Rapportage CIOT

2018

Concernaudit
Definitief
Versie 1.0
Versie datum 28 april 2020
Rubricering Vertrouwelijk

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	05 november 2019	Initiële versie
0.4	18 november 2019	Conceptversie t.b.v. team review
0.5	28 november 2019	Opmerkingen team review verwerkt
0.6	02 december 2019	Voorlopig concept
0.9	17 december 2019	Review coördinator CA verwerkt
0.99	14 januari 2020	wederhoor met PH CIOT verwerkt

Distributie

Versie	Verzend datum	Afdeling / Functie
0.9	17 december 2019	PH CIOT
0.9	17 december	Politiechef Landelijke Eenheid
0.99	16 januari 2020	Lid Korpsleiding
1.0	28 april 2020	Lid Korpsleiding

Inhoudsopgave

1. Managementsamenvatting

Concernaudit heeft een onderzoek uitgevoerd naar de CIS-bevragingen door de politie in 2018. Het doel van deze compliance audit is inzicht te geven in welke mate de politie voldoet aan wet- en regelgeving en afspraken verbonden aan de uitvoering van de bevraging van klantgegevens van telecom- en internetbedrijven via het CIS-systeem.

De centrale onderzoeksvraag van deze audit is:

Zijn de CIOT-bevragingen in 2018 uitgevoerd conform geldende wet- en regelgeving en de afspraken verbonden aan de uitvoering van de bevraging van klantgegevens van telecom- en internetbedrijven via het CIS-systeem?

Het antwoord op de onderzoeksvraag luidt:

Op een groot aantal punten wordt voldaan aan geldende wet- en regelgeving en de vastgelegde afspraken met het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Op enkele punten zijn afwijkingen geconstateerd. Hieronder wordt per organisatieonderdeel kort een aantal belangrijke bevindingen met aanbeveling weergegeven. Voor een volledig en meer gedetailleerd beeld verwijzen wij naar hoofdstuk vier van dit rapport.

Eenheden

Wij stellen vast dat de korpschef de aanwijzing van alle actieve gebruikers ongeveer twee maal per jaar achteraf bekrachtigt via een lijst met alle actieve gebruikers. De nationale coördinatoren CIOT (NCC) hebben aangegeven dat er een nieuw voorstel ligt om de aanwijzing van nieuwe beheerders en bevragers vooraf door de korpschef te laten plaatsvinden. Dit voorstel loopt via de lijn van de portefeuillehouder naar de KC. De NCC's geven aan nog geen terugkoppeling op het voorstel te hebben gehad. We bevelen aan om prioriteit te leggen bij het accepteren, formaliseren en implementeren van de werkwijze om geautoriseerde ambtenaren aan te wijzen voorafgaand aan het uitvoeren van bevragingen in het CIS.

Eén beheerder heeft in 2018 de beheerdersautorisaties in het CIS gekregen en werkzaamheden uitgevoerd als beheerder voordat diegene de beheerderscursus heeft gevolgd. De NCC geven aan dat de werkzaamheden uitgevoerd zijn onder begeleiding van een ervaren beheerder. Daarnaast heeft één beheerder in de loop van 2018 autorisaties als beheerder gekregen, maar heeft de beheerderscursus pas begin 2019 gevolgd. De NCC geeft aan dat de betreffende beheerder geen werkzaamheden heeft verricht tot na het volgen van de vereiste opleiding. Ook heeft een bevrager bevragingen in CIS uitgevoerd voordat diegene de bevragerscursus heeft gevolgd. We adviseren in de nieuwe procedure een werkwijze op te nemen waarmee is geborgd dat nieuwe beheerders en bevragers pas na het voltooien van de beheerdersopleiding beschikking krijgen over beheerdersautorisaties.

Interceptie en Sensing

Een medewerker heeft bevragingen uitgevoerd buiten de periode dat diegene opsporingsbevoegd is. Het account is inmiddels geblokkeerd. We bevelen aan op korte termijn een controle op de opsporingsbevoegdheid in te richten binnen het CIOT-proces.

Bij I&S zijn drie aanvragen niet teruggevonden, omdat de mailbox waarin de (spoed) aanvragen binnenkomen is geschoond voorafgaande aan de uitvoering van de audit 2018. We adviseren in de nieuwe procedure een bewaartermijn voor de onderliggende documenten van een bevraging op te nemen tot na behandeling van het auditrapport door de Minister in de Tweede Kamer over het betreffende tijdsvlak.

112-centrale

De 112-centrale voert ten behoeve van de meldkamers van de eenheden en de 112-centrale ook CIS-bevragingen uit. Deze bevragingen betreffen situaties waarin sprake is van noodhulp of dusdanig misbruik van het 112-nummer dat de bereikbaarheid van de 112-centrale of de meldkamers in gevaar komt.

De minister heeft in een schrijven van 14 november 2018 geconstateerd dat de 112-meldkamer in uitzonderlijke gevallen CIS-bevragingen uitvoert ten behoeve van noodhulp, terwijl hiervoor de wettelijke grondslag ontbreekt. Naar verwachting zou in april 2019 een nieuw 112-platform worden opgeleverd, waarin de directe aanlevering van NAWP-gegevens vanuit de telecomaanbieders technisch is geregeld.

De 112-centrale maakt gebruik van acht groepsaccounts. Door het gebruik van groepsaccounts is het voor ons niet onomstotelijk vast te stellen of de bevragers, die binnen de 112-centrale in 2018 een bevraging in het CIS hebben uitgevoerd, daadwerkelijk opsporingsbevoegd zijn. De 112-centrale houdt wel extracomptabel een administratie bij waarin een werknemer aan een CIOT ID wordt gekoppeld. Door verschillende omstandigheden was het 112-platform ultimo 2020 nog niet gerealiseerd en derhalve niet geïmplementeerd. We bevelen aan om een spoedige realisatie van het platform te blijven ondersteunen.

Deelwaarnemingen

We hebben deelwaarnemingen uitgevoerd binnen de eenheden waar we op basis van de data-analyse de grootste risico's verwachtten. De belangrijkste bevindingen zijn hieronder weergegeven:

- We constateren dat er in zes gevallen geen dossier is aangetroffen. Dit betreffen o.a. vijf posten van de 112-centrale. De 112-centrale geeft hierbij als toelichting dat bij een grote storm de centrale minder goed bereikbaar was. Er heeft toen vanuit de 112-centrale een terugbelactie plaats gevonden. Dit is niet in de extracomptabele administratie vastgelegd.
- Bij zes posten is de aanvraag voor een bevraging vanuit een andere Bijzondere Opsporingsdienst gedaan. We hebben de opsporingsbevoegdheid van de aanvragers niet kunnen toetsen aangezien zij niet tot de politieorganisatie behoren.

2. Inleiding

Dit hoofdstuk geeft in paragraaf één en twee de aanleiding en doelstelling van de audit CIOT 2018 weer. De scope en de onderzoeksmethode worden in paragraaf drie en vier toegelicht.

2.1 Aanleiding

De politie kan via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) klantgegevens van telecomaanbieders opvragen. De politie gebruikt deze informatie voor opsporingshandelingen en bij noodhulpverlening door de meldkamers.

Telecom- en internetbedrijven zijn wettelijk verplicht om persoonlijke gegevens die bij IP-adressen, telefoonnummers en e-mailadressen horen, beschikbaar te stellen aan het CIOT. Namens de minister van Justitie en Veiligheid zorgt het CIOT ervoor dat deze informatie, op verzoek, aan de politie verstrekt wordt. Hiertoe beheert het CIOT een geautomatiseerd CIOT-informatiesysteem (CIS) voor telefoon- en internetgegevens.
Regels voor de verstrekking van gegevens door aanbieders van openbare telecommunicatienetwerken en –diensten, met het oog op het strafvorderlijk onderzoek van telecommunicatie zijn vastgelegd in het Besluit verstrekking gegevens telecommunicatie.

In artikel 8 van dit besluit is bepaald dat de minister van Justitie en Veiligheid jaarlijks een verslag opstelt van een audit naar de goede uitvoering van dit besluit door de aanbieders van openbare telecomdiensten, van openbare telecommunicatienetwerkdiensten, van openbare telecommunicatienetwerken, het informatiepunt, de arrondissementsparketten en de politie, of andere opsporingsdiensten.
Daarbij worden ten minste de volgende onderwerpen behandeld:

a) de werking van het systeem;
b) de kwaliteit van de verstrekking van gegevens;
c) de bevraging van gegevens.

Voor de politie geldt dat de jaarlijkse audit naar de vaststelling van de goede uitvoering van het Besluit sinds 2013 onder verantwoordelijkheid van de korpschef van de politie valt. De korpschef heeft hiervoor de afdeling Concernaudit opdracht gegeven tot het uitvoeren van een audit over het kalenderjaar 2018.

2.2 Doelstelling en onderzoeksvraag

Het doel van deze compliance audit is inzicht te geven in welke mate de politie voldoet aan wet- en regelgeving en afspraken gesteld aan de uitvoering van de bevraging van klantgegevens van telecom- en internetbedrijven via het CIS-systeem. De periode van onderzoek is 2018.

De centrale onderzoeksvraag van deze audit is:

Zijn de CIOT-bevragingen in 2018 uitgevoerd conform geldende wet- en regelgeving en de afspraken gesteld aan de uitvoering van de bevraging van klantgegevens van telecom- en internetbedrijven via het CIS-systeem?

2.3 Scope van de audit

De scope van het onderzoek betreft de bevragingen van klantgegevens van telecom- en internetbedrijven via het CIS-systeem uitgevoerd in het jaar 2018 door de politie. Het gaat hierbij om het vaststellen of de bevragingen door politieambtenaren in het CIS hebben plaatsgevonden volgens geldende wetgeving en lopende afspraken met het CIOT.

De externe wet- en regelgeving die voor dit onderzoek van toepassing is, betreft:
- Besluit verstrekking gegevens telecommunicatie geldend van 28-12-2016 tot en met heden.

De afspraken verbonden aan de uitvoering van de bevraging van klantgegevens van telecom- en internetbedrijven via het CIS-systeem zijn vastgelegd in:

- Dossier afspraken en procedures (DAP) tussen CIOT en de politie versie 3.0 d.d. 14 maart 2013.
- Service level agreement (SLA) tussen CIOT en politie versie 3.0 d.d. 14 maart 2013.

Buiten de scope valt de beoordeling van de rechtmatigheid van de aanvraag op basis van het onderliggende bevel of een proces-verbaal.

Het onderzoek is uitgevoerd bij de eenheden:

- Midden-Nederland
- Zeeland-West-Brabant
- Limburg
- Landelijke Eenheid

Gezien de afwijkende werkwijze van de organisatieonderdelen Interceptie & Sensing en de 112-centrale, zijn deze onderdelen ook bezocht voor een interview en het uitvoeren van deelwaarnemingen.

2.4 Onderzoeksaanpak

De audit is uitgevoerd door Concernaudit in samenwerking met auditoren uit de auditfuncties binnen de eenheden van de politie.

Voor de uitvoering van ons onderzoek hebben we gebruik gemaakt van een toetsingskader. Dit toetsingskader is vastgesteld aan de hand van de regels en afspraken zoals vastgelegd in het besluit verstrekking gegevens telecommunicatie, het SLA en het DAP.

In tegenstelling tot voorgaande jaren, is geen onderzoek verricht naar alle eenheden. In plaats daarvan is een selectie gemaakt van eenheden waar we over 2018 de grootste risico's. verwachtten, op basis van een risicogerichte benadering. Hiervoor hebben we gebruik gemaakt van data-analyse. Daarbij zijn de volgende selectiecriteria gehanteerd:

- Eenheden met nieuwe beheerders en nieuwe bevragers.
- Bevragingen door eenheden uitgevoerd buiten kantoortijden.
- Een uitgevoerde trendanalyse op aantal bevragingen binnen eenheden en organisatieonderdelen.
- Bevragers met een beperkt aantal bevragingen.
- Overzicht materiële fouten binnen eenheden en organisatieonderdelen uit de audit 2017.
- Geautoriseerde bevragers die in 2018 geen bevraging hebben gedaan.

Bij de geselecteerde eenheden zijn interviews met een beheerder en een bevrager uitgevoerd. Tevens zijn in de geselecteerde eenheden aanvullend deelwaarnemingen uitgevoerd, ter validatie van de interviewuitkomsten.

2.5 Opvolging onderzoek 2017

In 2017 is een procesaudit uitgevoerd met betrekking tot het proces CIOT. In die audit is een aantal aanbevelingen gedaan. In hoofdstuk 5 geven we aan in hoeverre opvolging is gegeven aan deze aanbevelingen. Voor deze aanbevelingen hebben we aanvullende interviewvragen gesteld aan de nationale coördinatoren en in de eenheden aangezien het proces CIOT in de audit 2018 buiten de scope van het onderzoek valt.

3. Context

Dit hoofdstuk beschrijft de context waarbinnen de diverse organisatieonderdelen van de politie CIS-bevragingen uitvoeren.

3.1 Eenheden

De politie kan via het CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) actuele klantgegevens opvragen van telecomaanbieders. De politie is bevoegd deze informatie op te vragen in het kader van opsporingshandelingen. Het CIOT stelt deze gegevens beschikbaar via het CIOT Informatie Systeem (CIS). Toegang tot het CIS wordt door het CIOT verleend aan hiervoor geautoriseerde medewerkers bij de politie (CIS-bevragers), via hiertoe door CIOT geautoriseerde werkplekken.

Een CIS-bevrager biedt aan de hand van een verzoek van een opsporingsbevoegde de bevraging aan het CIS aan en verstrekt vervolgens het ontvangen antwoord aan de aanvrager.

De CIS-bevragingen voor de regionale eenheden worden uitgevoerd binnen Gemeenschappelijke Bijzondere Opsporing Bevoegdheid-kamers (GBK) per eenheid. Bij de Landelijke Eenheid worden de reguliere bevragingen uitgevoerd bij de afdeling Operationele Informatieverwerking (OIV).

3.2 Interceptie & Sensing

De afdeling Interceptie & Sensing (I&S) van de Landelijke Eenheid verzorgt de spoedbevragingen buiten kantoortijden en de no hit-doorbevragingen van alle regionale eenheden. Ook is de afdeling I&S het uitwijkpunt bij landelijke calamiteiten. Deze CIS-bevragingen vinden hun basis in het wetboek van strafvordering (WvSv). Door haar specifieke werkzaamheden wijkt I&S af van de werkwijze van andere eenheden. Om deze reden worden de bevindingen inzake I&S separaat weergegeven.

3.3 112-centrale

De 112-centrale voert ten behoeve van de meldkamers van de eenheden en de 112-centrale ook CIS-bevragingen uit. Deze bevragingen betreffen situaties waarin sprake is van noodhulp of dusdanig misbruik van het 112-nummer dat de bereikbaarheid van de 112-centrale of de meldkamers in gevaar komt (bijvoorbeeld de zogenoemde ‘broekzakbellers’).

De minister heeft in een schrijven van 14 november 2018 geconstateerd dat de 112-meldkamer in uitzonderlijke gevallen CIS-bevragingen uitvoert ten behoeve van noodhulp, terwijl hiervoor de wettelijke grondslag ontbreekt. De reden dat het CIOT voor noodhulpdoeleinden wordt bevraagd, is gelegen in het feit dat telecomaanbieders weliswaar wettelijk verplicht zijn om de NAWP-gegevens van hun klanten aan de landelijke 112-meldkamer aan te leveren conform artikel 11.10 lid 3 TW, maar dat de directe aanlevering soms nog op technische problemen stuit. Het CIOT-systeem, waar elke 24 uur door nagenoeg alle telecomaanbieders de NAWP-gegevens van klanten gekoppeld aan het telefoonnummer worden aangeleverd, biedt dan een uitwijk. De politie mag ten behoeve van de noodhulp dus wel rechtmatig over de gegevens beschikken, maar daarvoor niet het CIOT systeem raadplegen. Door de toegang tot het CIS is het mogelijk om toch de noodzakelijke gegevens te krijgen ten behoeve van noodhulp en het bovengenoemde misbruik van het 112-nummer.

Naar verwachting zou in april 2019 een nieuw 112-platform worden opgeleverd, waarin de directe aanlevering van NAWP-gegevens vanuit de telecomaanbieders technisch is geregeld.
Dit overwegende heeft de minister toestemming verleend om de bestaande werkwijze voort te zetten. Dat wil zeggen dat de landelijke 112-meldkamer in uitzonderingsgevallen voor het verlenen van snelle en adequate noodhulp, voor de duur van een halfjaar vanaf 14 november 2018 of zoveel eerder tot aan de oplevering van het nieuwe 112 platform, het CIS mag bevragen.

4. Bevindingen en aanbevelingen

In dit hoofdstuk worden de bevindingen en aanbevelingen van de uitgevoerde audit weergegeven. Hierbij wordt onderscheid gemaakt tussen de eenheden, I&S en de 112-centrale. Tevens zijn in paragraaf 4.4 de bevindingen uit de deelwaarnemingen opgenomen.

4.1 Eenheden

4.1.1 Aanwijzing door de korpschef

De korpschef (KC) wijst geautoriseerde ambtenaren aan die bevragingen in het CIS mogen uitvoeren.

Bevinding
We hebben vastgesteld dat de korpschef de aanwijzing van alle actieve gebruikers (CIS-bevragers en beheerders) ongeveer twee maal per jaar achteraf bekrachtigt via een lijst met alle actieve gebruikers. In de audit CIOT 2017 was dit reeds een bevinding. De nationale coördinatoren CIOT (NCC) hebben aangegeven dat er een nieuw voorstel ligt om de aanwijzing van nieuwe beheerders en bevragers vooraf door de korpschef te laten plaatsvinden. Hierin is reeds de bevoegdheid gemandateerd aan de sectorhoofden. De werkwijze is opgenomen in de nieuwe procedure CIOT die in het reguliere besluitvormingsproces wordt geformaliseerd.

Aanbeveling
We bevelen aan om prioriteit te leggen bij het accepteren, formaliseren en implementeren van de werkwijze om geautoriseerde ambtenaren aan te wijzen voorafgaand aan het uitvoeren van bevragingen in het CIS.

4.1.2 Beheerderscursus

CIOT geeft een cursus voor lokale beheerders over het beheer van CIS. Lokale beheerders dienen deze cursus gevolgd te hebben voordat zij als CIS-beheerder werkzaamheden mogen uitvoeren.

Bevinding
Een beheerder heeft in 2018 de beheerdersautorisaties in het CIS gekregen en werkzaamheden uitgevoerd als beheerder voordat diegene de beheerderscursus heeft gevolgd. De NCC geven aan dat de werkzaamheden uitgevoerd zijn onder begeleiding van een ervaren beheerder. In 2018 hebben de NCC een inventarisatie gehouden in hoeverre alle beheerders daadwerkelijk een beheerdersopleiding hebben gevolgd. Bij de constatering dat één beheerder nog geen opleiding had gevolgd, is de betrokken beheerder opgeleid. Hiervoor is een extra opleiding ingepland.
Eén beheerder heeft in de loop van 2018 autorisaties als beheerder gekregen, maar heeft de beheerderscursus pas begin 2019 gevolgd. De NCC' s. geven aan dat de betreffende beheerder geen werkzaamheden heeft verricht tot na het volgen van de vereiste opleiding.

Aanbeveling
We adviseren in de nieuwe procedure een werkwijze op te nemen waarbij is geborgd dat beheerders pas na het voltooien van de beheerdersopleiding beschikking krijgen over beheerdersautorisaties.

4.1.3 Deactivatie accounts

Bij het verlaten van de dienst of bij het uitvoeren van andere werkzaamheden dient de lokale beheerder dit te melden aan CIOT. De lokale beheerder maakt de betreffende gebruiker inactief in het webcliënt.

Bevinding
We hebben geconstateerd dat in 2018 42 accounts zijn gedeactiveerd. Drie bevragers hebben in 2018 een account gehad, maar hebben geheel 2018 geen bevragingen uitgevoerd. In de wet en de afspraken met het CIOT ontbreekt een SMART geformuleerde norm waarin beschreven staat binnen welke termijn dient te worden gedeactiveerd. Tevens staat niet beschreven indien en wanneer bij bijzondere situaties zoals langdurige ziekte of tijdelijke tewerkstelling elders een account dient te worden gedeactiveerd.

Aanbeveling
We bevelen aan een SMART geformuleerde norm op te nemen in de afspraken met CIOT voor omstandigheden en termijnen waarbinnen accounts (tijdelijk) gedeactiveerd dienen te worden

4.1.4 Bevragerscursus

CIOT geeft een cursus voor gebruikers (bevragers) over het gebruik van het CIOT. Gebruikers/aanvragers dienen deze cursus gevolgd te hebben voordat het gebruikersaccount wordt verstrekt.

Bevinding
Een bevrager heeft bevragingen in CIS uitgevoerd voordat diegene de bevragerscursus heeft gevolgd.

Aanbeveling
We adviseren in de nieuwe procedure een werkwijze op te nemen waarmee is geborgd dat bevragers pas na het voltooien van de vereiste opleiding beschikking krijgen over bevragersautorisaties.

4.2 Interceptie en Sensing

4.2.1 Opsporingsbevoegdheid

Alleen geautoriseerde opsporingsambtenaren hebben toegang tot het CIS. Dit betekent dat een actieve gebruiker van het CIS (beheerder en bevrager) ten tijde van zijn/haar bevragingen opsporingsbevoegd dient te zijn. Een beheerder of bevrager is opsporingsbevoegd als hij/zij algemeen opsporingsambtenaar of gecertificeerd BOA is.

Bevinding
Eén medewerker heeft bevragingen uitgevoerd buiten de periode dat diegene opsporingsbevoegd was. Het account is inmiddels geblokkeerd.

Aanbeveling
We bevelen aan een controle op de opsporingsbevoegdheid in te richten binnen het CIOT-proces.

4.2.2 Taak beheerder

De beheerder voert het beheer over de CIOT-gebruikers, het aanvragen van gebruikersaccounts en het uitreiken van de certificaten aan de gebruikers van het CIOT-informatiesysteem voor de organisatie/eenheid.

Bevinding
De aangewezen beheerders binnen I&S vervulden een rol van applicatiebeheerder. Zij maakten geen deel uit van de bevragersorganisatie. Hierdoor week qua werkzaamheden de rol van beheerder binnen I&S af van de standaardrol die beheerders in de eenheden vervullen. Per september 2019 is deze situatie beëindigd. Twee beheerders uit de bevragersorganisatie binnen I&S zijn aangewezen en vervullen nu de reguliere rol van beheerder.

Aanbeveling
Op basis van de in september 2019 doorgevoerde aanpassing is geen aanbeveling meer noodzakelijk.

4.2.3 Deactivatie accounts

Bij het verlaten van de dienst of bij het uitvoeren van andere werkzaamheden dient de lokale beheerder dit te melden aan CIOT. De lokale beheerder maakt de betreffende gebruiker inactief in het webcliënt.

Bevinding
Een bevrager heeft in 2018 een account gehad, maar heeft geheel 2018 geen bevragingen uitgevoerd. Zoals in paragraaf 4.1.3 is vermeld, ontbreekt in de wet en in de afspraken met het CIOT een SMART geformuleerde norm waarin beschreven staat binnen welke termijn dient te worden gedeactiveerd. Tevens staat niet beschreven indien en

wanneer bij bijzondere situaties zoals langdurige ziekte of tijdelijke tewerkstelling elders, een account dient te worden gedeactiveerd.

Aanbeveling
We bevelen aan een SMART geformuleerde norm op te nemen in de afspraken met CIOT voor omstandigheden en termijnen waarbinnen accounts (tijdelijk) gedeactiveerd dienen te worden.

4.2.4 Bewaartermijn

De administratie van bevragingen wordt bewaard tot na de audit over betreffend jaar.

Bevinding
Bij I&S zijn drie aanvragen niet teruggevonden, omdat de mailbox waarin de (spoed) aanvragen binnenkomen, is geschoond voorafgaande aan de uitvoering van de audit 2018.

Aanbeveling
We adviseren in de nieuwe procedure een bewaartermijn voor de onderliggende documenten van een bevraging op te nemen tot na behandeling van het auditrapport door de Minister in de Tweede Kamer over het betreffende tijdsvlak.

4.3 112-centrale

In deze paragraaf worden de bevindingen van de audit 2018 ten aanzien van de 112-centrale weergegeven.

4.3.1 Persoonsgebonden accounts

Toegang tot het CIOT hebben alleen bevragers met een persoonlijk en een persoonsgebonden certificaat. De gebruiker mag het certificaat en accountgegevens niet aan de lokale beheerder of andere personen verstrekken.

Bevindingen
De 112-centrale maakt gebruik van acht groepsaccounts. Door het gebruik van groepsaccounts is het voor ons niet onomstotelijk vast te stellen of de bevragers die binnen de 112-centrale in 2018 een bevraging in het CIS hebben uitgevoerd daadwerkelijk opsporingsbevoegd zijn. De 112-centrale houdt wel extracomptabel een administratie bij waarin een werknemer aan een CIOT ID wordt gekoppeld.

Aanbeveling
Ter ondersteuning van de bevragingsbehoefte bij 112 wordt al geruime tijd gewerkt aan de realisatie van een platform waarbij de directe aanlevering van NAWP-gegevens vanuit de telecomaanbieders technisch is geregeld. Door verschillende omstandigheden was het 112-platform ultimo 2020 nog niet gerealiseerd en derhalve niet geïmplementeerd. We bevelen aan om een spoedige realisatie van het platform te blijven ondersteunen.

4.3.2 Geldige rechtsgrondslag

Voorafgaand aan het vorderen van gegevens bij aanbieders via CIOT dient door de bevoegde autoriteit gecontroleerd te worden of de vordering geschiedt op basis van een geldige rechtsgrondslag. De telecomaanbieders zijn wettelijk verplicht om de NAWP-gegevens van hun klanten aan de landelijke 112-meldkamer aan te leveren conform artikel 11.10 lid 3 TW.

Bevindingen
In 2018 heeft de 112-centrale vier keer een bevraging in het CIS uitgevoerd waarbij de aanvraag op artikel 126N in plaats van artikel 11.10 lid 3 TW heeft plaatsgevonden. Dit betreft een administratieve fout die terug te voeren is naar één medewerker.

Aanbeveling
Ook met betrekking tot deze bevinding adviseren we om een spoedige realisatie van het 112-platform te blijven ondersteunen.

4.4 Deelwaarnemingen

In de volgende subparagrafen wordt de uitvoering van de deelwaarnemingen nader toegelicht en worden de bevindingen weergegeven.

4.4.1 Uitvoering deelwaarnemingen

De politie heeft in 2018 ruim 147.000 bevragingen[1] uitgevoerd in het CIS. Deze CIS-bevragingen zijn de basis geweest voor de selectie van de deelwaarnemingen van 164 bevragingen. Voor 2018 is gekozen om het aantal geautomatiseerde posten in de deelwaarnemingen te beperken. We hebben de deelwaarnemingen uitgevoerd binnen de eenheden waar we op basis van de data-analyse de grootste risico's verwachtten. De selectie van de posten bij deze eenheden is uitgevoerd met een focus op de hieronder geformuleerde risicovolle(re) posten:

- Nieuwe bevragers in de eenheid.
- Bevragers die in 2018 weinig bevragingen hebben uitgevoerd.
- Bevragingen op basis van en rechtsgrondslag anders dan 126N en 126NA (exoten).
- Spoedbevragingen.

Naast het selecteren van de risicovolle posten binnen de eenheid zijn aanvullend nog aselect deelwaarnemingen geselecteerd. Uit de data-analyse kan niet onomstotelijk worden vastgesteld of een post een handmatige of geautomatiseerde bevraging betreft. Wanneer een geselecteerde risicovolle post een geautomatiseerde bevraging betrof, is deze post vervangen door een aselecte post (indien het aantal afgesproken geautomatiseerde posten werd overschreden).

De aanvragen behorende bij de bevragingen zijn onder meer getoetst op de volgende punten:
- Komt de op de aanvraag door de opsporingsbevoegde ambtenaar (OA) ingevulde rechtsgrondslag overeen met de toegestane rechtsgrondslag?
- Is de aanvraag voor een CIS-bevraging gedaan door een bevoegde OA?
- Komt de daadwerkelijke bevraging in CIS overeen met de initiële aanvraag door de OA?
- is het onderzoeksnummer op de aanvraag vermeld?

In bijlage A is de gehanteerde werkinstructie voor de deelwaarnemingen opgenomen.

4.4.2 Bevindingen deelwaarnemingen

Uit de deelwaarnemingen komt een aantal bevindingen.
- We constateren dat in zes gevallen er geen dossier is aangetroffen. Dit betreffen o.a. drie posten van de 112-centrale. De 112-centrale geeft hierbij als toelichting dat bij een grote storm de centrale minder goed bereikbaar was. Er heeft toen vanuit de 112-centrale een terugbelactie plaatsgevonden. Dit is niet in de extracomptabele administratie vastgelegd.
- Bij zes posten is de aanvraag voor een bevraging vanuit een andere Bijzondere Opsporingsdienst (BOD) gedaan. We hebben de opsporingsbevoegdheid van de aanvragers niet kunnen toetsen aangezien zij niet tot de politieorganisatie behoren.
- Bij twee aanvragen hebben we de initiële aanvraag niet kunnen aansluiten met het resultaat van de bevragingen in het CIS, omdat een onderliggend document ontbrak of omdat het telefoonnummer in de vordering ontbrak.
- Ook constateerden we bij 14 posten een administratieve afwijking. Bij deze posten is namelijk de verkeerde rechtsgrondslag geselecteerd in het CIS.

[1] Eén bevraging in het CIS kan uit meerdere vragen bestaan.

5. Opvolging van aanbevelingen audit 2017

In onderstaande paragrafen wordt de stand van zaken van de aanbevelingen uit de audit CIOT 2017 weergegeven.

5.1 Landelijke procedure

We hebben geconstateerd in de audit 2017 dat de beschrijving van de landelijke procedure op een aantal punten aanscherping vergt. De NCC's geven aan dat een nieuwe (concept)procedure bijna gereed is. De conceptversie van de procedure is voorgelegd aan de lokale beheerders voor een toets op leesbaarheid en werkbaarheid. De procedure zal vervolgens in het reguliere besluitvormingsproces worden geformaliseerd. De NCC's geven aan dat de aanbevelingen met betrekking tot de verschillende bevragingen uit het rapport 2017 al wel zijn doorgevoerd in de opleidingen.

Tijdens het uitvoeren van de audit 2018 zijn de eisen op het gebied van de werkplekken uitgebreid aan de orde geweest. In voorgaande jaren is de in het besluit verstrekking gegevens telecommunicatie en de DAP opgenomen passage over de technische inrichting van de werkplekken altijd rechtstreeks toegepast op de werkplekinrichting bij de politie. Informatiepunt Bijzondere Opsporingsonderzoeken (IBO) heeft echter aangegeven dat de betreffende passage uit de DAP is bedoeld voor de werkplekken bij het CIOT. Daarmee kan dit aandachtspunt uit de rapportage 2017 vervallen. Hiermee blijft wel van toepassing dat de werkplekken binnen het politiedomein dienen te voldoen aan de inrichtings- en beveiligingseisen die van toepassing zijn binnen de politie organisatie. Tijdens de audit 2018 zijn hierover geen bevindingen te melden.

5.2 Autoriseren

In de audit 2017 zijn diverse bevindingen geconstateerd met betrekking tot autorisaties binnen het CIOT-proces. Hieronder wordt per bevinding kort de laatste stand van zaken beschreven.

- De NCC's geven aan dat een werkwijze is opgenomen in de nieuwe procedure om het vooraf aanwijzen van CIS-bevragers door een gemandateerd sectorhoofd te laten plaatsvinden. De procedure wordt op korte termijn geformaliseerd in het reguliere besluitvormingsproces.

- De NCC's geven aan dat er voor de controle op de opsporingsbevoegdheid van een CIS-bevrager of gebruiker aan een systeemtechnische oplossing wordt gewerkt, maar dat is nog moeilijk te realiseren. Ook merkt de NCC op dat een steekproef is ontwikkeld waarin een controle op de opsporingsbevoegdheid is opgenomen. De NCC laat weten dat in het landelijk overleg GBK/interceptiedesk is benoemd dat een taak ligt bij de leidinggevenden om toe te zien op de opsporingsbevoegdheid van medewerkers. De NCC's merken op dat de operationeel leidinggevenden van de GBK/Interceptiedesk de controle op de opsporingsbevoegdheid kunnen delegeren aan de beheerders. Er blijft tevens een verantwoordelijkheid liggen bij de gebruikers. In de cursussen en overlegmomenten wordt dit volgens de NCC ook gecommuniceerd.

- We hebben vastgesteld dat een administratie wordt bijgehouden om (historisch) inzicht in de deelname aan de verplichte opleidingsdag voor bevragers en beheerders van het CIS te verkrijgen. Sinds 2017 geeft CIOT (opleidings-)certificaten uit na deelname aan de opleidingsdag. Met het IBO is de afspraak gemaakt dat een wachtwoord voor de CIS-applicatie pas aan een nieuwe gebruiker of beheerder wordt verstrekt nadat de vereiste opleiding is gevolgd.

- De NCC's geven te kennen dat in de nieuwe (concept) procedure is opgenomen wie formeel een nieuwe beheerder aanwijst.

- Ook geven de NCC's aan dat een beschrijving van de rol van NCC is opgesteld. Deze beschrijving is ter akkoord en formalisering voorgelegd aan de Portefeuillehouder.

5.3 Interceptie en Sensing

In de audit 2017 zijn diverse bevindingen geconstateerd met betrekking tot I&S binnen het CIOT-proces. Hieronder wordt per bevinding kort de laatste stand van zaken beschreven.

- De NCC geeft aan dat in nieuwe (concept)procedure het proces spoedbevragingen is opgenomen. Alle taken die afwijkend werden uitgevoerd, zijn in de procedure aangepast aan de wenselijke situatie.

- Twee nieuwe beheerders zijn aangewezen bij I&S. Deze beheerders maken deel uit van de bevragersorganisatie van I&S en hebben zodoende toegang tot de afdeling. Ook geven de NCC's aan dat in de nieuwe (concept) procedure geen onderscheid wordt gemaakt tussen rollen van beheerders van verschillende eenheden binnen de politie.

- I&S voert incidenteel buiten kantoortijden voor Bijzondere Opsporingsdiensten (BOD's) spoedbevragingen uit. Art 126na SV is de basis voor het doen van NAW-bevragingen. Dat artikel stelt dat de opsporingsambtenaar een vordering kan doen voor NAW-gegevens. Dat geldt dus voor elke opsporingsambtenaar, zowel van politie als van BOD's. Het wetboek van SV noch het CIOT-besluit sluit uit dat een ambtenaar aangewezen door de politiechef een bevraging kan doen voor een BOD. Juridisch gezien is er dus geen enkele belemmering voor een bevraging door I&S voor een BOD, in het kader van de reeds bekende (spoed)procedure.

- Voor het uitvoeren van bevragingen bij I&S was de server geautoriseerd in plaats van de betreffende werkstations. De NCC's hebben verklaard dat de autorisatie van de server is aangepast, zodat deze alleen toegang geeft voor specifieke werkstations. De NCC heeft het aantal werkplekken bij I&S teruggebracht tot vier werkstations die toegang geven tot CIS.

- De NCC's hebben te kennen gegeven dat de procedure doorbevragingen bij providers na een no-hit nader is beschreven in de nieuwe (concept)procedure CIOT.

5.4 112-centrale

De minister heeft in een schrijven van 14 november 2018 geconstateerd dat de 112-meldkamer in uitzonderlijke gevallen CIS-bevragingen uitvoert ten behoeve van noodhulp, terwijl hiervoor de wettelijke grondslag ontbreekt. In de audit CIOT 2017 is aangegeven dat de 112-meldkamer op een aantal punten afwijkend van de regelgeving handelt, maar dat de minister tijdelijk instemt met het voortzetten van de bestaande werkwijze.
Ter ondersteuning van de bevragingsbehoefte bij 112 wordt al geruime tijd gewerkt aan de realisatie van een platform, waarbij de directe aanlevering van NAWP-gegevens vanuit de telecomaanbieders technisch is geregeld. Door verschillende omstandigheden heeft tot op heden geen realisatie en implementatie plaats kunnen vinden. De afwijkende werkwijze, de (afwijkende) procedure en aanvullende maatregelen zijn niet vastgelegd. De NCC heeft aangegeven dat deze zaken in de nieuwe conceptprocedure wel zijn opgenomen.

Bijlage

Bijlage A: Werkinstructie deelwaarnemingen audit CIOT 2018

CIOT-ID				
Type aanvraag	**Werkpro gramma**		**Norm**	**Hoe controle uitvoeren**
Aanvraag CIOT bevraging door opsp. Ambtenaar			De vordering van een **opsporingsambtenaar (OA)** kan worden gedaan op basis van: - art 126 NA Sv (verdenking misdrijf) - art 126 UA Sv (georganiseerd verband) - art 126 ZI Sv (terroristisch misdrijf) - art 565 lid 2 Sv (vaststellen verblijfplaats van de aan te houden persoon)	
			Eisen gesteld aan bevel en vordering	
	2B1	**126 NA 126 UA 126 ZI art 565 lid 2**	De aanvraag voor een CIS bevraging voldoet aan de volgende voorw aarden: - bevel/vordering is bijgevoegd - De gegevens die w orden gevorderd zijn vermeld	Gegevens controlen op vordering
			Aanvraag	
	2A1		Op aanvraag door OA ingevulde rechtsgrondslag komt overeen met toegestane rechtgrondslag	Ingevulde rechtsgrondslag op initiele aanvraag betreft 126NA, 126 UA 126 ZI of art 565 lid 2.
	2B1		De aanvraag voor een CIS bevraging is gedaan door een bevoegde OA	Indien BVH: systeemtechnisch afgevangen. Indien Summit: check bij HRM op OA van aanvrager bevraging.
			De daadw erkelijke bevraging in CIS komt overeen met de initiele aanvraag door de OA	Integrale controle op de aansluiting van de telefoonnummers op de aanvraag en de telefoonnummers in het resultaat.
			Onderzoeksnummer moet op aanvraag zijn vermeld	Gegevens op bevel of vordering
			Ruimte voor eventuele opmerkingen van de auditor:	
Aanvraag CIOT bevraging door Vordering OvJ			De vordering van een **Officier van Justitie (OvJ)** kan worden gedaan op basis van: - Art 126 N Sv (verkeersgegevens) - Art 126 U Sv (georganiseerd verband) - Art 126 II Sv (voorbereiding terroristisch misdrijf) - Art 126 ZH Sv (aanwijzingen terroristisch misdrijf) Historische verkeersgegevens	
			Eisen gesteld aan bevel en vordering	
	2B1	**126 N 126 ZH**	De aanvraag voor een CIS bevraging voldoet aan de volgende voorw aarden: - bevel/vordering is bijgevoegd en bevat: - De gegevens die w orden gevorderd	Gegevens controlen op vordering
	2B1	**126 U**	De aanvraag voor een CIS bevraging voldoet aan de volgende voorw aarden: - bevel/vordering is bijgevoegd en bevat: - De gegevens die w orden gevorderd	Gegevens controlen op vordering
	2B1	**126ii**	De aanvraag voor een CIS bevraging voldoet aan de volgende voorw aarden: - bevel/vordering is bijgevoegd en bevat: - de identificerende gegevens die w orden gevorderd - de termijn w aarbinnen ende w ijze w aarop de gegevens dienen te w orden verstrekt	Gegevens controlen op vordering
			Aanvraag	
	2A		Ingevulde rechtsgrondslag op aanvraagformulier komt overeen met toegestane rechtgrondslag	Ingevulde rechtsgrondslag op initiele aanvraag betreft 126NA, 126 UA 126 ZI of art 565 lid 2.
			De aanvraag voor een CIS bevraging is gedaan door een bevoegde OvJ	Indien BVH: systeemtechnisch afgevangen. Indien Summit: check bij HRM op OA van aanvrager bevraging.
			De daadw erkelijke bevraging in CIS komt overeen met de initiele aanvraag door de OA	Integrale controle op de aansluiting van de telefoonnummers op de aanvraag en de telefoonnummers in het resultaat.
			Onderzoeksnummer moet op aanvraag zijn vermeld	Gegevens op bevel of vordering
			Ruimte voor eventuele opmerkingen van de auditor:	