Auditdienst Rijk
Ministerie van Financiën

~~departementaal VERTROUWELIJK~~

Onderzoeksrapport
CIOT Beheer 2018, 2019 en 2020

Definitief

Colofon

Titel	CIOT Beheer 2018, 2019 en 2020
Uitgebracht aan	Directeur-generaal Rechtspleging en Rechtshandhaving
Datum	29 juni 2021
Kenmerk	2021-0000122883
Versie	V1.0

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Managementsamenvatting

Conform het Besluit verstrekking gegevens telecommunicatie moet de minister van Justitie en Veiligheid jaarlijks verslag doen van audits naar de uitvoering van het besluit. De audits hebben betrekking op de aanbieders van openbare telecommunicatiediensten of telecommunicatienetwerken, de beheerder van het CIOT-informatiesysteem en de gebruikers van dit systeem.

De Auditdienst Rijk (ADR) heeft in de periode oktober 2020 tot en met februari 2021 in opdracht van de directeur-generaal Rechtspleging en Rechtshandhaving (DGRR) een onderzoek uitgevoerd naar de beheersing van het CIOT Informatie Systeem (CIS) bij het Informatiepunt Bijzondere Opsporingsonderzoeken (IBO) over de jaren 2018, 2019 en 2020. De gehanteerde peildatums zijn 1 december 2018, 1 december 2019 en 1 oktober 2020.

Het voor dit onderzoek gehanteerde normenkader bevat zes thema's gebaseerd op het Besluit verstrekking gegevens telecommunicatie (en de Baseline Informatiebeveiliging Overheid (BIO)). Vanwege technische beperkingen heeft IBO bij vier van de zes thema's geen (historische) informatie gedocumenteerd waardoor wij het bestaan van (delen van) de maatregelen voor de jaren 2018 en 2019 niet hebben kunnen vaststellen.

IBO laat voor de jaren in scope van ons onderzoek verbetering zien in zowel het vastleggen en formaliseren van maatregelen als in het aantoonbaar voldoen aan de beheeruitgangspunten. Onder andere door een in 2019 opgesteld en geformaliseerd logbeleid en de tijdig met securityupdates bijgewerkte in het onderzoek betrokken servers.

Verbetering is echter mogelijk op het gestructureerd en beheerst uitvoeren van processen van een aantal thema's. Zo is vastgestelde en/of geformaliseerde documentatie niet voor alle thema's beschikbaar en daarnaast is niet overal de controle en monitoring ingericht. Bijvoorbeeld de controle op interne IBO-accounts en bij de monitoring en analyse van logging. Voorts hebben wij vastgesteld dat verbindingen naar de IBO-omgeving worden versleuteld maar dat dit in één geval niet conform de NCSC-richtlijn gebeurt, dat gegevens in de database en de applicatie niet worden versleuteld en dat er ongeautoriseerde administratoraccounts aanwezig zijn.

Wij adviseren om de niet noodzakelijke autorisaties te verwijderen en de server conform de NCSC-richtlijn te configureren. Daarnaast adviseren wij de interne controlefunctie binnen IBO steviger vorm te geven. Onder andere ten aanzien van de controle op accounts en bij de monitoring en analyse van logging, alsook het rapporteren over informatiebeveiligingsgebeurtenissen. Tevens adviseren wij documentatie waar nodig voor IBO te verbijzonderen en conceptversies van documenten definitief te maken en te formaliseren.

2 Inleiding opdracht

2.1 Aanleiding onderzoek en opdrachtgever

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

a) de werking[1] van het systeem;
b) de kwaliteit van de verstrekking van gegevens;
c) de bevraging van gegevens.

De Auditdienst Rijk (ADR) heeft in de periode oktober tot en met februari 2021 in opdracht van de directeur-generaal Rechtspleging en Rechtshandhaving (DGRR) een onderzoek uitgevoerd naar de beheersing van het CIOT Informatie Systeem (CIS) bij IBO. ADR heeft hiertoe met de opdrachtgever een intakegesprek gevoerd en zijn afspraken vastgelegd in de getekende opdrachtbevestiging met kenmerk 2020-0000185732. De onderdelen b. en c. 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 dit CIOT Beheer onderzoek.

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

2.2 Doelstelling en onderzoeksvraag

De doelstelling van het onderzoek is inzicht te geven of het ontwerp (opzet) en de operationele toepassingen (bestaan) van de beheersmaatregelen, in lijn met het Besluit, invulling geven aan de beheersingsdoelstellingen zoals geformuleerd in het normenkader voor het CIOT-beheer. Van de eventuele afwijkingen wordt het restrisico bepaald.

Met de resultaten van dit onderzoek kan de DGRR de minister van JenV informeren waarna de minister verslag kan doen aan de Tweede kamer conform artikel 8 van het Besluit.

In dit onderzoek wordt de volgende onderzoeksvraag beantwoord:

> "Welke beheersmaatregelen heeft IBO in opzet en bestaan voor het CIS-beheer geïmplementeerd om te voorzien in de in het normenkader geformuleerde beheersdoelstellingen?"

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

[1] Betreft niet de auditterm werking waarmee de effectiviteit over een vooraf bepaalde periode wordt getoetst

2.3 Afbakening

Object van onderzoek is het technisch-, functioneel- en applicatiebeheer gericht op het centrale deel van de CIS-applicatie in beheer bij IBO.

2.4 Context

De afdeling IBO is onderdeel van de Justitiële Informatiedienst (Justid) van het ministerie JenV en voert voor diverse productlijnen, waaronder het CIS, het technisch beheer, het functioneel -en applicatiebeheer uit.

IBO is aangewezen om het verkeer van informatieverzoeken en het antwoord tussen de afnemers w.o. de (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten (BOID's) en aanbieders van telecommunicatiediensten door te geleiden. Doorgeleiding vindt met het CIS geheel geautomatiseerd plaats.

De informatieverzoeken van afnemers hebben betrekking op persoonsgegevens zoals, NAPW[2], IP-adressen, telefoonnummers en e-mailadressen. Deze gegevens worden ten behoeve van opsporingsonderzoek geleverd aan opsporings-, veiligheids- en inlichtingendiensten, die hun bevoegdheid ontlenen aan het Wetboek van Strafvordering.

Telecom- en internetaanbieders zijn verplicht om klantgegevens beschikbaar te stellen voor onderzoek naar criminele activiteiten en leveren elke 24 uur een actueel digitaal bestand van hun klantgegevens aan IBO.

2.5 Leeswijzer

De feitelijke bevindingen van dit onderzoek worden per onderwerp gegroepeerd weergegeven in hoofdstuk 2. Indien nodig worden direct in de tekst de risico's geduid en aanbevelingen gedaan. De verantwoording van het onderzoek is in hoofdstuk 3 beschreven. Hoofdstuk 4 betreft de ondertekening.

[2] Naam, adres, postcode, woonplaats

3 Feitelijke bevindingen

In dit hoofdstuk worden de feitelijke bevindingen van het onderzoek weergegeven. Aanbevelingen worden in de tekst per norm gedaan.

Bij het weergeven van de feitelijke bevindingen in onderstaande paragrafen volgen wij de volgorde van behandelde onderwerpen uit het normenkader (zie ook hoofdstuk 3.1).

Als geen jaartal wordt vermeld dan gelden bevindingen voor alle jaren (2018, 2019 en 2020) in scope van het onderzoek. Zo niet, dan wordt het specifieke jaar vermeld.

3.1 Security algemeen

Norm: Gevoelige informatie wordt versleuteld verzonden (in transit) en opgeslagen (at rest) volgens passende standaarden.

In het 'Handboek Beveiliging' van Justid van 2011 dat door IBO wordt gehanteerd, wordt ingegaan op de versleuteling van netwerkverkeer en gegevensopslag. Hierin is opgenomen dat het management op basis van een risicoafweging bepaalt welke gegevens versleuteld moeten worden. Een overzicht waaruit blijkt welke gegevens door IBO versleuteld zouden moeten worden is niet aangereikt.
Justid heeft een encryptiebeleid uit 2019, hierin ontbreekt de beschrijving van de opslag van gevoelige gegevens. In het IBO integraal beveiligingsplan uit 2019 is een paragraaf gewijd aan cryptografische beheersmaatregelen. Dit beslaat niet de onderwerpen zoals het versleuteld verzenden en opslaan van gevoelige informatie.

<u>Transport aanlevering klantenbestand</u>
Wij hebben vastgesteld dat:

- in 2019 en 2020 de server bij IBO die het klantenbestand van de telecomaanbieders ontvangt is ingesteld om niet versleutelde verbindingen (over HTTP) te ontvangen. Vanwege het gebrek aan historische gegevens konden wij de situatie niet vaststellen voor het jaar 2018.
- in 2020 het klantenbestand zonder transportencryptie wordt doorgestuurd voor ontsleuteling. Vanwege het gebrek aan historische gegevens konden wij de situatie niet vaststellen voor de jaren 2018 en 2019.

Wij merken op dat klantenbestand zelf is versleuteld (zie hieronder bij 'Opslag aanlevering klantenbestand'). Op het moment dat deze encryptie door omstandigheden niet werkt biedt transportversleuteling uitkomst om onbevoegde inzage te voorkomen.

<u>Transport CIS-bevragingen</u>
Wij hebben vastgesteld dat:

- bevragingen door de BOID's[3] (CIS-afnemers) over een versleutelde verbinding naar IBO worden verzonden;
- de ontvangende server niet conform de NCSC 'ICT-beveiligingsrichtlijnen voor TLS' is geconfigureerd.

[3] Bijzondere Opsporings-en Inlichtingendiensten

Eerder ADR-onderzoek heeft uitgewezen dat in 2018 en een deel van 2019 de verbinding tussen de webserver en de CIS-applicatie niet werd versleuteld (zie rapport ADR CIOT Beheer 2017). Wij hebben vastgesteld dat in 2020 de communicatie tussen de webserver en de CIS-applicatie wel versleuteld plaatsvindt.

Opslag aanlevering klantenbestand
Wij hebben vastgesteld dat in 2019 en 2020 een door een telecomaanbieder aangeleverd klantenbestand is versleuteld. Vanwege het gebrek aan historische gegevens konden wij dit niet vaststellen voor het jaar 2018.

Opslag CIS-bevragingen
Wij hebben vastgesteld dat gegevens in de databases en de CIS-applicatieserver onversleuteld worden opgeslagen. Indien een onbevoegde zich toegang weet te verschaffen tot deze gegevens kan dit mogelijk leiden tot manipulatie of inzage in deze gegevens.

Wij bevelen aan om de server conform de NCSC 'ICT-beveiligingsrichtlijnen voor TLS' te configureren. Overweeg de ontvangende server van het klantenbestand geschikt te maken voor ontvangst van versleuteld verkeer.
Laat het IBO-management:

- op basis van een risicoafweging bepalen welke gegevens versleuteld moeten worden;
- onderzoeken of de situatie van het CIS een specifiek CIS encryptiebeleid rechtvaardigt;
- onderzoeken welke mogelijkheden er zijn om gegevens in de database en applicatieserver te versleutelen en hoe goed sleutelbeheer hierop is te voeren.

Norm: Alleen de (centrale) CIOT Servicedesk is bevoegd certificaten uit te geven (c.q. pending certificaten te activeren). Dit houdt in dat alleen de CIOT Servicedesk het door een gebruiker aangevraagde certificaat goedkeurt en deze activeert.

In het IBO-organisatierapport uit 2016 is opgenomen dat de Servicedesk verantwoordelijk is voor het accountbeheer van CIS-gebruikers (BOID's). In een werkinstructie uit 2018 wordt de omgang en behandeling van een certificaat voor gebruikers beschreven. Pas nadat de Servicedesk een account heeft aangemaakt kan de gebruiker een certificaat downloaden en installeren en van het CIS gebruik maken. Het wachtwoord wordt separaat per post verzonden.

Wij hebben vastgesteld dat in 2020 zowel Servicedesk medewerkers als IBO-beheerders geautoriseerd zijn om een gebruikersaccount en een certificaat aan te maken. Vanwege het gebrek aan historische informatie konden wij dit niet voor 2018 en 2019 vaststellen.
N.B. door de Covid-19 situatie in 2020 mochten de servicedeskmedewerkers geen werkzaamheden uitvoeren in de productieomgeving. Per interview hebben wij vernomen dat, vanwege de borging van de continuïteit in de aanmaak van nieuwe accounts en uitgifte van certificaten, de CIS-beheerders op aanwijzing van het IBO-management tijdelijk ook gebruikersbeheer werkzaamheden uitvoeren.

Norm: Alle medewerkers betrokken bij de productlijn CIOT beschikken bij indiensttreding over een VOG en hebben een geheimhoudingsverklaring

getekend, waarin is vastgelegd dat de persoon ook na beëindiging van de functie hieraan gehouden is. Daarnaast beschikken personen met een vertrouwensfunctie over een geldige VGB-B.

VOG en geheimhoudingsverklaring

In het beleid Veilig Personeel van Justid uit 2019 is opgenomen dat elke medewerker bij indiensttreding over een Verklaring Omtrent het Gedrag (VOG) moet beschikken met een geldigheidsduur van vijf jaar. Externe medewerkers zijn daarnaast verplicht tot het tekenen van een geheimhoudingsverklaring. Voor interne medewerkers geldt het afleggen van de eed of gelofte.

In de geheimhoudingsverklaring voor externe medewerkers is met de verwijzing naar artikel 272 in het Wetboek van Strafrecht opgenomen dat de geheimhouding ook van toepassing blijft na beëindiging van contract of ontslag.

Bij zowel de indienst-, uitdiensttreding en bij wijziging van de functie gebruikt IBO in de jaren in scope een controlelijst waarop te nemen activiteiten zijn vermeld. Als de activiteit is afgerond wordt hiervoor door het management of teamleider geparafeerd met vermelding van de datum. Op de controlelijst bij uitdiensttreding van interne medewerkers is de activiteit 'Ondertekenen van de geheimhoudingsverklaring bij ontslag' opgenomen.

Wij hebben vastgesteld dat:

- Vier interne IBO-medewerkers die in dienst zijn getreden in 2018 en 2019 niet over een geldige VOG beschikten.
- De medewerker die in 2020 in dienst trad bij IBO over een geldige VOG beschikte.
- Drie externe medewerkers die in dienst zijn getreden in 2018 en 2019 niet beschikten over een geldige VOG.

De medewerkers met een ongeldige VOG beschikten wel over een geldige Verklaring van Geen Bezwaar (VGB).

Wij hebben vastgesteld dat zes van de zeven medewerkers die in 2018, 2019 en 2020 bij IBO in dienst zijn getreden een geheimhoudingsverklaring hebben getekend en/of de eed of gelofte hebben afgelegd.

Wij hebben per inspectie van de controlelijst vastgesteld dat:

- In 2019 de actie 'Ondertekenen van de geheimhoudingsverklaring bij ontslag' niet is geparafeerd voor een interne medewerker die in 2019 uitdienst is gegaan.
- Eén geheimhoudingsverklaring van een medewerker die in 2020 uitdienst is gegaan niet is aangeleverd ondanks dat deze was geparafeerd. IBO heeft in reactie hierop aangegeven dat bij vertrek niet opnieuw een geheimhoudingsverklaring wordt getekend, maar dat de medewerker mondeling wordt gewezen op de verplichtingen jegens de geheimhoudingsplicht na uitdiensttreding.

VGB-B

In het beleid Veilig Personeel van Justid uit 2019 is opgenomen dat medewerkers die een vertrouwensfunctie vervullen in bezit moeten zijn van een Verklaring van Geen Bezwaar (VGB) op niveau B.

In het Besluit aanwijzing vertrouwensfuncties IBO 2017 zijn voor IBO vier type vertrouwensfuncties aangewezen:

1. Manager IBO — Middenmanager (1x);
2. Teamleider DevOps - Operationeel manager (1x);
3. (Senior) Ops engineer – Senior medewerker IV (6x);
4. Externe tijdelijke medewerker (5x).

Wij hebben vastgesteld dat voor 2018, 2019 en 2020 er een geldige VGB-B is afgegeven voor:

- 1x Manager IBO;
- 1x Teamleider DevOps;
- 6x (Senior)Ops engineers.

IBO kon geen overzicht aanleveren waaruit wij eenduidig konden afleiden welke externe medewerkers in welk jaar werkzaam waren in een vertrouwensfunctie. Wij hebben op basis van aangeleverde informatie vastgesteld dat in totaal 3 externe medewerkers in 2018 en 2019 voor het CIS werkzaam zijn geweest. Deze 3 externe medewerkers beschikten in 2018 en 2019 over een geldige VGB. Van 1 externe medewerker was de VGB geldig tot september 2020. Per mededeling van IBO hebben wij vernomen dat er geen externe beheermedewerkers in een vertrouwensfunctie in 2020 aan het CIS werkzaam waren maar dat het softwareontwikkelaars betreft die geen toegang hadden tot de productieomgeving.

Wij bevelen aan om te zorgen dat IBO over een duidelijke personeelsregistratie beschikt waarin wordt vastgelegd welke personen in welke periode werkzaamheden voor het CIS hebben uitgevoerd. In geval van een vertrouwensfunctie dient duidelijk aangegeven te worden dat dit een vertrouwensfunctie 'Externe tijdelijke medewerker' betreft, zoals in het aanwijzingsbesluit is opgenomen.
Maak expliciet waar de vertrouwensfunctie 'externe tijdelijke medewerkers' op betrekking heeft. Bijvoorbeeld door aan te geven in het aanwijzingsbesluit dat het wel betrekking heeft op de Ops engineers (beheerders) maar niet op Developers (ontwikkelaars). Verder bevelen wij aan de relatie tussen een VOG en een VGB in beleid duidelijker aan te (laten) brengen zodat overlap wordt voorkomen.
Laat externe medewerkers bij aanvang van werkzaamheden aan het CIS een geldige VOG overleggen aan IBO.

3.2 Invoer en verwerking

Norm: Er moeten controles worden uitgevoerd op de invoer van gegevens (klantenbestand). Daarbij wordt minimaal gecontroleerd dat het bestand 1x 24 uur wordt aangeleverd, op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en naamgeving van het bestand.

IBO heeft maatregelen in de vorm van automatische controlescripts ingericht, om de door de aanbieder geleverde klantgegevens in het klantenbestand te controleren en te valideren voordat ze worden opgenomen in het CIS. Deze controlevereisten zijn in 2017 door IBO beschreven in een handleiding 'Samenstellen Klantenbestanden' die bestemd is voor telecomaanbieders. Telecomaanbieders kunnen dezelfde controlescripts toepassen voor de dagelijkse verzending van het klantenbestand.

De status van de dagelijkse aanlevering door telecomaanbieders wordt door de IBO Servicedesk op werkdagen 1 keer per dag gemonitord en in een statusoverzicht opgenomen. In geval van een verkeerde aanlevering neemt de Servicedesk van IBO contact op met de betreffende telecomaanbieder en volgt regstratie in het incidentenregistratiesysteem.

Per inspectie van het statusoverzicht over 2020 hebben wij vastgesteld dat een niet succesvolle aanlevering van klantenbestanden in een weekend in december 2020 betrekking had op ICT uitval in de IBO omgeving. Hierdoor zijn gedurende twee dagen geen actuele klantengegevens van telecomaanbieders in het CIS geladen. IBO heeft dit op de eerstvolgende werkdag opgemerkt en direct opgelost. Een niet succesvolle aanlevering in januari 2020 dateert reeds uit mei 2019 waarbij met name aan de kant van de telecomaanbieder verschillende problemen zijn geconstateerd zoals het niet op de hoogte zijn van de bestandsvereisten, het niet beschikken over validatie schema's, een verlopen certificaat en het gebruik van een foutieve URL. Na herhaaldelijke aansporing van IBO is de eerste correcte aanlevering op september 2020 hervat. Het statusoverzicht voor de jaren 2018 en 2019 is niet beschikbaar.

Wij bevelen aan om in de audit naar de CIOT telecomaanbieders, voorzover dat nog niet is gebeurd, de validatie conform de handleiding 'Samenstellen Klantenbestand' als norm toe te voegen. Daarnaast bevelen wij aan om te onderzoeken of monitoring van aanlevering van klantenbestanden in het weekend noodzakelijk inzake de beschikbaarheid van actuele informatie voor opsporingsactiviteiten.

Norm: Een match tussen bevraging en het bestand vindt slechts plaats aan de hand van een in het verzoek opgenomen gegevens betreffende naam, adres, postcode, huisnummer plus nummertoevoeging of nummer.

Norm: Er worden niet meer gegevens verwerkt (doorgeleiding) in het CIS dan noodzakelijk.

In het CIS zijn technische maatregelen geïmplementeerd zodat een bevraging alleen kan worden gedaan aan de hand van naam, adres, postcode, huisnummer plus nummertoevoeging of telefoonnummer. Wij hebben vastgesteld dat de database alleen informatie accepteert die past in de vooraf gedefinieerde databasevelden waardoor doorgeleiding van andere soorten gegevens niet mogelijk is.

In de CIS-testomgeving (representatief voor productieomgeving) hebben wij vastgesteld dat in 2020 informatie in een bevraging beperkt is tot de naam, adres, postcode, huisnummer plus nummertoevoeging of telefoonnummer. Omdat er geen historische informatie beschikbaar is konden wij dit niet vaststellen voor 2018 en 2019.

Norm: Bevragingen en doorgeleiding van de match door het CIS kan in principe 24 uur per dag plaatsvinden. Voor eindgebruikers geldt een minimale beschikbaarheid van 99%.

Afspraken over de beschikbaarheid, zoals de minimale beschikbaarheid van 24 uur, zijn opgenomen in een Diensten Niveau Overeenkomst (DNO) tussen IBO en de gebruikers (BOID's).
Op basis van documentatie over de beschikbaarheid van het CIS-systeem hebben wij de volgende beschikbaarheidspercentages vastgesteld: 99,98% (2018), 99,965% (2019) en 99,97% (2020).

Om buiten kantooruren de afspraken over de beschikbaarheid te waarborgen heeft IBO een piketregeling in gebruik. In de praktijk werd een piketrooster in 2018 en 2019 voor de technisch beheerders als weekenddienst ingevuld. In 2019 en 2020 is dit uitgebreid en gebeurde dit op basis van weekdiensten. Piketmaatregelen waren in 2018 nog niet beschreven. IBO heeft in 2019 een piket werkinstructie in gebruik genomen.

Wij hebben geen informatie aangetroffen die voorziet in de technische borging (in architectuur) van de beschikbaarheidseis van 24 uur.

Wij bevelen aan om de gewenste beschikbaarheidseisen in bijvoorbeeld een architectuurontwerp vorm te geven die als leidraad kan dienen voor eventueel nog te nemen technische maatregelen zoals de redundantie van componenten.

3.3 Logische toegangsbeveiliging

Algemeen

Omdat er voor het jaar 2018 geen formele gebruikerstoegangsverleningsprocedure aanwezig is hebben wij voor meerdere normen met betrekking tot logische toegangsbeveiliging de situatie in 2018 in opzet niet kunnen vaststellen. Wanneer dit wel het geval is wordt dit expliciet benoemd.

In 2019 en 2020 hanteerde IBO het Logisch Toegangsbeveiligingsbeleid d.d. 2019 van Justid als formele gebruikerstoegangsverleningsprocedure. Hierin zijn onder andere procedures opgenomen omtrent de logische toegangsbeveiliging en de omgang met wachtwoorden. In de bevindingen hieronder wordt dan ook regelmatig naar dit beleid verwezen. Wanneer een specifieke beleidssituatie van toepassing is dan wordt dit als zodanig benoemd.

Norm: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

Norm: Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.

Norm: Er is een actueel mandaatregister waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.

In 2019 en 2020 hanteerde IBO het Logisch Toegangsbeveiligingsbeleid d.d. 2019 van Justid als formele gebruikerstoegangsverleningsprocedure voor interne gebruikersaccounts. In dit beleid is opgenomen dat voor IT-systemen een autorisatiematrix moet worden opgesteld die jaarlijks door de verantwoordelijk leidinggevende moet worden beoordeeld.

De aangeleverde autorisatiematrices voor de jaren 2018 en 2019 zijn niet voor akkoord getekend door het IBO-management, zijn niet gedateerd en ontbreekt een versienummer. De aangeleverde autorisatiematrix voor 2020 is wel door het IBO-management voor akkoord getekend.

In verschillende werkinstructies is beschreven dat de Servicedesk is geautoriseerd om externe gebruikersaccounts van het CIS (de accounts voor de BOID's) uit te geven.

Van alle indiensttredingen bij IBO van de jaren in scope van zowel interne (7) als externe medewerkers (3) hebben wij de controlelijsten ingezien. Wij merken op dat de controlelijsten niet eenduidig door IBO worden opgeslagen.

Voor twee interne medewerkers die in 2018 en 2019 bij IBO in dienst zijn getreden hebben wij niet kunnen vaststellen dat conform de autorisatieprocedure is gehandeld.

Wij hebben vastgesteld dat voor het toekennen en intrekken van gebruikersaccounts bij de BOID's:

- Voor zowel de aanvraag van een nieuw account als het opheffen van een bestaand account in 2018 niet is opgenomen op wie het account betrekking heeft.
- Voor het opheffen van een bestaand account in 2020 niet is opgenomen op wie het account betrekking heeft.
- Twee aanvragen in 2020 als één melding zijn geregistreerd.

Wij adviseren om een overkoepelende procedure voor het toewijzen of intrekken van toegangsrechten voor externe CIS-gebruikers op te stellen, deze procedure te formaliseren en nauwgezet toe te passen. Completeer de administratie waar mogelijk naar aanleiding van geconstateerde verschillen. Regel een controlemechanisme in voor het uitgeven van de externe accounts, zodat aantoonbaarheid achteraf geborgd is.

Norm: Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.

Het logisch toegangsbeveiligingsbeleid van Justid, d.d. 2019 beschrijft dat alle gebruikersaccounts en bijbehorende rechten twee keer per jaar moeten worden beoordeeld door de leidinggevende en daarnaast behoren uitgegeven speciale bevoegdheden minimaal ieder kwartaal te worden beoordeeld. IBO heeft een RACI-tabel uit 2020 waarin is opgenomen wie (eind)verantwoordelijk is voor de controle van zowel de interne IBO-gebruikersaccounts als de externe gebruikersaccounts.

Wij hebben niet kunnen vaststellen dat controle heeft plaatsgevonden op de interne IBO-gebruikersaccounts.
IBO heeft niet vastgesteld dat uitgegeven accounts juist en geautoriseerd zijn.

Voor de controle van externe gebruikersaccounts worden de BOID's maandelijks verzocht de door IBO uitgegeven accounts te controleren op actualiteit. Wij hebben vastgesteld dat in een door IBO in 2018 verzonden bericht de lijst van geautoriseerden niet is meegestuurd. In 2019 worden bevestigingen of reacties van deze controle niet altijd door de BOID's geretourneerd. Hierdoor heeft IBO niet kunnen vaststellen dat de controle door de betreffende BOID is uitgevoerd. Voor 2020 zijn er geen bevindingen.

Wij adviseren de interne gebruikersaccounts (inclusief beheeraccounts) binnen IBO conform het beleid minimaal eenmaal per half jaar aantoonbaar te beoordelen. Daarnaast adviseren wij om aantoonbaar te voldoen aan de werkinstructie zoals het registreren van verzonden rappel ten behoeve van de controle van externe gebruikersaccounts zodat de administratie actueel is en toegangsrechten tijdig kunnen worden ingetrokken.

Norm: De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

In het logisch toegangsbeveiligingsbeleid van Justid, d.d. 2019 staat beschreven dat de leidinggevende verantwoordelijk is voor het in gang zetten van het wijzigen of deactiveren/opheffen van het gebruikersaccount wanneer een medewerker van functie wijzigt of de organisatie verlaat.

Wij hebben vastgesteld dat accounts niet meteen worden verwijderd maar eerst worden 'disabled'. Met een disabled account kan niet meer worden ingelogd maar is nog wel aanwezig en behoudt toegekende rechten. IBO heeft medegedeeld dat op deze manier navolgbaarheid van informatie in logging zoals een gebruikersnaam beschikbaar blijft. Er is geen termijn beschreven hoe lang een account de status 'disabled' mag houden.

De status van administratoraccounts in 2018 en 2019 kunnen wij niet vaststellen omdat er inherent aan de technische autorisatievoorziening bij IBO geen historische gegevens beschikbaar zijn. Voor het jaar 2020 hebben wij vastgesteld dat van de acht administratoraccounts er twee accounts van dit type (langer dan 6 maanden) niet actief zijn. Het eerste administratoraccount is van een medewerker die in 2018 binnen IBO van functie is gewisseld. Omdat dit account niet is gedisabled is inloggen in principe mogelijk. Het tweede account heeft de status 'disabled' waardoor inloggen niet mogelijk is.
Misbruik van een administratoraccount kan mogelijk leiden tot (onbeperkte) toegang tot gegevens en ongeautoriseerde uitgifte van rechten.

Wij bevelen aan beide niet gebruikte administratoraccounts te disabelen, de rechten hiervan te ontnemen en beide accounts te verwijderen. Tevens bevelen wij aan om technische maatregelen te treffen (zoals logging op autorisatiebeheer) zodat historische gegevens beschikbaar zijn ten behoeve van de interne controle.

Norm: Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak (need to know/least privileged).

Het logisch toegangsbeveiligingsbeleid Justid, d.d. 2019 beschrijft dat gebruikers toegangsrechten verkrijgen op basis van de principes 'need-to-know' en 'need-to-have'. IBO heeft daarnaast een 'breaking glass' procedure in gebruik waarbij IBO-beheerders buiten kantooruren administratorrechten kunnen krijgen. De procedure mag alleen worden uitgevoerd met toestemming van het IBO-management en alleen indien noodzakelijk, zoals ingeval van een incident.
De 'breaking glass' procedure is volgens mededeling van IBO tweemaal in 2018 en eenmaal in 2019 toegepast. Wij hebben door het ontbreken van informatie niet kunnen vaststellen of de procedure conform geldende beleid is verlopen.

Om de 24 uurs beschikbaarheid te kunnen garanderen draaien vier beheerders van de andere twee productlijnen mee in de CIS piketdienst. Deze vier beheerders hebben vanwege uit te voeren werkzaamheden in geval van aan calamiteit ook toegang tot het CIS.

Wij hebben vastgesteld dat in 2020 er zes ongeautoriseerde accounts met administratorrechten voorkomen. Hiervan dienen twee

administratoraccounts geen doel meer. Het betreft één medewerker uit dienst en één Servicedeskmedewerker die voor de uitvoering van Servicedeskwerkzaamheden geen administrator rechten nodig heeft. Eén van de twee accounts is disabled waarmee niet kan worden ingelogd. De overige vier accounts zijn serviceaccounts.
Omdat er inherent aan de technische autorisatievoorziening geen historische gegevens beschikbaar zijn hebben wij alleen de situatie van 2020 kunnen vaststellen en niet voor 2018 en 2019. Als beheeraccounts met te ruime rechten worden gecompromitteerd dan levert dit een risico ten aanzien van de vertrouwelijkheid en integriteit van gegevens waarbij onbevoegden inzage kunnen krijgen in gegevens of gegevens kunnen manipuleren.

Wij bevelen aan om het aantal administratoraccounts te beperken en niet benodigde accounts te laten verwijderen.

Norm: Toegang tot een account wordt na drie direct achtereenvolgende foutieve inlogpogingen geblokkeerd. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.

In het logisch toegangsbeveiligingsbeleid Justid, d.d. 2019 is opgenomen dat na vijf keer verkeerd inloggen een account minimaal tien minuten moet worden geblokkeerd. Indien er geen lock-out periode kan worden ingesteld, moet het account worden geblokkeerd totdat de gebruiker een verzoek bij de organisatie doet om de blokkade op te heffen. In het IBO integraal beveiligingsplan uit 2019 is opgenomen dat een account na 3 foutieve inlogpogingen moet worden geblokkeerd.

Per inspectie van de wachtwoordpolicyinstellingen hebben wij vastgesteld dat in 2018, 2019 en 2020 na drie foutieve inlogpogingen een account wordt geblokkeerd, dat de tijdsduur dat een account wordt geblokkeerd is vastgelegd en dat vervolgens een beheerder dit account moet deblokkeren.

Norm: User-id's en wachtwoorden zijn persoonsgebonden.

In het logisch toegangsbeveiligingsbeleid Justid, d.d. 2019 is opgenomen dat zowel interne als externe medewerkers toegang verkrijgen tot IT-systemen op basis van een persoonsgebonden gebruikersaccount met wachtwoord. Gebruikersaccounts met een generieke naamgeving zijn niet toegestaan en mogen alleen met geregistreerde goedkeuring van de leidinggevende worden uitgegeven. Hiervoor worden vier verschillende omstandigheden beschreven waarin dit nodig is. Dit zijn de communicatie/systeemgebruikers, noodprocedure, default accounts en leverancier accounts.

Omdat er inherent aan de technische autorisatievoorziening geen historische gegevens beschikbaar zijn hebben wij alleen de situatie van 2020 kunnen vaststellen en niet voor 2018 en 2019.

Wij hebben de aanwezigheid vastgesteld van zeven unieke niet persoonsgebonden serviceaccounts in 2020. Niet vastgesteld is of het IBO-management toestemming heeft verleend voor het gebruik van serviceaccounts en tot welke omstandigheid zoals hiervoor beschreven, deze behoren. Beheeraccounts en accounts van Servicedeskmedewerkers zijn herleidbaar naar een persoon.

Indien een serviceaccount wordt gecompromitteerd kan dat mogelijk leiden tot onbevoegde inzage en manipulatie van gegevens met administratorrechten, waarvan het gebruik niet naar een persoon is te herleiden.

Wij adviseren het gebruik van administratorrechten op serviceaccounts zoveel mogelijk specifiek op de behoefte van de applicatie af te stemmen en de remote access toegang voor deze accounts zoveel mogelijk te beperken.

Norm: De wachtwoordlengte is minimaal acht posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis.

Norm: Het initiële wachtwoord en wachtwoorden die gereset zijn hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.

Norm: Wachtwoorden die voldoen aan het wachtwoordbeleid, hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van zes maanden.

Het Logisch Toegangsbeveiligingsbeleid van Justid, d.d. 2019 stelt eisen aan de lengte van het wachtwoord (minimaal acht karakters), de complexiteit van het wachtwoord en de maximale geldigheidsduur voor een wachtwoord (90 dagen). Initiële wachtwoorden moeten daarnaast bij eerste gebruik worden gewijzigd en mogen één werkdag geldig zijn.

Per inspectie van de wachtwoordpolicyinstellingen hebben wij vastgesteld dat in 2018, 2019 en 2020 een wachtwoord minimaal 12 posities lang moet zijn, dat de optie 'Wachtwoorden moeten voldoen aan complexiteitsvereisten' is ingesteld en dat de maximale geldigheidsduur voor een wachtwoord gelijk is aan 90 dagen.

Wij hebben voor 2018, 2019 en 2020 niet kunnen vaststellen of initiële wachtwoorden voor alle CIS-accounts bij het eerste gebruik worden gewijzigd omdat dit niet technisch maar procedureel wordt afgedwongen.

Voor vijf administratoraccounts hebben wij vastgesteld dat het wachtwoord al langer dan drie jaar niet is gewijzigd. Voor 28 (voornamelijk service-) accounts hebben wij vastgesteld dat het wachtwoord van deze accounts nooit verloopt. Indien het wachtwoord is gecompromitteerd geeft dit hackers langer de tijd om deze accounts te misbruiken.

Wij adviseren onderzoek te doen naar het gebruik van z.g. managed serviceaccounts (MSA's) om zodoende de veiligheid ten opzichte van deze accounts te verbeteren. Met MSA's is geautomatiseerde wachtwoordwijziging mogelijk.

3.4 Vernietiging van gegevens

Norm: In elke informatieverstrekking is een kenmerk vastgelegd aan de hand waarvan kan worden herleid door welke aanbieder, aan welke bevoegde autoriteit en op welke rechtsgrondslag informatie is verstrekt.

Het concept functioneel ontwerp uit 2007 voor het CIS beschrijft de functionele inrichting van het CIS. Hierin is opgenomen dat door de bevrager een kenmerk wordt vastgelegd, hetzij automatisch of via invoervelden.

Per observatie van de invoerschermen van het CIS in 2020 hebben wij vastgesteld dat de verstrekking:

- herleidbaar is naar de telecomaanbieder;
- herleidbaar is naar de bevoegde autoriteit;
- op welke rechtsgrondslag de verstrekking betrekking heeft.

Norm: De vastlegging wordt gedurende drie jaren bewaard.

Er zijn geen minimale bewaartermijnen voor de vastlegging van het kenmerk beschreven voor de jaren 2018 en 2019. In juli 2020 heeft het IBO management een document geformaliseerd waarin per gegevenssoort de bewaartermijn, opslaglocatie, verantwoordelijkheden en onderliggende wetsartikelen zijn opgenomen. In dit document is tevens opgenomen dat de logging met betrekking van de verstrekking drie jaar moet worden bewaard.

Wij hebben vastgesteld dat in 2018 en 2019 de logging inzake bevragingen vijf jaar beschikbaar was waarmee de bewaartermijn van drie jaar is gehanteerd. IBO heeft tijdens dit onderzoek conform het Besluit de bewaartermijn aangepast naar drie jaar.

Norm: In de vastlegging zijn geen gegevens opgenomen die herleidbaar zijn tot personen op wie een verzoek om informatie betrekking heeft.

In de Gebruikershandleiding CIOT-informatiesysteem uit 2015 zijn de vereisten opgenomen voor de gegevensinvoer in het CIS. Per observatie van een CIS bevraging in de testomgeving in 2020 hebben wij vastgesteld dat er geen gegevens in de bevraging worden opgenomen die herleidbaar zijn naar de persoon op wie het verzoek betrekking heeft.
Voor de vastlegging van gegevens bij het doen van een bevraging geldt dat sprake is van een afhankelijkheid van de kwaliteit van invoer bij derden (de BOID gebruiker) die de bevraging doet. In theorie zou een BOID gebruiker gegevens herleidbaar naar een persoon tijdens een bevraging in kunnen invoeren omdat het CIS de vrijheid biedt om vrije tekst in een bevraging op te nemen. IBO voert geen technische controle uit op de invoerwaardes (teksten) in deze velden. In de gebruikershandleiding CIS is niet expliciet opgenomen dat het een BOID gebruiker niet is toegestaan om in het verzoek gegevens op te nemen van personen op wie een onderzoek om informatie betrekking heeft.

Als er gegevens worden opgenomen die herleidbaar zijn tot een persoon op wie een verzoek om informatie betrekking heeft dan is dit strijdig met het Besluit en privacywetgeving.

Wij bevelen aan:

- De gebruikershandleiding op deze vereisten aan te scherpen en in de opleiding voor gebruikers CIS aandacht te besteden aan de invoer van gegevens in het CIS.
- Te onderzoeken wie verantwoordlijk is voor het (technisch) controleren van de vrije invoervelden op de aanwezigheid van persoonsgegevens en of dit past in wet- en regelgeving. Onderzoek daarnaast of dit onderdeel moet zijn van de interne controle bij IBO danwel de CIS onderzoeken bij gebruikers.

3.5 Logging en monitoring

Algemeen

In het concept logbeleid van Justid uit 2018 wordt het onderscheid tussen automatische en handmatige logging beschreven. In 2019 heeft Justid het 'Logging en Monitoring' beleid (hierna Justid logbeleid 2019) vastgesteld

waarin de uitgangspunten van logging zijn opgenomen en is geldig voor de onderzochte jaren 2019 en 2020. In het Justid logbeleid 2019 zijn de minimale informatievereisten waaruit een logregel moet bestaan opgenomen en de plicht om over logbestanden te rapporteren na periodieke beoordeling.
IBO hanteert het Justid logbeleid 2019 inzake de CIS logging.
In de bevindingen hieronder wordt regelmatig naar het Justid Logbeleid uit 2019 verwezen. Wanneer er sprake is van specifiek logbeleid dan wordt dit benoemd.

Norm: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

Norm: Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.

Norm: Logging wordt geaggregeerd op een centraal logbeheersysteem voor analyse en beoordeling.

Norm: Een logregel bevat minimaal:
a. de gebeurtenis;
b. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;
c. het gebruikte apparaat;
d. het resultaat van de handeling;
e. een datum en tijdstip van de gebeurtenis.

Wij hebben vastgesteld dat voor de jaren in 2018, 2019 en 2020:

- activiteiten en gebeurtenissen van gebruikers en van systeembeheerders worden vastgelegd;
- een logregel de gebeurtenis, het gebruikte apparaat, het resultaat van de handeling en een datum en tijdstip van de gebeurtenis bevat;
- gebruikers en beheerders in logregels zijn te herleiden tot een natuurlijk persoon.

Wij hebben vastgesteld dat een verzoek voor handmatige inzage in logging in de productieomgeving in 2018, 2019 en 2020 met betrekking tot het 4-ogen principe anders is afgehandeld dan in de geregistreerde melding in het incidentmanagementsysteem is vermeld.

Medio 2019 heeft IBO een nieuwe centrale logvoorziening in gebruik genomen. Als onderdeel van de centrale logvoorziening is eind 2019 een Security Information & Event Management (SIEM) geinstalleerd voor het monitoren van cyberdreigingen en cybergebeurtenissen. Wij hebben vastgesteld dat nog niet alle CIS componenten zijn aangesloten op de centrale logvoorziening. Daarnaast wordt logging niet periodiek geanalyseerd en beoordeeld.

Wij bevelen aan om de overige CIS-componenten aan te laten sluiten op de centrale logvoorziening. Onderzoek vervolgens de mogelijkheid om de integriteit van de loginformatie veilig te stellen (bijvoorbeeld door het gebruik van hashing op de logging) als onderdeel van de bestaande SIEM tooling.

Vanwege Corona geldt de verplichting voor interne en externe IBO medewerkers (ook ontwikkelaars en testers) om zoveel mogelijk thuis te werken. Om inzicht te krijgen in geslaagde en mislukte inlogsessies op de ontwikkel-, test- en acceptatieomgeving stelt de Informatie Security Officer (ISO) van IBO maandelijks een rapportage op voor het IBO management. Voor de productieomgeving worden geen rapportages opgesteld.

Wij bevelen aan maatregelen te implementeren om de betrouwbaarheid van de handmatige registratie vergroten bijvoorbeeld door monitoring door de ISO. Alhoewel de ISO de eerste stappen heeft gezet om te rapporteren over de telewerkomgving adviseren wij de analyse en beoordeling van lograpportages steviger vorm te geven.

Norm: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.

In het concept Justid Logbeleid uit 2015 is opgenomen dat logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. IBO heeft geen aanvullende maatregelen getroffen (anders dan de beheersingsmaatregelen omtrent logische toegangsbeveiliging) om de integriteit van de logfaciliteit en informatie in logbestanden te beschermen.

Hierdoor ontstaat er een mogelijkheid dat onbevoegden (bewust) of een beheerder (onbewust, per abuis) loginformatie kan verwijderen of aanpassen. Hackers bijvoorbeeld kunnen op deze manier sporen uitwissen.

Wij bevelen aan te onderzoeken welke maatregelen IBO moet implementeren om tegemoet te komen aan de gestelde integriteitseisen aan logfaciliteiten en loginformatie.

Norm: Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.

Het concept Justid Logbeleid uit 2015 beschrijft dat een minimale bewaartermijn van drie maanden wenselijk is vanwege de noodzakelijke loganalyse op de loginformatie. Logging omtrent (vermoedelijke) informatiebeveiligingsincidenten moet minimaal drie jaar worden bewaard.
In het concept Justid Logbeleid uit 2018 is opgenomen dat de bewaartermijn voor logging en de logcyclus afhankelijk is van het organisatiebelang.
In het vastgestelde Justid Logbeleid uit 2019 is opgenomen dat het belang van de log wordt afgezet tegen de frequentie van de logroulatie (dagelijks/wekelijks of maandelijks) en de bewaarlocatie. Geen van de beleidsdocumenten beschrijven maatregelen om de beschikbaarheid van loginformatie te waarborgen.

IBO heeft geen expliciete risicoafweging voor de jaren 2018, 2019 en 2020 aangereikt waarin de bewaarperiode van de logging is bepaald. Wel zijn er bewaartermijnen opgesteld gebaseerd op wet- en regelgeving.

Wij hebben per inspectie van de serverlogging vastgesteld dat in 2018 en 2019 loginformatie tot en met het jaar 2014 beschikbaar was. Per observatie van de loginstellingen hebben wij vastgesteld dat de logging in de centrale voorziening in 2019 en 2020 een bewaartermijn had van 365

dagen. Tot 10 december 2020 was de logging inzake de bevragingen tot het jaar 2014 beschikbaar. Per 10 december 2020 heeft IBO deze bewaartermijn aangepast en beperkt tot drie jaar.

Norm: De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

In zowel het concept Justid Logbeleid 2018 als in het vastgestelde IBO Logbeleid uit 2019 is opgenomen dat de interne klokken van informatiesystemen moeten worden gesynchroniseerd met een overeengekomen tijdsbron.

Wij hebben vastgesteld dat in 2020 de objecten in onderzoek de tijd synchroniseren met een referentietijdbron op het internet. Voor 2018 en 2019 kon dit wegens het ontbreken van historische gegevens niet worden vastgesteld.

3.6 Patchmanagement (en kwetsbaarhedenmanagement)

Norm: Zodra kwetsbaarheden bekend zijn dienen de te beoordelen IT-systemen tijdig te worden gepatcht en ge-update. De tijdigheid wordt bepaald aan de hand van de urgentie van de kwetsbaarheid. Het patchen vindt plaats volgens de reguliere procedure of via een goedgekeurde noodprocedure.

Norm: Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC-classificatie), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.

IBO hanteert het patchbeleid van Justid uit 2018. Daarnaast heeft IBO een eigen patchprocedure en is er een noodprocedure voor kritieke patches. De procedure schrijft voor dat reguliere patches uiterlijk een half jaar na het uitbrengen van een patch moeten zijn doorgevoerd. Voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is geldt dat patches zo spoedig mogelijk worden doorgevoerd, doch uiterlijk binnen één week.

Wij hebben vastgesteld dat de ons onderzochte servers in 2018, 2019 en 2020 op peildatum binnen de afgesproken periode van één maand zijn bijgewerkt met de benodigde updates. Patches worden niet als wijziging geregistreerd.

Bij één door het Nationaal Cyber Security Center (NCSC) in 2020 uitgebrachte kritieke update hebben wij vastgesteld dat deze binnen de gestelde periode is geïnstalleerd. Over 2018 en 2019 hebben wij dit niet kunnen vaststellen aangezien er bij het IBO in die periode geen kritieke patches zijn gemeld.

4 Verantwoording onderzoek

4.1 Werkzaamheden, periode van uitvoering en afbakening

Voor dit onderzoek is in de periode oktober 2020 tot en met februari 2021 dossieronderzoek uitgevoerd, zijn interviews gehouden en zijn waarnemingen ter plaatse uitgevoerd. Daarmee hebben wij de overeengekomen werkzaamheden conform opdrachtbevestiging uitgevoerd.
Op verzoek van de opdrachtgever wordt in deze rapportage niet piramidaal gerapporteerd.

De ADR heeft onderzoek gedaan naar opzet en bestaan van de maatregelen voor de in paragraaf 3.2 genoemde thema's.
Hierbij zijn de volgende peildatums gehanteerd:

Jaar	Peildatum
2018	1 december 2018
2019	1 december 2019
2020	1 oktober 2020

Onder opzet verstaan wij dat organisatorische processen en procedures actueel en gedocumenteerd zijn. Onder bestaan verstaan wij dat de processen en procedures daadwerkelijk zijn ingericht conform de opzet (het bestaan is op één moment vastgesteld).

Het normenkader wat voor dit onderzoek is gebruikt is gebaseerd op het:

- Besluit verstrekking gegevens telecommunicatie (inwerking vanaf 18-7-2019).
- Standaard Diensten Niveau Overeenkomst (DNO) tussen het ministerie van JenV en aanbieders en afnemers van het CIS.
- Voorschrift Informatiebeveiliging Rijksdienst voor Bijzondere Informatie (VIRBI-2013).
- Baseline Informatiebeveiliging Overheid (BIO v1.04).

En maakt een onderverdeling naar de volgende thema's:

- Algemeen zoals VGB/VOG en certificaten beheer.
- Invoer en verwerking.
- Logische toegangsbeveiliging (incl. wachtwoordenbeheer).
- Vernietiging van gegevens.
- Logging en monitoring.
- Patchmanagement.

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

De concept bevindingen uit ons onderzoek zijn in het kader van hoor en wederhoor op 13 januari 2021 met IBO besproken. Eventuele feitelijke onjuistheden zijn (door IBO gemotiveerd) aangepast in de bevindingenmatrix. De definitieve bevindingenmatrix is op 29 januari 2021 afgestemd met IBO.

De inhoudelijke afstemming van dit rapport heeft op 6 april 2021 plaatsgevonden met de opdrachtgever.

Gezien het rubriceringsniveau van de CIS-informatie wordt een deel van het auditdossier (inclusief de onderbouwing van de bevindingen) op locatie onder verantwoordelijkheid van IBO bewaard. De geldende wet- en regelgeving en bewaringstermijn van ten minste zeven jaar is hierop van toepassing. Niet vertrouwelijke informatie zoals de opdrachtbevestiging en de eindversie van de rapportage worden in het auditmanagementsysteem van de ADR opgeslagen.

Het auditdossier is alleen op basis van 'need-to-know' toegankelijk. Alleen met uitdrukkelijke toestemming van de ADR is deze informatie voor afdoende gescreende medewerkers raadpleegbaar, waaronder de kwaliteitstoetsers van de ADR. Van de overdracht van het dossier is een protocol van overdracht opgemaakt, door beide partijen ondertekend en opgenomen in het auditdossier.

4.2 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).

Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden wij wellicht andere zaken hebben geconstateerd en gerapporteerd. Het rapport bevat de feitelijke bevindingen van het uitgevoerde onderzoek en geeft handelingsperspectief aan de opdrachtgever.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.
De interne Opdrachtgerichte Kwaliteitsbeoordeling (OKB) is uitgevoerd door een onafhankelijke kwaliteitsbeoordelaar van de ADR, welke niet betrokken is geweest bij de uitvoering van het onderzoek.

Het voor dit onderzoek aangelegde dossier is conform deze richtlijnen ingericht en blijft eigendom van de ADR.

4.3 Verspreiding rapport

De opdrachtgever, [redacted] (DGRR) van het ministerie van Justitie en Veiligheid, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (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 www.rijksoverheid.nl.

5 Ondertekening

Den Haag, 29 juni 2021

[redacted]

Projectleider

Auditdienst Rijk

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