastgelegd om herstelacties te kunnen monitoren. Als de herstelactie is uitgevoerd, wordt de controlebevinding verwijderd. Tijdens het locatiebezoek hebben we gezien dat opmerkingen lang open blijven staan, in mei 2019 waren opmerkingen van begin 2018 nog niet alle opgelost. Bij deze dienst wordt geen rapportage opgesteld over de controle en de bevindingen. De uitkomsten worden indien nodig mondeling gedeeld met de plaatsvervangend portefeuillehouder en leidinggevenden. Er is geen formele rapportage aan het bevoegd gezag.

Bij de derde dienst zijn op uitgevoerde bevragingen geen controles uitgevoerd. En is in de werkinstructie hierover niets beschreven.

2 Afspraken inzake de (toegangs)beveiliging zijn passend gemaakt bij de eigen organisatie

2.1 Inrichting van de werkplekken bij alle drie naar eigen inzicht

De norm eist dat de BOD ingerichte werkplekken waarop het CIS wordt benaderd in een ruimte moeten staan die is geclassificeerd als kritische ruimte[6], deze ruimte mag alleen toegankelijk zijn voor bevoegd personeel en al CIS via een andere locatie te benaderen is, zijn daarvoor maatregelen getroffen.

Wij hebben de volgende bevindingen:
Alle drie de diensten hebben voor het inrichten van de werkplek waarop het CIS wordt benaderd een andere invulling gegeven aan de kwalificatie "kritische ruimte."
Bij één dienst wordt gebruikt gemaakt van een stand alone pc met een dedicated lijn naar het CIS. Deze pc is geplaatst achter een tweede toegangszone voor geautoriseerde medewerkers met specifieke werkzaamheden.
Bij de andere twee diensten is CIS te benaderen via de werkplek.

Bij één dienst is sprake van vier locaties waar CIS bevragingen worden uitgevoerd. Van deze dienst hebben wij één locatie bezocht. Bij twee diensten wordt op één locatie CIS bevragingen gedaan.
Bij alle drie bezochte locaties is de ruimte waar CIS benaderd kan worden ook toegankelijk voor directe collega's anders dan geautoriseerde gebruikers.
Bij één dienst is de werkplek van de beheerders in een afgesloten ruimte waartoe collega's van de afdeling toegang hebben. De bevragers hebben geen werkplek in een afgesloten ruimte. Bij de andere dienst is de werkplek een aparte afsluitbare ruimte en wordt gebruik gemaakt van specifiek beveiligde pc's.

Het benaderen van CIS van een andere locatie dan het kantoor is bij twee van de drie niet mogelijk. Bij de dienst waar dit technisch wel mogelijk is, zijn afspraken gemaakt over tijd en plaats afhankelijk werken (TPAW). Medewerkers kunnen hierover met de teamleider individuele afspraken maken.

2.2 De geheimhoudingsverklaring bij indiensttreding als ambtenaar van kracht

De norm eist dat alle gebruikers die in aanraking komen met CIS een geheimhoudingsverklaring hebben getekend.

Wij hebben de volgende bevindingen:
Bij geen van de diensten is er een separate geheimhoudingsverklaring voor geautoriseerden in CIS in gebruik. De generieke geheimhoudingspassage in de eed/belofte van de Rijksoverheid, aangevuld met een opsporingsbevoegdheid of een veiligheidsonderzoek is bij alle drie als maatregel ingericht.

Bij alle drie de diensten hebben wij de getekende eed of belofteformulieren van tenminste één gebruiker en één beheerder ingezien.

2.3 Bij twee diensten is de vertrouwelijkheid geborgd passend bij het eigen proces

De norm eist dat in geval informatie wordt uitgewisseld bij spoedbevragingen of bij een calamiteiten procedure (zie ook paragraaf 4.4) moet de vertrouwelijkheid van de gegevens zijn gewaarborgd.

[6] DAP Bijlage 10: Aansluitvoorwaarden (bijzondere) opsporings en inlichtingen diensten

Wij hebben de volgende bevindingen:
Bij geen van de drie diensten zijn specifieke maatregelen ingericht om de vertrouwelijkheid van de gegevens bij de spoedprocedure of de calamiteitenprocedure te waarborgen. Bij twee van de drie diensten vindt de uitwisseling van gegevens met een andere Bijzondere Opsporingsdienst (BOD) plaats via het netwerk dat geschikt is voor het delen van gerubriceerde informatie. Bij één dienst voor het uitwisselen bij calamiteiten bij de andere dienst voor spoedbevragingen. Bij de derde dienst was niet bekend welke maatregelen voor de uitwisseling van de informatie zijn getroffen.

2.4 De incidentprocedure is bij één dienst beschreven, twee diensten hebben mondelinge (interne) afspraken

De norm eist dat de dienst afspraken in een (incidenten)procedure moet opnemen over het melden en afhandelen van incidenten. De beheerder registreert, meldt en monitort incidenten t.a.v. CIS.

Wij hebben de volgende bevindingen:
Bij één dienst zijn maatregelen beschreven voor het afhandelen van issues met IBO. De lokale beheerder speelt hierbij een rol. In geval van bijzonderheden wordt de portefeuillehouder door de beheerder geïnformeerd. Niet beschreven is of van incidenten een registratie wordt bijgehouden. In de praktijk verlopen meldingen via de mail.

Twee diensten hebben geen maatregelen beschreven. Eén van de diensten die geen maatregelen heeft beschreven, geeft aan dat incidenten die door IBO Servicedesk worden gemeld, indien nodig aan de gebruikers op locatie worden gecommuniceerd. Hiervan wordt geen registratie bijgehouden. Voor zover geïnterviewden zich konden herinneren, hebben zich in 2018 geen incidenten voorgedaan.

De andere dienst die geen maatregelen heeft beschreven, geeft aan dat voorkomende incidenten t.a.v. CIS worden afgehandeld conform een mondelinge interne werkwijze. Incidenten worden gemeld bij de privacyfunctionaris. Deze dienst heeft een openstaand incident ten aanzien het installeren van een certificaat.

3 De diensten hebben het gebruikersbeheer ingericht op basis van aangeleverde informatie

3.1 De drie diensten hebben een passend gebruikersbeheer ingericht

De norm eist dat de dienst een certificaten beheerproces moet hebben, waarbij de beheerder het gebruik van de certificaten monitort en toezicht houdt op het installeren van certificaat.

Wij hebben de volgende bevindingen:
De drie onderzochte diensten hebben alle een beperkte groep bevragers waaronder enkele beheerders. Het gebruikersbeheerproces is daarom zeer eenvoudig ingericht.

dienst	bevragers	waarvan beheerders	aantal bevragingen 2018
A	4	1	67
B	12	2	249
C	6	3	4

Tabel 1: overzicht per onderzochte dienst van aantal gebruikers, beheerder en bevragingen in 2018

Bij één dienst is een procedure aanwezig voor de beheerder om het gebruikersbeheer uit te voeren. Het verlengen van accounts en certificaten, toezicht en monitoring van accounts zijn hierin niet opgenomen. De andere twee diensten hebben geen procedure beschreven omdat het verloop beperkt is en men gebruik maakt van beschikbare informatie uit de IBO-cursus waardoor een beschreven procedure niet nodig gevonden wordt.

Het toezicht op het gebruik van geldige certificaten vindt bij de drie diensten plaats. Bij alle diensten wordt op basis van de periodieke informatie die door de IBO Servicedesk wordt toegestuurd, inzicht verkregen in de geldigheid van de certificaten en allen kunnen hierop actie ondernemen als het gaat over het intrekken of verlengen van het certificaat. De diensten voeren geen andere (pro)actieve beheeractiviteiten uit voor certificaten.

Voor de installatie van het certificaat maken beheerders gebruik van de in CIS beschikbare beschrijving. Alle 3 hebben hun eigen werkwijze voor het installeren van certificaten.
Bij één dienst worden bevragingen op vier locaties uitgevoerd. Hiervoor wordt installatie van certificaten op afstand begeleid.
Bij één dienst wordt het certificaat door de ICT dienstverlener uitgevoerd en verbonden aan het persoonlijke profiel van de medewerker. Bij één dienst geeft de beheerder aan aanwezig te zijn bij de installatie van het certificaat.

3.2 Blokkeren van toegang bij verandering van functie of vertrek van een medewerker gebeurt op basis van informatie van de IBO Servicedesk

De norm eist dat bij het verlaten van de dienst of wijziging van de werkzaamheden van een bevrager de lokale beheerder zorgdragen dat via IBO toegang tot het CIS wordt beëindigd.

Wij hebben de volgende bevindingen:
Eén dienst heeft het beëindigen van de toegang tot CIS beschreven.
Bij geen van de drie diensten wordt actief de toegang beëindigd bij het verlaten van de dienst of bij wijziging van de werkzaamheden. Informatie van de IBO Servicedesk is aanleiding om accounts te blokkeren.

Bij één dienst geven beheerders aan dat zij accounts inactief hebben gemaakt. Echter, uit het overzicht van actieve accounts in CIS blijkt dat er vier accounts op staan van medewerkers die geen beheerder/bevrager meer zijn en waarvan het account niet is gedeactiveerd. Deze accounts komen niet voor op het overzicht van geldige certificaten dat wordt gebruikt bij de controle. Deze accounts kunnen door het ontbreken van een geldig certificaat niet worden gebruikt.

3.3 Niet persoonsgebonden accounts komen niet voor

De norm eist dat een account en het certificaat persoonsgebonden moeten zijn.

Wij hebben de volgende bevindingen:
Tijdens het locatiebezoek is vastgesteld dat accounts en certificaten persoonsgebonden zijn. Alle drie diensten geven aan dat dit ook zo wordt gebruikt. In het CIOT rapport Overzicht bevragers over 2018 komen bij de drie onderzochte diensten niet persoongebonden accounts niet voor.

4 Processen zijn deels beschreven, de detaillering varieert sterk en procedures zijn voor een beperkt deel formeel vastgesteld.

4.1 Eén van de drie diensten heeft een formeel vastgestelde procedure met een passende detaillering

De norm vereist dat een BOD een geformaliseerd proces moet hebben waarin de afspraken conform de DNO[7] en DAP[8] betreffende CIOT Informatiesysteem zijn opgenomen.

Wij hebben de volgende bevindingen:
Bij één dienst is er een in 2018 geformaliseerde procedure aanwezig, de mate van detaillering sluit aan bij gestelde eisen en het proces is conform de beschrijving ingericht.

Bij twee diensten blijkt niet of de aanwezige beschrijvingen door het management zijn geformaliseerd.
Van deze twee zijn bij één niet alle afspraken opgenomen. Bovendien dateert de beschrijving van vér voor de DNO en DAP van 2018 namelijk uit 2014. In 2018 heeft hebben zij aandacht geschonken aan dossiervorming door separate afspraken te maken met de gebruikers van CIS. Deze zijn opgenomen in de notulen van hun reguliere overleg.
Bij de andere dienst is deze beschrijving een werkinstructie die summier een aantal onderwerpen beschrijft. Daarbij is het verloop van een aanvraag voor een bevraging in een stroomdiagram opgenomen. Dit diagram is niet volledig en bevat te weinig detail om af te leiden welke activiteit wordt uitgevoerd, op welke wijze en hoe de activiteit wordt vastgelegd. Deze dienst heeft in 2018 een selfassesment ontwikkeld, met als doel inzicht te verkrijgen in de stand van zaken ten aanzien van processen rondom CIS bevragingen.

4.2 Beschikbaar materiaal kan eenvoudig worden verwerkt tot formele procedures

Bij een aantal normen wordt de eis gesteld dat er geformaliseerde procedures zijn.

Bij het onderzoek hebben wij gezien dat voor een aantal processen en (beheers)activiteiten door alle drie diensten gebruik wordt gemaakt van door IBO beschikbaar gestelde informatie. Bijvoorbeeld in de vorm van cursusmateriaal, een gebruikershandreiking CIOT informatiesysteem of informatie ten behoeve van de periodieke controle van certificaten. In deze informatie is een aantal van de afspraken in de overeengekomen met de normen (en dus met DNO en DAP afspraken) opgenomen. Met een beperkte aanpassing van voor de dienst specifieke maatregelen en een akkoord van de leiding, kan de reeds beschikbare informatie gebruikt worden als voor de dienst hanteerbare, procedures.

4.3 Eén dienst heeft een formeel vastgestelde toegangsprocedure

De norm vereist dat er een geformaliseerde procedure is voor het verkrijgen van toegang tot het CIS die alle stappen in het proces beschrijft.

Wij hebben de volgende bevindingen:

[7] Dienstniveau overeenkomst
[8] Dossier Afspraken en Procedures

Bij één dienst is er een geformaliseerde toegangsprocedure aanwezig die alle stappen beschrijft. De twee andere diensten hebben de te volgen stappen niet volledig beschreven. Onderdelen die wel beschreven zijn, zijn niet formeel vastgesteld.

4.4 De inrichting rondom spoedbevragingen en calamiteiten verschilt sterk

De norm vereist dat de dienst een calamiteitenprocedure heeft bij onverwachte interruptie van het CIS en een procedure voor spoedbevragingen.

Wij hebben de volgende bevindingen:
Een inrichting van spoedbevragingen[9] en calamiteiten[10] is niet bij alle drie diensten aanwezig. Eén dienst hanteert beide procedures, één dienst heeft geen calamiteitenprocedure en één dienst heeft geen spoedprocedure omdat volgens deze dienst spoedbevragingen niet voorkomen.

De dienst die beide procedures hanteert, heeft zowel voor bevragingen bij calamiteiten als in geval van spoedbevragingen maatregelen beschreven en afspraken gemaakt. Bij calamiteiten is in 2018 bij deze dienst gebruik gemaakt van de afspraken met de collega BOD. Bij bevragingen die een collega BOD uitvoert, is deze collega BOD verantwoordelijk. In de logging informatie is zichtbaar om welke bevragingen het gaat. Door de registratie van alle binnengekomen vragen in een checklist[11] is er bij deze dienst inzicht in de bevragingen die naar de collega BOD zijn toegestuurd.

De dienst die alleen spoedbevragingen onderscheidt, heeft de afspraken daarover zodanig vastgelegd dat deze tegemoet komen aan de afspraken met IBO.

De dienst die geen spoedbevragingen doet, maar wel een calamiteitenprocedure heeft, heeft daarover afspraken met de FIOD. Deze afspraken zijn niet beschreven.

Uit de bevragingen in de deelwaarneming kon niet worden afgeleid of sprake was van een spoedbevraging.

4.5 De no-hit procedure is deels beschreven maar wordt niet gebruikt

De norm vereist dat voor 'No hits' de dienst een speciale procedure voor registratie en verdere behandeling moet hebben geïmplementeerd.

Wij hebben de volgende bevindingen:
Twee van de drie diensten hebben een no-hit procedure beschreven. De diensten geven aan dat deze niet wordt gebruikt. De derde dienst heeft geen no-hit procedure.

In de deelwaarneming is in één geval een ingevuld no hit formulier aangetroffen, maar was de no-hit bevraging niet uitgevoerd. Deze dienst geeft aan dat ook andere informatiebronnen worden geraadpleegd om informatie te verkrijgen voor de onderzoeken.

---

[9] Spoedbevraging : Bevraging die z.s.m. wordt uitgevoerd, het onderliggend dossier wordt later in orde gebracht.
[10] Calamiteitenprocedure : Voorziening om bevragingen te kunnen doen als de eigen verbinding met CIS niet functioneert.
[11] op de checklist worden de eisen dat het bevel van daartoe bevoegde autoriteit afkomstig is en de basis van de grondslag geregistreerd

5 Verantwoording onderzoek

5.1 Werkzaamheden en afbakening

De met de opdrachtgever overeengekomen werkzaamheden zijn uitgevoerd conform de opdrachtbevestiging 2019-0000008110 d.d. 15 januari 2019.
Het onderzoek heeft zich gericht op de opzet en bestaan in 2018 van gemaakte afspraken in de DNO en DAP voor zover die betrekking hebben op het doen van CIS bevragingen.
Voor het onderzoek hebben wij één locatie van de geselecteerde diensten bezocht. Voorafgaand aan het bezoek hebben wij een prepared by client lijst opgemaakt. Deze hebben wij gebruikt als leidraad voor het bezoek. Voorafgaand aan het locatiebezoek bij de drie diensten in april 2019 hebben we een deel van de gevraagde documentatie ontvangen en hebben we deze bestudeerd.
Op de locatie heeft bij elke dienst een gesprek plaatsgevonden met de verantwoordelijke portefeuillehouder en de beheerder. Bij één dienst was op het moment van het onderzoek geen actieve bevrager aanwezig, de beheerder kon hier de noodzakelijke informatie geven. Bij de twee andere diensten is gesproken met een beheerder, bij één heeft deze in 2018 ook bevragingen uitgevoerd.
Na het voeren van de gesprekken in de eerste helft van de dag, is de tweede helft van de dag besteed aan het uitvoeren van een deelwaarneming van 25 bevragingen in de periode van 1-1-2018 tot en met 31-12-2018. Bij één dienst zijn in 2018 4 bevragingen gedaan. Deze zijn allen in de deelwaarneming betrokken. Hierdoor is het totaal aantal bevragingen in de deelwaarneming 54.
Het onderzoek heeft geen betrekking gehad op informatiebeveiligingsmaatregelen van het CIS of de dienst zelf noch op (wettelijke) privacy vereisten bij het gebruik van het CIS door de dienst.

Op basis van documentenanalyse, interviews en waarnemingen is per norm de bevinding in een matrix opgenomen. Hieraan is per norm een evaluatie van de inrichting van de maatregel vermeld. De evaluatie van de deelwaarneming is eveneens onderdeel van deze matrix. De matrix is in het kader van hoor en wederhoor met de diensten afgestemd ten aanzien van feitelijke onjuistheden in mei 2019 en is na verwerking van de opmerkingen in juni 2019 voor akkoord aangeboden. De goedgekeurde matrix is de basis voor de concept rapportage aan de (gedelegeerd) opdrachtgever.

De conceptrapportage is op 9 juli 2019 aangeboden en besproken met de (gedelegeerd) opdrachtgever. Deze draagt zorg voor afstemming met de onderzochte diensten en een reactie die integraal is opgenomen in de rapportage (zie bijlage 1)

Het onderzoek is uitgevoerd door mw. mr. J.T.N. Tjin A Tsoi RE en dhr. ing H.J. de Beuze RE. De opdrachtgerichte kwaliteitsbeoordeling is uitgevoerd door dhr. G. van Huuksloot RE RA.

5.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd overeenkomstig NOREA Richtlijn 4401 "Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie.

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd. Indien aanvullende werkzaamheden zouden zijn verricht of indien er een assurance-opdracht zou zijn uitgevoerd, zouden wellicht andere onderwerpen zijn geconstateerd en gerapporteerd.

Tevens verwijzen wij naar het Audit Charter van de ADR die de algemene uitgangspunten bevat voor de uitoefening van de interne auditfunctie bij de rijksdienst.

5.3 Verspreiding rapport

De opdrachtgever, mw. mr J.G. Vegter, dgRR Directeur generaal Rechtspleging en Rechtshandhaving is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

6 Ondertekening

Den Haag, 1 oktober 2019

Bijlage 1 Managementreactie van de opdrachtgever

Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Auditdienst P,J
T.a.v
Postbus 20201
2500 EE Den Haag

Minister van Justitie en Veiligheid
DGRR DRC-GC

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
[redacted]

T 070 370 68 89
F 070 370 79 39

Ons kenmerk
2688391

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts een zaak in uw brief behandelen

Datum 25 september 2019
Onderwerp Managementreactie op audit CIOT afnemers 2018

Geachte [redacted]

De minister van Justitie en Veiligheid is conform artikel 8 tweede lid van het Besluit Verstrekking Gegevens Telecommunicatie gehouden jaarlijks een verslag op te stellen van een audit naar de goede uitvoering van het besluit door aanbieders van openbare telecommunicatiediensten of -netwerken, het informatiepunt, de arrondissementsparketten en de politiekorpsen, of andere opsporingsdiensten. Ik heb u derhalve gevraagd onderzoek te doen naar de rechtmatigheid van de bevraging bij de afnemers Rijksrecherche, ILT-IOD en NVWA-IOD.

Ik heb kennisgenomen van het concept 'Rapport van bevindingen gebruikers CIOT 2018 NVWA-IOD, ILT-IOD, Rijksrecherche". Ik stel vast dat u met succes inzicht heeft kunnen verschaffen in de rechtmatigheid van de bevragingen. De door u onderzochte afnemers hebben mij meegedeeld zich in de bevindingen te herkennen en mogelijke verbeteringen ter hand te zullen nemen.

Uw bevindingen uit dit onderzoek zullen betrokken worden bij het brede verslag dat opgesteld zal worden naar aanleiding van dit onderzoeksrapport, waarin tevens de bevindingen uit de overige lopende onderzoeken, zoals naar CIOT beheer, betrokken zullen worden, opdat een integrale beoordeling gemaakt kan worden.

Met vriendelijke groet,

[redacted]

Bijlage 2 Normenkader CIS afnemers 2018

Volgnr.	Norm
	ALGEMEEN
1	De BOID heeft een geformaliseerd proces waarin de afspraken conform de DNO[12] en DAP[13] betreffende CIOT Informatiesysteem (CIS) zijn opgenomen.
2	De door de BOID ingerichte werkplekken waarop het CIS wordt benaderd voldoet aan de volgende eisen: -de ruimte is geclassificeerd als kritische ruimte[14] -alleen bevoegd personeel heeft toegang tot deze ruimte -als CIS via een andere locatie te benaderen is, zijn daarvoor maatregelen getroffen. (bijvoorbeeld thuiswerken is pas toegestaan als er een specifiek certificaat door de medewerker is behaald of alleen met medeweten van de leidinggevende is toegestaan).
3	Er is een geformaliseerde toegangsprocedure voor het verkrijgen van toegang tot het CIS die alle stappen in het proces beschrijft.
4	De organisatie heeft een certificaten beheerprocedure. -Beheerder monitort het gebruik van certificaten -Beheerder houdt toezicht op het installeren van een certificaat met hoog beveiligingsniveau en dat gebruiker een persoonlijk wachtwoord toevoegt.
	GEBRUIKERS
5	Alle gebruikers (zowel lokale beheerder als bevrager) zijn door bevoegd gezag aangewezen.
6	Alle gebruikers van het CIS hebben een daartoe passende opleiding gevolgd en zijn aangewezen OA of BOA, als hij/zij het BOB middel opmaakt. Externen die in aanraking komen met het CIS zijn gescreend.
7	Alle gebruikers die in aanraking komen met CIS hebben een geheimhoudingsverklaring getekend.
8	Een account en certificaat is persoonsgebonden en wordt ook zo gebruikt.
9	Het doen van een bevraging in CIS kan alleen door daartoe aangewezen gebruikers op basis van een bevel[15] van een daartoe bevoegde autoriteit[16] en op basis van een geldige grondslag[17].
10	Een bevraging heeft altijd een identificerend kenmerk op basis waarvan een eenduidiger relatie kan worden gelegd met het onderliggende (straf)dossier. Van een bevraging wordt daarnaast in CIS vastgelegd: • Bevoegde autoriteit; • Kenmerk; • Organisatie eenheid/ opsporingsteam • Rechtsgrondslag
11	De geautoriseerde ambtenaar houdt dossier, zodat te allen tijde de rechtmatigheid van de uitgevoerde bevraging tot op dossierniveau kan worden aangetoond.

[12] Dienstniveau overeenkomst
[13] Dossier Afspraken en Procedures
[14] DAP Bijlage 10: Aansluitvoorwaarden (bijzondere) opsporings- en inlichtingen diensten
[15] *Een bevel is een vordering van een bevoegde autoriteit om een verzoek te doen in het kader van een onderzoek van telecommunicatie, met daarbij bepaald op welke rechtsgrond lag die bevel toepassing heeft*
[16] *Het verzoek van de bevoegde autoriteit is op papier (in handen of fax) of elektronisch (e-mail) bij de geautoriseerde ambtenaar bezorgd bijvoorbeeld Proces verbaal OA voor artikel 126 na, 126 ua en 126 zi ; OvJ voor artikel 126n 126 u, 126 n en 126 zi WvSv*
[17] *Artikel 126 na, 126 ua, 126 zi 126n 126 u 126 n en 126 zi WvSv (zie toelichting)*

12	Er is een calamiteitenprocedure voor spoedbevragingen bij onverwachte interruptie van het CIS zodat de voor langere tijd niet beschikbaar is. De vertrouwelijkheid van de gegevens zijn gewaarborgd.
13	Voor 'No hits' is een speciale procedure voor registratie en verdere behandeling geïmplementeerd.
	Lokaal BEHEER
14	De beheerder heeft een gebruikersbeheerproces voor de CIS. (hierin is beschreven het aanvragen van gebruikersaccounts en het uitreiken van accounts /certificaten, installeren en verlengen of intrekken van accounts/certificaten).
15	Bij het verlaten van de dienst of wijziging van de werkzaamheden zorgt de lokale beheerder dat via IBO toegang tot het CIS wordt beëindigd.
16	De beheerder controleert aantoonbaar en periodiek dat de uitgevoerde bevragingen alleen door de juiste personen met een rechtmatige vordering toegang hebben tot het CIS en rapporteert hierover aan het bevoegd gezag en IBO.
17	De organisatie heeft afspraken inzake het melden en afhandelen van incidenten opgenomen in een (incidenten)procedure. De beheerder registreert, meldt en monitort incidenten t.a.v. CIS.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00