Auditdienst Rijk
Ministerie van Financiën

Rapport van bevindingen IBO Beheerprocessen 2016

Colofon

Titel	IBO Beheerprocessen 2016
Uitgebracht aan	Ministerie van Justitie en Veiligheid, Directeur-Generaal Rechtspleging en Rechtshandhaving mw. mr. J.G. Vegter
Datum	20 december 2017
Status	Definitief
Aantal pagina's	18
Kenmerk	2017-0000239634

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Aanleiding opdracht

1.1 Inleiding

In artikel 8 van het Besluit verstrekking gegevens telecommunicatie (Besluit Telecom) is opgenomen dat de Minister van Justitie en Veiligheid jaarlijks een verslag opstelt van een audit naar de correcte uitvoering van het Besluit door de volgende organisaties:

- de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken;
- het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT);
- de arrondissementsparketten;
- de Politiekorpsen;
- andere opsporingsdiensten.

Onderwerpen die hierin tenminste behandeld moeten worden zijn de werking van het systeem, de kwaliteit van de verstrekking van gegevens en de bevraging van gegevens. In het kader van deze verplichting is de Auditdienst Rijk (ADR) door de directeur-generaal Rechtspleging en Rechtshandhaving (DGRR) gevraagd een onderzoek uit te voeren bij de afdeling IBO (Informatiepunt Bijzondere Opsporingsonderzoeken). Doel van dit onderzoek is het verschaffen van inzicht in de werking van het CIOT Informatiesysteem (CIS).

1.2 Opbouw rapportage

De feitelijke bevindingen van dit onderzoek worden per onderwerp gegroepeerd weergegeven in hoofdstuk 2. In hoofdstuk 3 is de verantwoording van het onderzoek beschreven. In bijlage 1 is de managementreactie van Justid/IBO op dit rapport opgenomen.

2 Bevindingen

De afdeling Informatiepunt Bijzondere Opsporingsonderzoeken (IBO) is onderdeel van de Justitiële Informatiedienst (Justid) van het ministerie van Justitie en Veiligheid (JenV). IBO is aangewezen om de informatieverzoeken van de (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten (BOID's) door te geleiden naar de aanbieders van telecommunicatiediensten. IBO voert voor de productlijn CIOT het technisch beheer, functioneel beheer en applicatiebeheer voor het CIOT Informatiesysteem (CIS) uit.

Hieronder worden de feitelijke bevindingen van alle per onderwerp getoetste normen weergegeven. Deze bevindingen zijn afgestemd met IBO. Conform de NOREA Richtlijn 4401 worden er geen aanbevelingen gedaan.

2.1 Beheerprocessen

2.1.1 Incidentmanagement

IBO hanteert (en heeft zich geconformeerd aan) het Justid beleid ten aanzien van de inrichting van de beveiligingsorganisatie en het beleggen van verantwoordelijkheden op het gebied van de informatiebeveiliging. Het lijnmanagement van IBO is verantwoordelijk voor de informatiebeveiliging en wordt daarbij ondersteund door de Integrale Beveiligingsfunctionaris (IBF). IBO is een kleine organisatie met veel "sociale controle" waarbij, volgens mededeling, medewerkers elkaar aanspreken op het gedrag en medewerkers hiaten direct signaleren bij de leidinggevende.

Een procesbeschrijving met onderliggende procedures t.b.v. incidentmanagement is aanwezig. Voor de sturing op en de afhandeling van incidenten zijn proceseigenaren en procesrollen gedefinieerd.

Incidenten worden geregistreerd in een incidentmanagementsysteem waarover maandelijks wordt gerapporteerd aan de teamleider van de servicedesk, de adviseur procesmanagement en het IBO lijnmanagement. Actuele incidenten worden maandelijks in het afdelingsoverleg besproken. Hiervan wordt geen verslag gemaakt.

IBO hanteert een escalatieprocedure waarbij incidenten of meldingen die langer dan vijf dagen openstaan worden geëscaleerd naar de teamleider servicedesk. Incidenten of meldingen die langer dan tien dagen openstaan worden geëscaleerd naar het IBO lijnmanagement.

2.1.2 Changemanagement

IBO beschikt over een change- en releasemanagementprocedure t.b.v. wijzigingen aan het CIS. Hierbij wordt gebruik gemaakt van gestandaardiseerde methoden en technieken gebaseerd op de Agile/DevOps ontwikkelmethodieken.

Gebruikerswensen worden in een gebruikersoverleg besproken, geprioriteerd en vervolgens ter goedkeuring voorgelegd aan de changemanager. Na akkoord wordt dit voorgelegd aan het Change Advisory Board waarin wordt bepaald of en wanneer wijzigingen in productie worden genomen.

Wijzigingen worden conform de OTA (Ontwikkel-, Test- en Acceptatieomgeving) strategie uitgevoerd. Hierin is de productieomgeving gescheiden van de OTA omgeving en worden voorgestelde wijzigingen op basis van testscripts en

testplannen getest. Wijzigingen worden in een changemanagementsysteem geregistreerd.

Controle op ongeautoriseerde wijzigingen vindt plaats door het vierogen principe bij wijzigingen aan het systeem. De scrummaster/lead-developer houdt code reviews op alle wijzigingen in het systeem. Daarnaast is alleen de teamleider DevOps geautoriseerd tot het doorvoeren van wijzigingen in de productieomgeving.

2.1.3 *Servicelevel- en suppliermanagement*

IBO heeft overeenkomsten afgesloten met producten- en dienstenleveranciers en met de aanbieders van openbare telecommunicatiediensten.

Proces en overeenkomsten
IBO voert zelfstandig contractbeheer uit maar is daarnaast voor het beheer van een aantal overeenkomsten afhankelijk van het dienstencentrum van JenV.

Een aanpassing in de dienstverlening wordt middels een addendum toegevoegd aan een Diensten Niveau Overeenkomst (DNO). DNO's worden niet periodiek geëvalueerd.

Aanbieders
Met de aanbieders heeft IBO een DNO afgesloten. Deze DNO beschrijft de afspraken tussen IBO en de aanbieders en gaat onder andere in op geheimhouding en gewenste dienstverlening. Daarnaast is er een audit- en bewerkersovereenkomst opgesteld welke geëffectueerd wordt middels een door de aanbieder getekend toetredingsdocument. Via waarneming ter plaatse hebben wij vastgesteld dat IBO beschikt over getekende toetredingsdocumenten.

Leveranciers
Met de diensten- en productenleveranciers heeft IBO DNO's afgesloten. Deze DNO beschrijft de afspraken tussen IBO en leveranciers en gaat onder andere in op geheimhouding en gewenste dienstverlening. Voor één leverancier is geen DNO aangetroffen. In één DNO is geheimhouding niet meegenomen.

Externe inhuur
IBO maakt voor de inhuur van externe medewerkers gebruik van de vastgestelde processen en procedures van Justid. Procesbeschrijvingen zijn aanwezig.

Externe medewerkers worden geautoriseerd overeenkomstig de bijbehorende rol. Afhankelijk van het type werkzaamheden die de externe medewerker gaat uitvoeren moet een Verklaring Omtrent Gedrag (VOG) of een Verklaring van Geen Bezwaar (VGB) overlegd kunnen worden. Voor aanvang van werkzaamheden moet een geheimhoudingsverklaring worden getekend.

2.1.4 *Logische toegangsbeveiliging CIOT domein*

Toegangsbeleid CIOT domein
IBO hanteert een autorisatiematrix voor de logische toegangsbeveiliging, die afgeleid is van het Justid autorisatiebeheer. In de matrix zijn medewerkers-groepen gemaakt en de daarbij horende rollen zijn toegewezen en gekoppeld aan de taken en bevoegdheden. Autorisatie vindt plaats op basis van de 'need to know' en 'least privileged' principes.

In- en uitdiensttreding
Bij in- en uitdiensttreding van medewerkers hanteert IBO een controlelijst die coördinatoren en managers gebruiken als controlemiddel. Toegangsrechten en identiteits- en authenticatiemiddelen worden ingetrokken bij uitdiensttreding. Het

IBO management ontvangt maandelijks van personeelsbeheer een overzicht van actieve medewerkers ter ondertekening voor akkoord. Een controlelijst voor functiewijzigingen (interne doorstroom) is niet aangetroffen. Interne functiewijzigingen vinden zeer beperkt plaats.

Verhoogde privileges
Beheerders loggen in met een op naam gesteld (gepersonaliseerd) account zonder verhoogde privileges. Er wordt geen gebruik gemaakt van groeps- of serviceaccounts voor het uitvoeren van beheerwerkzaamheden. In geval van een incident of wijziging waarbij verhoogde privileges nodig zijn, zijn beheerders aangewezen op een daartoe specifiek ingerichte procedure. Verhoogde privileges worden uitsluitend verleend door specifiek hiervoor bevoegde functionarissen. Het aantal hiervoor bevoegde functionarissen is op dit moment gering waardoor in geval van een calamiteit een probleem kan optreden ten aanzien van de continuïteit.

Tijdens het onderzoek is vastgesteld dat andere beheeraccounts buiten de procedure om toegang hebben tot verhoogde privileges. Volgens het management van IBO betrof dit een tijdelijke situatie vanwege een storing tijdens de onderzoeksperiode die alleen opgelost kon worden door de beheerders. Vastgesteld is dat IBO tijdens het onderzoek direct verbetering heeft aangebracht.

Autorisatiebeheer Blackboxen
De Blackboxen zijn als object van onderzoek nader onderzocht. Vastgesteld is dat het autorisatiebeheer van de Blackboxes is ingericht conform het IBO beleid.

2-factor authenticatie
Toegang tot de CIS applicatie voor eindgebruikers vindt plaats op basis van 2-factor authenticatie. [redacted]

2.2 Digikoppeling berichtenservice

Beveiliging
IBO maakt t.b.v. het Elektronisch Berichten Verkeer (EBV) gebruik van de Digikoppeling van de JUstitie BErichten Service (Jubes). Jubes functioneert hierbij als een "berichtenmakelaar" en IBO is afnemer. Telecomaanbieders sluiten aan via de CIOT gegevensaanlevervoorziening hetgeen hen in staat stelt om het klantenbestand aan IBO te leveren. Telecomaanbieders worden eerst geauthentiseerd alvorens toegang wordt verleend tot de CIS omgeving.

Communicatie binnen bovengenoemde berichtenservice wordt versleuteld. [redacted]

Monitoring
IBO heeft een geautomatiseerd dashboard om de berichtenservice te monitoren. Documentatie omtrent de inrichting is niet aangetroffen. De IBO Servicedesk heeft een belangrijke rol in het tijdig signaleren van verstoringen in het afleveren van het klantenbestand en notificeert beheerders in geval van een incident.

2.3 Importeren en valideren klantenbestand

Aanbieden klantenbestand door aanbieders

Er is een geautomatiseerd en beveiligd proces aangetroffen dat voorziet in de aanlevering (import en validatie) van het klantenbestand.

Aanbieders leveren tenminste één keer per 24 uur een versleuteld en gecomprimeerd klantenbestand aan. Deze klantenbestanden worden geautomatiseerd gevalideerd op juistheid en volledigheid. Wanneer een klantenbestand onjuist of onvolledig blijkt krijgt de betreffende aanbieder hiervan bericht. De IBO Servicedesk houdt aan de hand van een dashboardmonitor de aanleverstatus bij.

Pas na een succesvolle import van een nieuw klantenbestand worden de oude gegevens verwijderd.

2.4 Logging en monitoring importproces

Vastlegging import- en validatieproces
Wij hebben vastgesteld dat het resultaat van aanleveringen en validatie van klantenbestanden navolgbaar zijn en dat inleesfouten geregistreerd worden. Logging wordt, naast op de servers zelf, separaat op een centrale logvoorziening opgeslagen in een gescheiden beheeromgeving, uitsluitend toegankelijk voor bevoegden. De volledigheid van de logbestanden is herleidbaar en navolgbaar.

Logging importproces
IBO legt vast door welke aanbieder, aan welke bevoegde autoriteit en op welke rechtsgrondslag informatie is verstrekt. De vastlegging wordt gedurende drie jaren bewaard conform artikel 7.1 van het Besluit verstrekking gegevens telecommunicatie.

Logging van beheerdershandelingen
Vastgesteld is dat alle, volgens de norm vereiste beheerdershandelingen worden vastgelegd.

Overzicht bewaartermijnen
Een overzicht met daarin bewaartermijnen, de toelichting op de gegevens, de opslaglocatie, verantwoordelijken en de onderliggende wettelijke bepaling is aangetroffen doch moet geactualiseerd worden.

De klokken van CIS informatiesystemen worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

2.5 Verbindingen CIS server en Blackboxes en webservers

Monitoring
IBO heeft een geautomatiseerd dashboard om verbindingen te monitoren. Documentatie omtrent de inrichting is niet aangetroffen.

Bevragingen door BOID's vanuit het externe domein worden versleuteld verzonden naar de webservers.

Beveiliging ongeautoriseerd gebruik
Gebruikers worden voorafgaand aan een bevraging geauthentiseerd en moeten o.a. beschikken over een gebruikersaccount. De webserver is conform best practices van de leverancier gehardend.

Content-scanning op koppelvlakken

Servers in het CIS domein worden real-time gescand op malware. De antimalwareproducten worden regelmatig geüpdate en zijn actueel ten tijde van het onderzoek.

[redacted]

Het schonen van internet- en e-mailverkeer op de IBO kantooromgeving wordt uitgevoerd door de leverancier van deze omgeving en valt buiten de scope van dit onderzoek.

2.6 CIS server en certificatenbeheer

Proces certificatenbeheer

IBO hanteert een proces m.b.t. het certificatenbeheer. Op basis van procesregistraties is vastgesteld dat de registratie, uitgifte en blokkering van certificaten navolgbaar, herleidbaar en gecontroleerd verloopt. Certificaten zijn persoonsgebonden [redacted]. IBO heeft inzicht in het aantal uitgegeven certificaten en actieve eindgebruikers.

Bevragingen

Eindgebruikers kunnen middels bevragingen informatie uit het CIS opvragen. Deze bevragingen vinden uitsluitend plaats met vooraf gedefinieerde, niet aan te passen queries. De contextinformatie van de bevraging (zonder de vraag en het antwoord) wordt, in overeenstemming met de bewaartermijn in artikel 7 van het Besluit verstrekking gegevens telecommunicatie, gedurende drie jaar bewaard.

Om de legitimiteit van elke bevraging achteraf te kunnen verifiëren is het noodzakelijk dat eindgebruikers het resultaat van reeds uitgevoerde bevragingen en de content informatie niet kunnen wijzigen. De applicatie is zodanig ingericht dat deze geen functionaliteit biedt om uitgevoerde bevragingen te verwijderen. Afgeronde verzoeken worden automatisch verwijderd na drie dagen.

Rapportagefunctie aantal bevragingen

Jaarlijks dient IBO te rapporteren over het aantal uitgevoerde bevragingen conform artikel 8 van het Besluit verstrekking gegevens telecommunicatie. Ten aanzien van de rapportagefunctie van de CIS applicatie is vastgesteld dat de mogelijkheid voor het genereren van de wettelijke rapportages aanwezig is in het systeem.

Backup en recovery

Voor de continuïteit en integriteit van het dienstverleningsproces is het van belang dat kopieën van programmatuur en gegevens aanwezig zijn in geval van een grote verstoring. Het backupbeleid is gefragmenteerd aanwezig. Het regulier testen van een backup en een restore wordt niet periodiek uitgevoerd en de rapportage hierover vindt beperkt plaats. Back-ups worden op mobiele gegevensdragers opgeslagen en op een externe locatie bewaard.

2.7 CIOT portal (cliëntside)

Toegangsbeleid eindgebruikers

Gebruikers worden voorafgaand aan een bevraging geauthentiseerd en moeten o.a. beschikken over een gebruikersaccount. Het aanvragen van een gebruikersaccount verloopt volgens procedure via een decentrale, lokale beheerder van een BOID die geautoriseerd is een aanvraag in te dienen bij de IBO servicedesk. Het toegangsbeleid bij de BOID's valt buiten scope van dit onderzoek.

Logging van gebruikershandelingen

Zowel succesvolle als niet-succesvolle inlogpogingen op de CIS applicatie worden gelogd. Daarnaast worden activiteiten van eindgebruikers (gepseudonimiseerd) gelogd. Uitgevoerde handelingen zijn herleidbaar naar degene die de bevraging heeft uitgevoerd.

3 Verantwoording onderzoek

3.1 Doelstelling

De doelstelling van dit onderzoek is het verschaffen van inzicht in mogelijke risico's op het gebied van de gegevensaanlevering en -verstrekking bij IBO. Het resultaat van het onderzoek stelt de minister van Justitie en Veiligheid in staat verslag te doen conform de wettelijke bepaling in artikel 8 van het Besluit verstrekking gegevens telecommunicatie.

3.2 Werkzaamheden, periode van uitvoering

Voor dit onderzoek is gedurende de periode mei t/m augustus 2017 door de ADR dossieronderzoek uitgevoerd, zijn interviews gehouden en zijn waarnemingen ter plaatse uitgevoerd. Het onderzoeksdossier blijft op locatie van IBO en zal daar worden gearchiveerd. Er is geen onderzoek gedaan naar de kwaliteit van de verstrekking van gegevens en de bevraging van gegevens.

Omdat de uitvoering van het onderzoek vertraging heeft opgelopen zijn er planningsconflicten ontstaan met andere lopende ADR onderzoeken. Hierdoor hebben de onderzoekswerkzaamheden voor IBO enige tijd stil gelegen waardoor dit rapport met vertraging is opgeleverd.

3.3 Object van onderzoek, afbakening

Het object van onderzoek is het proces van gegevensaanlevering en -verstrekking bij IBO. Dit is afgebakend tot het beheer van het CIOT Informatiesysteem (CIS) bestaande uit de volgende vier beheerprocessen, die in §2.1.1 t/m §2.1.4 van dit rapport zijn beschreven:

- Incidentmanagement;
- Change management
- Servicelevel- en suppliermanagement;
- Logische toegangsbeveiliging.

Daarnaast zijn acht onderwerpen onderzocht die verband houden met de risico's in de uitvoering van de gegevensaanlevering en —verstrekking in het CIS. Deze acht onderwerpen volgen het chronologische proces van gegevensaanlevering en –verstrekking en zijn in zes paragrafen (§2.2 t/m §2.7) beschreven:

- Digikoppeling;
- Importeren en valideren;
- Logging en monitoring importproces;
- Blackboxes;
- Verbinding CIS server en Blackboxes;
- CIS server en certificatenbeheer;
- Verbinding CIS server en webserver;
- CIOT portal (cliëntside).

3.4 Gehanteerde Standaard

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

Met dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd. In het rapport zijn daarom enkel de feitelijke bevindingen beschreven en is geen samenvattende conclusie of eindoordeel opgenomen. Indien aanvullende werkzaamheden zouden zijn verricht of indien er een

assuranceopdracht zou zijn uitgevoerd, zouden wellicht andere onderwerpen zijn geconstateerd en gerapporteerd.

3.5 Kwaliteitsborging

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. Gelet op de vertrouwelijkheid van de informatie in het dossier blijft het dossier op locatie bij IBO.

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

3.6 Verspreiding rapport

De opdrachtgever, mw. mr. J.G. Vegter, directeur-generaal Rechtspleging en Rechtshandhaving (DGRR) van het Ministerie van Justitie en Veiligheid, is eigenaar van dit rapport. De opdrachtgever is verantwoordelijk voor de verdere verspreiding van het 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, 20 december 2017

w.g.

Projectleider
Auditdienst Rijk

Bijlage 1: Managementreactie Justid/IBO

Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag

Informatiepunt Bijzondere Opsporingsonderzoeken
Turfmarkt 147
2511 DP Den Haag
Postbus 484
2501 CL Den Haag
www.justid.nl | www.ciot.nl

Datum
15 december 2017

memo

Managementreactie Justid/IBO op Rapport van bevindingen IBO beheerprocessen 2016

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. U bent derhalve verzocht onderzoek te doen naar het technisch beheer, functioneel beheer en applicatiebeheer voor het CIOT Informatiesysteem (CIS). Dit beheer wordt uitgevoerd door IBO, onderdeel van Justid.

Ik heb kennisgenomen van het onderzoeksrapport "IBO beheerprocessen 2016", opgesteld door de ADR in opdracht van DGRR. In de rapportage zijn de bevindingen van dit onderzoek opgenomen. Ik stel met tevredenheid vast dat u met succes inzicht heeft kunnen verschaffen. U stelt onder meer vast dat de beheersmaatregelen bij het CIOT toereikend zijn om de risico's op inbreuken op beveiliging of integriteit van de informatie-uitwisseling te beperken.

Enkele bevindingen van de ADR, die met name betrekking hebben op de interne beheerprocessen van het CIOT, vragen nadere aandacht. Justid/IBO neemt de bevindingen in het rapport over. Ten aanzien van een aantal bevindingen zijn waar nodig door Justid/IBO reeds verbeteracties ingezet. Hieronder ga ik nader in op een aantal van deze specifieke punten.

1. *Beveiliging digikoppeling berichtenservice*
   IBO maakt t.b.v. het Elektronisch Berichten Verkeer (EBV) gebruik van de Digikoppeling van de JUstitie BErichten Service (Jubes). Jubes functioneert hierbij als een "berichtenmakelaar" en IBO is afnemer. Telecomaanbieders sluiten aan via de CIOT gegevensaanlevervoorziening hetgeen hen in staat stelt om het klantenbestand aan IBO te leveren. Telecomaanbieders worden eerst geauthentiseerd alvorens toegang wordt verleend tot de CIS omgeving. Communicatie binnen bovengenoemde berichtenservice wordt versleuteld. [redacted]

[redacted]

2. *Logische toegangsbeveiliging CIOT domein*
   Toegang tot de CIS applicatie voor eindgebruikers vindt plaats op basis van 2-factor authenticatie. [redacted]

3. *Logging en monitoring importproces*
   ADR stelt vast dat IBO voldoet aan de normen voor vastlegging import- en validatieproces, logging importproces en logging van de beheerdershandelingen.

   ADR stelt vast dat een overzicht met daarin bewaartermijnen, de toelichting op de gegevens, de opslaglocatie, verantwoordelijken en de onderliggende wettelijke bepaling is aangetroffen doch geactualiseerd moet worden. Het management van IBO onderkent deze verbetermaatregel en zal deze in het voorjaar van 2018 ter hand nemen.

4. *Verbindingen CIS server en Blackboxes en webservers*
   ADR stelt vast dat bevragingen door BOID's vanuit het externe domein worden versleuteld verzonden naar webservers, de webserver conform best practices van de leverancier is gehardend en de servers in het CIS domein real-time gescand worden op malware en dat op deze punten wordt voldaan aan de normen.

   [redacted]

5. *CIS server en certificatenbeheer – Back-up en recovery*
   ADR stelt vast dat IBO voldoet aan de normen voor proces certificatenbeheer, bevragingen en de rapportagefunctie aantal bevragingen. Ten aanzien van backup en recovery stelt ADR vast dat voor de continuïteit en integriteit van het dienstverleningsproces het van belang is dat kopieën van programmatuur en gegevens aanwezig zijn in

geval van een grote verstoring. Het backupbeleid is gefragmenteerd aanwezig. Het regulier testen van een backup en een restore wordt niet periodiek uitgevoerd en de rapportage hierover vindt beperkt plaats. Het management van IBO heeft aangegeven dat in 2018 deze omissie wordt opgepakt en dat het backupbeleid wordt aangepast.

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

Justid/IBO hoopt met deze reactie inzicht gegeven te hebben in de stand van zaken met betrekking tot de bevindingen van de audit.

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