Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Onderzoek CIOT Beheer 2017

Definitief v1.0

Colofon

Titel	Onderzoek CIOT Beheer 2017
Uitgebracht aan	[redacted] Justitie en Veiligheid
Datum	15 oktober 2019
Kenmerk	2019-0000172044

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Managementsamenvatting

In artikel 8 van het Besluit verstrekking gegevens telecommunicatie is opgenomen dat de minister van Justitie en Veiligheid jaarlijks een verslag opstelt van een audit naar de goede uitvoering van het Besluit verstrekking gegevens telecommunicatie door de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het Informatiepunt Bijzondere Opsporingsonderzoeken, de arrondissementsparketten en de Politie, of andere opsporingsdiensten.

Dit onderzoek is uitgevoerd op basis van de bevindingen uit het ADR-rapport 'rapport van bevindingen IBO Beheerprocessen 2016' aangevuld met normen met betrekking tot het CIS-serverbeheer en certificatenbeheer.

[redacted] Verder worden de relevante stappen binnen het importproces gelogd en is het CIS-Serverbeheer en de uitgifte van certificaten ingericht.

[redacted] Daarnaast is er geen inzicht in de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij. Een logisch toegangsbeveiligingsbeleid voor het CIOT-domein ontbreekt en daarnaast zijn er geen formele procedures voor het registreren en afmelden van beheerders en voor het verlenen en intrekken van toegangsrechten.

[redacted]

Wij adviseren om de veranderingen in de dienstverlening van leveranciers te monitoren en om de dienstenniveau overeenkomsten (DNO's) periodiek te evalueren. Verder adviseren wij om inzicht te krijgen in de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening bij leveranciers.

Wij adviseren om onderzoek te doen naar de bij Justid in gebruik zijnde kaders zoals het toegangsbeleid en deze voor het CIOT te verbijzonderen daar waar nodig. Verder adviseren wij de autorisaties frequenter (bijv. 2x per jaar) te evalueren en om procedures op te laten stellen voor het registreren en afmelden van beheerders en voor het verlenen en intrekken van toegangsrechten

.

1 Aanleiding opdracht

In artikel 8 van het Besluit verstrekking gegevens telecommunicatie (hierna Besluit) is opgenomen dat de minister van Justitie en Veiligheid jaarlijks een verslag opstelt van een audit naar de goede uitvoering van het Besluit door de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het Informatiepunt Bijzondere Opsporingsonderzoeken (IBO), de arrondissementsparketten en de Politie, of andere opsporingsdiensten. Volgens het Besluit behoort de audit ten minste de volgende onderwerpen te behandelen:

1. de werking van het CIOT-Informatiesysteem (CIS);
2. de kwaliteit van de verstrekking van gegevens;
3. de bevraging van gegevens.

De Auditdienst Rijk (ADR) heeft in de maanden november en december 2018 in opdracht van de directeur-generaal Rechtspleging en Rechtshandhaving (DGRR) een onderzoek uitgevoerd naar de werking (betreft de juridische werking en niet de auditterm waarmee naleving over langere tijd wordt bedoeld) van het CIS. De doelstelling van het onderzoek is het verschaffen van inzicht in de risico's op het gebied van de gegevensaanlevering en -verstrekking bij het IBO met het beheer van het CIS als object van onderzoek. De onderdelen met betrekking tot de kwaliteit van de verstrekking van gegevens en de bevraging van gegevens worden separaat door de ADR onderzocht en zijn geen onderdeel van het onderzoek CIOT Beheer 2017.

Dit rapport bevat de feitelijke bevindingen van het uitgevoerde onderzoek en verschaft derhalve geen zekerheid, omdat er geen assurance-opdracht is uitgevoerd.

1.1 Context

IBO voert als onderdeel van de Justitiële Informatiedienst (Justid) van het ministerie van Justitie en Veiligheid (JenV) voor de productlijn CIOT het technisch beheer, functioneel beheer en applicatiebeheer uit voor het CIS.

Informatieverzoeken van de (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten (BOID's) worden door IBO doorgeleid naar de aanbieders van telecommunicatiediensten en levert hiermee persoonsgegevens die horen bij IP-adressen, telefoonnummers en e-mailadressen aan opsporingsdiensten, veiligheidsdiensten en inlichtingendiensten. Met deze gegevens kunnen deze diensten verdachten van criminele activiteiten opsporen. IBO kan in die zin worden beschouwd als een "berichtenmakelaar".

Aanbieders leveren elke 24 uur een bestand met klantgegevens aan waarvoor zij een vergoeding krijgen van de overheid.

1.2 Opbouw rapportage

De feitelijke bevindingen van dit onderzoek met betrekking tot het CIS worden per onderwerp gegroepeerd weergegeven in hoofdstuk 2. Indien nodig worden direct in de tekst de aanbevelingen gedaan. De verantwoording van het onderzoek is in hoofdstuk 3 beschreven. Hoofdstuk 4 betreft de ondertekening. Bijlage 1 bevat de managementreactie van IBO op dit onderzoek.

2 Bevindingen

In dit hoofdstuk worden de feitelijke bevindingen van het onderzoek weergegeven waarin wij antwoord geven op de onderzoeksvragen:

> *"Welke verbetermaatregelen zijn in opzet en bestaan door IBO getroffen naar aanleiding van de ADR-rapportage IBO-beheersprocessen 2016 waaronder de logging en de juiste autorisatie inzake de verstrekking?"*
> Paragraaf 2.2 en 2.7.
>
> *"Welke beheersmaatregelen heeft IBO in opzet en bestaan getroffen ten aanzien van het CIS-server- en certificatenbeheer en de verbinding CIS-server en webserver?"*
> Paragraaf 2.1, 2.3, 2.4, 2.5 en 2.6.

De feitelijke bevindingen en geconstateerde afwijkingen van alle normen zijn opgenomen in dit hoofdstuk. Bij het weergeven van de feitelijke bevindingen in onderstaande paragrafen volgen wij de volgorde van behandelde onderwerpen uit het normenkader (zie ook hoofdstuk 3.2).

2.1 Versleutel-algoritmes en de gebruikte protocollen conform NCSC-richtlijnen ingericht

Norm: Bestandsoverdracht via Digikoppeling ebMS vindt plaats via een beveiligde verbinding.

De CIOT Gegevens Aanlever Voorziening (GAV) voorziet in de bestandsoverdracht tussen aanbieders (telecomproviders) en IBO. De GAV maakt gebruik van de Digikoppeling ebMS[1] als onderdeel van de berichtencommunicatie. Voor het ministerie van JenV wordt de Digikoppeling ontsloten middels de JUstitie BErichten Service (Jubes) en functioneert Jubes als een "berichtenmakelaar". De beveiligingseisen gesteld aan de Digikoppeling ebMS zijn beschreven.

[redacted]

2.2 Relevante stappen binnen importproces worden gelogd

Norm: Loginformatie wordt bewaard en is toegankelijk (achterwaartse compatibiliteit) totdat de bewaartermijnen verstreken zijn. De bewaartermijn is afgestemd op de eisen van wet- en regelgeving en op de controle -en auditcyclus van de betreffende gegevens.

In het in 2017 uitgevoerde IBO Beheeronderzoek over het controlejaar 2016 is geconstateerd dat een overzicht met daarin bewaartermijnen, de toelichting op de

[1] ebMS is het protocol waarop de Digikoppeling ebMS Koppelvlakstandaard is gebaseerd

gegevens, de opslaglocatie, de verantwoordelijken en de onderliggende wettelijke bepaling is aangetroffen dat echter geactualiseerd moest worden. IBO heeft in 2018 de bewaartermijnen geactualiseerd voor zover het de verwerking van persoonsgegevens betreft. In geval dat er geen persoonsgegevens worden verwerkt wordt er geen limiet gesteld aan de duur van de bewaartermijn zoals bijvoorbeeld in geval van bepaalde systeemlogging. Hierdoor ontstaat het risico op niet tijdige verwijdering van logging indien wet- en regelgeving dat eist.

Van de relevante stappen uit het importproces wordt loginformatie bewaard. De loginformatie uit het importproces is actueel en toegankelijk en wordt meerdere jaren bewaard. Wij hebben vastgesteld dat de logging beschikbaar is vanaf 2014 tot en met het moment van onderzoek.

Foutieve en succesvolle inlogpogingen binnen het importproces worden middels auditlogging voor de duur van één tot twee dagen gelogd. Naar aanleiding van deze bevinding heeft IBO per direct de logretentie verlengd.

Wij adviseren om het overzicht van de bewaartermijnen te actualiseren naar de laatste wet- en regelgeving (AVG). Onderzoek of er een wettelijke bepaling is ten aanzien van de bewaar- en/of vernietigplicht ingeval er geen persoonsgegevens worden verwerkt en pas de bewaartermijnen daaropaan.

2.3 Verbindingen tussen CIS-server en Blackboxen zijn versleuteld

Norm: Communicatie tussen de CIS-server en de Blackboxen wordt versleuteld.

[redacted] De blackbox is een beveiligde omgeving waarin de aanbieder eenmaal per 24 uur een bestand opslaat met de wettelijk vastgestelde klantgegevens. Omdat de black box een afgeschermde omgeving is, kunnen de verschillende aanbieders elkaars bestanden niet benaderen.
[redacted] Wij hebben vastgesteld op basis van één waarneming op één moment in 2018 dat de gehanteerde versleutel-algoritmes en de gebruikte protocollen conform de NCSC-richtlijnen zijn ingericht.

Beveiligingsinstellingen ten behoeve van de versleuteling van verbindingen zijn niet beschreven. Hierdoor ontstaat het risico dat in geval van een nieuw systeem of in geval van een herstelactie naar aanleiding van een incident of calamiteit er geen eenduidige configuratierichtlijn is. IBO past door de leverancier geleverde best-practices toe om versleutelde verbindingen te configureren.

Wij adviseren om de beveiligingsinstellingen vast te leggen voor toekomstig gebruik.

2.4 [redacted]CIS-server en webserver

Norm: Communicatie tussen de applicatie- en de webserver is versleuteld. De webserver is beveiligd tegen ongeautoriseerd gebruik.

[redacted]

[redacted]

Beveiligingsinstellingen ten behoeve van de versleuteling van verbindingen zijn niet beschreven. Hierdoor ontstaat het risico dat in geval van een nieuw systeem of in geval van een herstelactie naar aanleiding van een incident of calamiteit er geen eenduidige configuratierichtlijn is. IBO past door de leverancier geleverde best-practices toe om versleutelde verbindingen te configureren.

Op de webserver zijn een beperkt aantal beheerders opgevoerd conform een autorisatiematrix. Deze beheerders zijn door IBO specifiek toegewezen voor de uitvoering van CIOT-beheertaken.

Wij adviseren om de beveiligingsinstellingen vast te leggen voor toekomstig gebruik.
[redacted]

2.5 CIS-Serverbeheer en uitgifte van certificaten ingericht

Norm: De webapplicatie authentiseert een gebruiker, alvorens een bevraging kan worden uitgevoerd. Hiervoor wordt gebruik gemaakt van persoonsgebonden certificaten en een unieke, door de gebruiker te definiëren persoonlijke pincode met een geldigheidsduur van 1 jaar.

Gebruikers (afnemer bij een BOID) kunnen alleen bevragingen uitvoeren nadat toegang tot het CIS is verleend. Gebruikers worden geauthentiseerd op basis van gebruikersnaam en wachtwoord [redacted] in combinatie van een persoonlijk certificaat. Wij hebben vastgesteld op basis van één waarneming op één moment in 2018 dat ongeautoriseerde toegang tot het CIS zonder geldig certificaat niet mogelijk is. IBO heeft een procedure om een persoonsgebonden certificaat toe te kennen aan een gebruiker. Vastgesteld is op basis van één waarneming op één moment in 2018 dat aan een gebruiker verstrekt certificaat een beperkte levensduur heeft van één jaar en dat de gebruiker zelf een wachtwoord [redacted] instelt.

Norm: Per BOID zijn maximaal twee lokale beheerders aangewezen. Aan hun gebruikersaccount zijn applicatiebeheerdersrechten gekoppeld. Er is inzicht in de (aantallen) uitgegeven certificaten en actieve gebruikers per BOID.

IBO heeft de uitbreiding van de rechten van een gebruiker -als deze gebruiker de functie van een beheerder krijgt- beschreven. Deze uitbreiding van rechten gebeurt op basis van specifieke rollen in de CIS-applicatie. We hebben vastgesteld op het moment van waarnemen met peildatum december 2018 dat er maximaal 2 beheerders per BOID geregistreerd zijn en dat de aantallen uitgegeven certificaten per BOID en van IBO inzichtelijk zijn.

Norm: Alleen de (centrale) CIOT-servicedesk is bevoegd certificaten uit te geven. Na goedkeuring door het bevoegd gezag wordt door de CIOT-servicedesk het door een gebruiker (afnemer) aangevraagde account aangemaakt of ingetrokken.

Wij hebben (eenmalig vastgesteld) dat het alleen mogelijk is om een certificaat te verkrijgen wanneer de CIOT-servicedesk een account heeft aangemaakt voor de gebruiker. Verzoeken voor het toevoegen en het afvoeren van gebruikers worden door de servicedesk geadministreerd en afgehandeld conform een werkinstructie. We hebben vastgesteld voor een willekeurige aanvraag voor zowel een nieuw als een op te heffen gebruikersaccount conform de werkinstructie is afgehandeld en dat

dit controleerbaar is in het registratiesysteem. Uit de registratie blijkt dat het bevoegd gezag (management IBO) deze aanvraag heeft goedgekeurd en dat vervolgens een medewerker van de servicedesk het door een BOID-beheerder aangevraagde account heeft uitgegeven.

Norm: Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up en hersteltijd. Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.

In het in 2017 uitgevoerde IBO Beheeronderzoek over het controlejaar 2016 is geconstateerd dat het back-upbeleid gefragmenteerd aanwezig is en beschrijft de rapportage van 20 december 2017 "Het regulier testen van een back-up en een restore wordt niet periodiek uitgevoerd en de rapportage hierover vindt beperkt plaats.". Deze situatie is in 2017 onveranderd.

IBO heeft hierop in 2018 het back-upbeleid geactualiseerd. Het back-upbeleid beschrijft de in de norm gestelde eisen behalve de frequentie van de uitvoering van een back-up- en recoverytest. Hierdoor ontstaat het risico dat er geen gevolg wordt gegeven aan de uitvoering van back-up- en recoverytesten omdat het als iets vrijblijvends wordt opgevat. Een periodieke back-up- en recoverytest heeft in 2017 niet plaatsgevonden. Op basis van deze bevinding heeft IBO in 2018 eenmalig een back-up- en recoverytest uitgevoerd waarover is gerapporteerd.

Wij hebben vastgesteld dat back-ups conform dit beleid in 2018 worden uitgevoerd. Er zijn overzichten aangetroffen met daarin de succesvolle en niet succesvolle back-ups. Aan de niet succesvolle back-upjobs wordt opvolging gegeven door technisch beheer. We hebben vastgesteld op basis van één waarneming op één moment in 2018 dat de back-up software op een zodanige wijze is geconfigureerd dat daarin geen gegevens worden opgenomen die herleidbaar zijn tot personen op wie een verzoek om informatie betrekking heeft en dat back-ups versleuteld worden opgeslagen.

Wij adviseren om de periodiciteit van de back-up en recoverytest toe te voegen aan het back-upbeleid. IBO heeft aangegeven een frequentie van één keer per jaar te hanteren.

2.6 Aandacht voor veranderingen in de dienstverlening van leveranciers

Norm: Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.

Norm: Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's. De SLA's worden periodiek (jaarlijks) geëvalueerd en daar waar noodzakelijk bijgesteld.

<u>Aanbieders</u>
IBO heeft met de aangesloten aanbieders een ondertekende dienstenniveau overeenkomst (DNO). De DNO beschrijft de afspraken tussen IBO en de aanbieders over de te bewerkstelligen beveiligingsmaatregelen, de definities van de dienstverlening en niveaus van dienstverlening. De DNO wordt aangegaan voor onbepaalde tijd.

Naast de DNO wordt er tussen IBO en de aanbieders een bewerkersovereenkomst[2] en een auditovereenkomst getekend. Ondertekening van een DNO, bewerkersovereenkomst en auditovereenkomst gebeurt door middel van een zogenoemd toetredingsdocument dat alleen nog door de aanbieder moet worden getekend.

De ons onderzochte aanbieders hebben een door beide partijen ondertekend toetredingsdocument.

Leveranciers
IBO heeft DNO's afgesloten met leveranciers en op het gebied van huisvesting, facilitaire zaken, post en repro, informatievoorziening, beveiliging, inkoop, ICT, housing van IT-apparatuur en telefonie. Van één overeenkomst met een leverancier is vastgesteld dat deze is geëindigd op 31 december 2015. Hierdoor ontstaat het risico op het niet nakomen van de (voorheen) contractuele verplichtingen.

Afnemers
Er zijn DNO's opgesteld tussen afnemers en Justid om afspraken over het niveau van de CIOT-dienstverlening (conform het Besluit) vast te leggen. Het gaat om afspraken aanvullend op het basisniveau dienstverlening van Justid. Als aanvulling hierop heeft IBO een dossier afspraken en procedures (DAP) opgesteld die de operationele afspraken en procedures beschrijft die relevant zijn voor het nastreven van de afgesproken dienstverlening in de hierboven genoemde DNO. De DAP geeft een verdere concretisering van de werkwijze tussen beide partijen (waaronder de incidentenprocedure, wijzigingsprocedure, no-hit procedure en certificatenprocedure). De ons onderzochte afnemers hebben een getekende overeenkomst met Justid. We hebben vastgesteld dat met één van de afnemers afspraken zijn gemaakt over beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening.

We hebben vastgesteld er niet gerapporteerd wordt over veranderingen in dienstverlening en dat DNO's niet periodiek worden geëvalueerd. Verder heeft IBO geen inzicht in de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij. Hierdoor ontstaat het risico dat de gewenste dienstverlening en/of informatiebeveiliging niet overeenkomt met de overeengekomen overeenkomst.

Wij adviseren om het geëindigde contract met de leverancier te bezien en te verlengen. Actualiseer de afgesloten bewerkersovereenkomsten zodat ze aansluiten op de vigerende privacywetgeving (AVG). Wij adviseren ook veranderingen in de dienstverlening van leveranciers te beheren en adviseren wij daarbij ook om DNO's periodiek te evalueren. Verder adviseren wij om inzicht te krijgen in de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening bij leveranciers. Bijvoorbeeld aan de hand van ISAE3402 verklaring of een ISO27001 certificering.

2.7 Logisch toegangsbeveiligingsbeleid voor CIOT-domein ontbreekt

Norm: Er behoren formele procedures voor het registreren en afmelden van beheerders te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
Functiewijzigingen en in- en uitdiensttreding worden tijdig verwerkt.

[2] De AVG spreekt van een verwerkersovereenkomst. Voor het controle jaar 2017 was de Wbp vigerende privacywetgeving en spreken we in dat verband van een bewerkersovereenkomst.

Er zijn geen formele procedures aangetroffen voor het registreren en afmelden van beheerders en voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten. Hierdoor ontstaat het risico dat er niet op uniforme wijze wordt gehandeld met als gevolg onterecht of verkeerd uitgegeven of ingetrokken autorisaties.

Een in- en uitdiensttredingsformulier wordt gehanteerd bij de in- en uitdiensttreding van medewerkers waaronder beheerders en is voorzien van een controlelijst. De onderwerpen in de controlelijst worden door de coördinatoren en het management van IBO voor akkoord geparafeerd en hebben o.a. betrekking op de toegangsrechten en de uitgifte of inname van identiteits- en authenticatiemiddelen.

Van een nieuwe medewerker in dienst hebben wij een indiensttredingsformulier aangetroffen met daarbij een door het bevoegd gezag ingevulde controlelijst. Van één medewerker die de dienst heeft verlaten is geen uitdiensttredingsformulier aangetroffen. IBO heeft hierop aangegeven dat de toegangsrechten voor deze medewerker direct na vertrek zijn ingetrokken en conform het uitdiensttredingsformulier is afgehandeld.

Volgens mededeling hebben zich geen functiewijzigingen voorgedaan in 2017.

Wij adviseren om procedures op te laten stellen voor het registreren en afmelden van beheerders en voor het verlenen en intrekken van toegangsrechten en deze procedure toe te passen.

Norm: Alleen daartoe geautoriseerde gebruikers (beheerders) hebben toegang tot de Blackboxen. Rechten zijn op basis van het "need-to-know" principe toegekend aan deze personen.

Wij hebben vastgesteld dat IBO op basis van één waarneming op één moment in 2018 beheerders autoriseert aan de hand van een autorisatiematrix. Deze matrix bestaat uit medewerkersgroepen gekoppeld aan taken en bevoegdheden. Autorisatie vindt plaats op basis van de 'need-to-know' en 'least privileged' principes. Verder voeren beheerders beheertaken uit met een gepersonaliseerd beheeraccount. Er wordt geen gebruik gemaakt van groeps- of serviceaccounts voor het uitvoeren van beheerwerkzaamheden. Beheerders kunnen indien noodzakelijk domain administrator rechten krijgen middels een daartoe specifiek ingerichte procedure. Uitsluitend specifiek hiervoor bevoegde functionarissen (management IBO) verlenen deze verhoogde rechten.

Van één account uit de groep domain administrators is vastgesteld op basis van één waarneming op één moment in 2018 dat deze geen functie heeft. Tijdens het onderzoek heeft IBO per direct het betreffende account uit de betreffende groep verwijderd en geïnactiveerd.

De aanwezige service- en beheeraccounts op de databaseserver kunnen door IBO worden verklaard.

Norm: Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.

Een toegangsbeveiligingsbeleid is niet aangetroffen. Hierdoor ontstaat het risico op onduidelijkheid ten aanzien van te nemen maatregelen voor toegangsbeheersing (bijvoorbeeld 2-factor authenticatie). We hebben vastgesteld dat toegang tot de CIS-applicatie voor eindgebruikers verleend wordt op basis van 2-factor authenticatie op basis van een waarneming op één moment in 2018. [redacted]

[redacted]

Wij adviseren om onderzoek te doen naar de bij Justid in gebruik zijnde kaders zoals het toegangsbeleid en deze voor het CIOT te verbijzonderen daar waar nodig. Verder adviseren wij de autorisaties frequenter (bijv. 2x per jaar) te evalueren.

3 Verantwoording onderzoek

3.1 Doelstelling

De doelstelling van het onderzoek is het verschaffen van inzicht in de risico's op het gebied van de gegevensaanlevering en -verstrekking bij het IBO.

De DGRR kan op basis van dit onderzoek de minister van Justitie en Veiligheid informeren om deze in staat te stellen verslag te doen aan de Tweede Kamer conform de wettelijke bepaling in artikel 8 van het Besluit verstrekking gegevens telecommunicatie.

In dit onderzoek worden de volgende onderzoeksvragen beantwoord:

> "Welke verbetermaatregelen zijn in opzet en bestaan door IBO getroffen naar aanleiding van de ADR-rapportage IBO-beheersprocessen 2016 waaronder de logging en de juiste autorisatie inzake de verstrekking?"
>
> "Welke beheersmaatregelen heeft IBO in opzet en bestaan getroffen ten aanzien van het CIS-server- en certificatenbeheer en de verbinding CIS-server en webserver?"

Om handelingsperspectief te bieden zijn op verzoek van de opdrachtgever aanbevelingen gedaan.

3.2 Werkzaamheden en periode van uitvoering

Voor dit onderzoek is gedurende de periode oktober en november 2018 dossieronderzoek uitgevoerd, zijn interviews gehouden en zijn waarnemingen ter plaatse uitgevoerd.

Voor het onderzoek is een normenkader opgesteld op basis van de bevindingen uit het ADR-rapport 'rapport van bevindingen IBO Beheerprocessen 2016' aangevuld met normen met betrekking tot het CIS-serverbeheer en certificatenbeheer. Dit normenkader is in samenspraak met de opdrachtgever tot stand gekomen en betreft de volgende onderwerpen:

1. Digikoppeling ebMS;
2. Logging en monitoring importproces;
3. Verbindingen CIS-server en Blackboxen;
4. Verbinding CIS-server en webserver;
5. CIS-Server en certificaten(beheer);
6. Servicelevel & supplier management;
7. Logische toegangsbeveiliging CIOT-domein.

De onderzochte normen per onderwerp zijn integraal opgenomen binnen hoofdstuk 2.

De concept bevindingen uit ons onderzoek zijn in het kader van hoor en wederhoor op 4 december 2018 met IBO besproken. Voor zover deze opmerkingen betrekking hadden op feitelijke onjuistheden zijn deze aangepast in de bevindingenmatrix en op 14 maart 2019 afgestemd met IBO alvorens deze definitief te hebben gemaakt.

Het auditdossier inclusief de onderbouwing van de bevindingen wordt beperkt en onder voorwaarden in het auditmanagementsysteem van de ADR bewaard. Gezien

het rubriceringsniveau van de informatie in het auditdossier wordt deze op locatie bij IBO conform geldende wet- en regelgeving- ten minste 7 jaar bewaard.

Het dossier is alleen toegankelijk met uitdrukkelijke toestemming van de ADR voor gescreende medewerkers en op 'need-to-know' basis raadpleegbaar, zoals de kwaliteitstoetsers van de ADR in verband met de afronding van het onderzoek. Van de overdracht van het dossier is een protocol van overdracht opgemaakt.

3.3 Object van onderzoek en afbakening

Het object van onderzoek is het beheer van het CIOT Informatiesysteem (CIS).

De ADR heeft onderzoek gedaan naar opzet en bestaan van de maatregelen voor de in paragraaf 3.2 genoemde onderwerpen. De peildatum voor vaststelling van de opzet en het bestaan is 1 december 2017.

Onder opzet verstaan we dat organisatorische processen en procedures zijn gedocumenteerd. Onder bestaan verstaan we dat de processen en procedures daadwerkelijk zijn ingericht conform de opzet (eenmalig het bestaan vaststellen).

3.4 Gehanteerde Standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (Standaarden IIA 2200-2440 en 2600).

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd. Het rapport bevat de feitelijke bevindingen van het uitgevoerde onderzoek en geeft handelingsperspectief aan de opdrachtgever.

De opdracht is uitgevoerd conform de bij de ADR geldende kwaliteitsrichtlijnen. Het voor dit onderzoek aangelegde dossier is conform deze richtlijnen ingericht en blijft eigendom van de ADR.

De interne Opdrachtgerichte Kwaliteitsbeoordeling (OKB) waarborgt de kwaliteit van de producten. Deze is uitgevoerd door een onafhankelijke kwaliteitsbeoordelaar van de ADR, welke niet betrokken is geweest bij de uitvoering van het onderzoek.

3.5 Verspreiding rapport

De opdrachtgever, [redacted] van het ministerie van Justitie en Veiligheid, 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.

4 Ondertekening

Den Haag, 15 oktober 2019

IT-Auditor
Auditdienst Rijk

Bijlage 1 Managementreactie IBO

Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 484 2501 CL Den Haag

Informatiepunt Bijzondere Opsporingsonderzoeken
Centraal Informatiepunt
Onderzoek Telecommunicatie

Turfmarkt 147
2511 DP Den Haag
Postbus 484
2501 CL Den Haag
www.justid.nl

Ons kenmerk
2019153

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

Datum 11 oktober 2019
Onderwerp Managementreactie audit rapport CIOT beheer 2017

Geachte heer/mevrouw,

Conform artikel 8 van het Besluit verstrekking gegevens telecommunicatie is de minister van Justitie en Veiligheid gehouden jaarlijks een verslag op te stellen van de audit op de uitvoering van het Besluit door de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het informatiepunt, de arrondissementsparketten en de politie, of andere opsporingsdiensten. In dat kader heeft de Auditdienst Rijk (ADR) in opdracht van het Directoraat-Generaal Rechtspleging en Rechtshandhaving onderzoek gedaan naar het technisch, functioneel en applicatiebeheer van het CIOT-Informatiesysteem over 2017. Dit beheer wordt uitgevoerd door het Informatiepunt Bijzondere Opsporingsonderzoeken (IBO), onderdeel van de Justitiële Informatiedienst (Justid).

Justid/IBO heeft kennisgenomen van het onderzoeksrapport 'Onderzoek CIOT beheer 2017' en constateert dat een significant deel van de adviezen uit de vorige auditrapportage is gerealiseerd. De technische adviezen zijn veelal geïmplementeerd. [redacted] De ADR adviseert nog wel om de frequentie van het uitvoeren van een recoverytest vast te leggen. Aan dit advies is inmiddels opvolging gegeven.

Een aantal bevindingen vergt nog nadere aandacht. Vanzelfsprekend is Justid/IBO voornemens aan de adviezen naar aanleiding van deze bevindingen opvolging te geven. De ADR stelt bijvoorbeeld vast dat een contract met een leverancier is geëindigd. Justid/IBO evalueert en verbetert haar proces- en contractmanagement en zal het advies om het contract te actualiseren en periodiek te evalueren hierin meenemen. De ADR heeft ook geconstateerd dat Justid/IBO bij in- en uitdiensttreding van medewerkers een in- en uittredingsformulier en controlelijst

hanteert. De ADR adviseert aanvullend een procedure op te stellen voor in- en uitdiensttreding. Justid/IBO zal opvolging geven aan dit advies.

Justid/IBO hoopt met deze reactie voldoende inzicht te hebben geven in hoe opvolging wordt gegeven aan de auditbevindingen.

Met vriendelijke groet,

Informatiepunt Bijzondere Opsporingsonderzoeken
Centraal Informatiepunt Onderzoek Telecommunicatie

Datum
11 oktober 2019

Ons kenmerk
2019153

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