Auditdienst Rijk
Ministerie van Financiën

departementaal VERTROUWELIJK

Onderzoeksrapport
Normstelling Inrichting Interceptieketen 2017

Definitief

Colofon

Titel	Normstelling Inrichting Interceptieketen 2017
Uitgebracht aan	Directeur-Generaal Politie en Veiligheidsregio's
Datum	12 december 2019
Kenmerk	2019-0000213568
Status	V1.0

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Centrale boodschap

In 2017 heeft actualisatie plaatsgevonden van de Normstelling Inrichting Interceptiefaciliteit (hierna normstelling) die betrekking heeft op de interceptieketen die ten dienste staat van alle opsporingsdiensten. In deze normstelling zijn normen opgenomen die de authenticiteit en de integriteit van de geïntercepteerde data waarborgen.

Tussen de minister van JenV, de politie, het OM en de Nederlandse Orde van Advocaten (NOvA) is in 2011 een Convenant Nummerherkenning (hierna convenant) afgesloten inzake de communicatie met geheimhouders en verschoningsgerechtigden. Dit convenant bevat afspraken over de omgang met geheimhouderscommunicatie en is in 2018 tot nader order verlengd.

De ADR constateert dat de implementatie van zowel de normstelling als van het convenant aandacht behoeft. Documentatie over de sturing op de informatiebeveiliging en verantwoordelijkheden gericht op de naleving van de normstelling interceptie 2017 is niet beschikbaar of alleen in concept aanwezig. Er moeten additionele maatregelen worden getroffen om beheerprocessen in lijn te brengen met de normstelling en de normen van het convenant moeten nog verder worden vertaald in maatregelen.

Wij adviseren daarom een project te starten dat invulling geeft aan de openstaande vereisten uit het convenant en de normstelling en de voortgang van dit project te monitoren. Daarnaast adviseren wij de politie om de normstelling kritisch te bezien en indien nodig aan te passen. Sluit daarbij voor zover mogelijk aan op gangbare standaarden zoals ISO of BIR.

1 Aanleiding opdracht

1.1 Aanleiding

De minister van Justitie en Veiligheid (JenV) heeft in een brief aan de Tweede Kamer (30517-31, d.d. 19 december 2017) toegezegd om in 2018 een audit te laten uitvoeren door de Auditdienst Rijk (ADR) naar de interceptieketen van de politie op basis van de in 2017 aangepaste en vastgestelde Normstelling Inrichting Interceptiefaciliteit (hierna normstelling). Op basis van deze toezegging heeft de ADR in opdracht van de Directeur-Generaal Politie en Veiligheidsregio's (DGPenV) in 2018 een onderzoek uitgevoerd naar de inrichting van de interceptieketen. Naast de nieuwe normstelling was het Convenant Nummerherkenning van 15 maart 2011 (hierna convenant) van toepassing op deze opdracht.

Afspraken en details over de aanpak, scope en diepgang van het onderzoek, alsook het toegepaste normenkader zijn opgenomen in de overeengekomen opdracht van 27 juli 2018 met kenmerk 2018-0000131678. Enkele herzieningen die later met u als opdrachtgever overeen zijn gekomen zijn beschreven in paragraaf 3.2.

1.2 Scope en Normering

De scope van de audit heeft zich gericht op twee specifieke onderdelen van de interceptieketen, namelijk de dataopslag van onbewerkte (ruwe) gegevens (hierna de coldstore) en het geheimhoudersfilter. De eisen uit de normstelling en het convenant zijn vertaald naar een door de opdrachtgever goedgekeurd normenkader[1] welke gehanteerd is voor dit onderzoek en kent de volgende verdeling:

1. Sturing op de informatiebeveiliging en verantwoordelijkheden;
2. Beheerprocessen:
    - Incidentmanagement;
    - Changemanagement;
    - Patchmanagement;
    - Autorisatiebeheer;
    - Logging en monitoring;
3. Normen Convenant Nummerherkenning.

De normen met betrekking tot de sturing op de informatiebeveiliging en verantwoordelijkheden en de beheerprocessen (onderdelen één en twee) hebben betrekking op de coldstore en het geheimhoudingsfilter. De normen met betrekking tot het convenant nummerherkenning (derde onderdeel) heeft uitsluitend betrekking op het geheimhoudersfilter. In paragraaf 3.2 wordt nader ingegaan op de uitgevoerde werkzaamheden in relatie tot de objecten van onderzoek.

1.3 Onderzoeksvraag

In deze rapportage wordt de volgende onderzoeksvraag beantwoord:

> *Welke informatiebeveiligingsmaatregelen heeft de politie in opzet en bestaan getroffen ten aanzien van de Normstelling Inrichting Interceptieketen 2017 en het Convenant Nummerherkenning 2011?*

Deze rapportage vermeldt in hoofdstuk 2 alleen de geconstateerde afwijkingen op hoofdlijnen en bevat niet de met de politie afgestemde volledige onderzoeksresultaten zoals deze zijn opgenomen in het onderliggende auditdossier.

---

[1] De toezegging van de minister een de Tweede Kamer om het resultaat van de door de politie uitgevoerde risicoanalyse in het onderzoek te betrekken, is hierin meegenomen (30517-29, d.d. 12 februari 2016). Mede op basis van deze risicoanalyse hebben de opdrachtgever en de politie een selectie van normen gemaakt die in het door ons gehanteerde normenkader is opgenomen.

1.4 Context

De politie – met tien regionale eenheden, de Landelijke Eenheid (LE) en het Politiedienstencentrum (PDC) staat onder leiding van de korpschef. De CIO politie is lid van de korpsleiding en wordt ondersteund door de Directie Informatievoorziening (Directie IV). De Directie IV is onder andere verantwoordelijk voor de ontwikkeling van ICT-strategie en het IV-beleid van de politie en de ontwikkeling en monitoring op kwaliteit en toezicht op de informatievoorziening.

De bedrijfsvoering van de politie – waaronder financiën, facilitaire zaken, informatiemanagement, ICT, communicatie en personeelszaken – is landelijk georganiseerd in het Politiedienstencentrum (PDC). De dienst ICT (DICT) en de dienst informatiemanagement (DIM) zijn onderdeel van het PDC. De DICT is verantwoordelijk voor de ontwikkeling en het beheer van ICT-middelen. De DIM is verantwoordelijk voor de vertaling van de eisen en wensen vanuit het primaire proces naar de IV-organisatie.

In 2016 heeft de korpsleiding besloten om het technische- en functionele beheer van het interceptiesysteem van de afdeling I&S over te brengen naar de DICT. De overdracht is ondergebracht in een transitietraject.
Dit transitietraject geeft invulling aan de centralisatie en het onderbrengen van het functionele beheer en het technisch beheer bij het Speciaal Beheer Team (SBT) van de DICT te Driebergen. Tijdens het onderzoek waren de betrokken organisatieonderdelen bezig met het verder vorm en inhoud geven aan de nieuwe rollen/organisatie.

In 2017 is de normstelling op initiatief van het Bureau Platform Interceptie Decryptie & Signaalanalyse (PIDS) met alle betrokken partijen (OM, PIDS, politie) geactualiseerd. De normstelling heeft betrekking op de interceptieketen die ten dienste staat van alle opsporingsdiensten. In de normstelling zijn procedurele- en technische normen (op het gebied van techniek, personeel en organisatie) opgenomen zodat de authenticiteit en de integriteit van de geïntercepteerde data kan worden gewaarborgd.

Tussen de minister van JenV, de politie, het OM en de Nederlandse Orde van Advocaten (NOvA) is in 2011 een convenant afgesloten inzake de communicatie met geheimhouders en verschoningsgerechtigden. Dit convenant bevat afspraken over de omgang met geheimhouderscommunicatie en is in 2018 tot nader order verlengd.

In hoofdstuk 2 worden de bevindingen over de getroffen maatregelen ten opzichte van de normen op hoofdlijnen beschreven. In hoofdstuk 2.1 wordt ingegaan op de sturing op de informatiebeveiliging en verantwoordelijkheden, in hoofdstuk 2.2 op de beheerprocessen en in hoofdstuk 2.3 op de bevindingen betreffende het convenant nummerherkenning. De aanbevelingen naar aanleiding van onze bevindingen zijn opgenomen in 2.4. Hoofdstuk 3 bevat ten slotte de verantwoording van onze werkzaamheden.

2 Implementatie normstelling en convenant vraagt aandacht

In dit hoofdstuk worden de bevindingen weergegeven gerelateerd aan de onderzoeksobjecten zoals aangegeven in hoofdstuk 1.

2.1 Documentatie over de sturing op de informatiebeveiliging en verantwoordelijkheden gericht op de naleving van de normstelling interceptie 2017 niet beschikbaar of nog in concept

Sturing op de informatiebeveiliging

De normen aangaande de sturing op de informatiebeveiliging zijn naar verschillende thema's onder te verdelen. Dit zijn de thema's kwaliteitszorgsysteem, informatiebeveiligingsbeleid, kwaliteitscontroles en pakket van informatiebeveiligingsmaatregelen, onderkende ketens, verbeterplannen, rapportages, risicomanagement, procedure rond of inkoop van informatiesystemen en naleving van de normstelling. Wij hebben opmerkingen bij de wijze waarop de politie maatregelen heeft getroffen om in opzet te voldoen aan de normen bij de thema's. Dit geldt bij alle thema's. Wij hebben bijvoorbeeld vastgesteld dat documenten die invulling kunnen geven aan deze eisen niet beschikbaar zijn, nog in concept zijn of geen volledige invulling geven aan de eisen van de normering.

Uit ons onderzoek is onder meer gebleken dat er een kwaliteitszorgsysteem (PDCA-cyclus) op concernniveau in het informatiebeveiligingskader is opgenomen, maar dat deze niet specifiek is uitgewerkt voor de interceptieketen. Het document beschrijft de kaders voor de informatiebeveiliging welke ingevuld dienen te worden door de politiechef door op basis van een risicoanalyse maatregelen te (laten) treffen die passend zijn voor de situatie. De invulling in maatregelen is vrij en kan naar de eigen situatie aangepast worden zolang dit resulteert in het beheersen van de risico's. Daarmee is het functionele kader bindend, maar wordt de naleving van de maatregelen overgelaten aan de individuele politiechef.

Er is niet beschreven dat de betrouwbaarheid van informatievoorziening van de interceptieketen wordt getoetst en dat hierover aan het management wordt gerapporteerd. De implementatie van de informatiebeveiliging is beschreven in architectuurdocumentatie.

Een beschrijving van het risicomanagementproces ontbreekt waarmee wordt gewaarborgd dat de organisatie bekend is met de risico's die men loopt doordat maatregelen eventueel (nog) niet operationeel zijn.

Verantwoordelijkheden

De normen aangaande de verantwoordelijkheden zijn naar verschillende thema's onder te verdelen. Dit zijn het benoemen en toewijzen van verantwoordelijken (inclusief functiescheiding), vastleggen van specifieke verantwoordelijkheden van de lijnmanager, beheer- en overige betrokken medewerkers, dienstverband bij de organisatie en vervangingsregeling. Wij hebben opmerkingen bij de wijze waarop de politie maatregelen heeft getroffen om in opzet te voldoen aan de normen bij de thema's. Dit geldt bij alle thema's. Wij hebben bijvoorbeeld vastgesteld dat documenten die invulling kunnen geven aan deze eisen veelal niet beschikbaar zijn, nog geen volledige invulling even aan de eisen van de normering of een onbekende status hebben.

Uit ons onderzoek is onder meer gebleken dat er geen interceptieketen brede beschrijving van de verantwoordelijkheden (functiescheiding) voor de interceptieketen is en dat een beschrijving ontbreekt dat ingaat op de eisen vanuit de normering ten aanzien van de verantwoordelijkheden van het management. Er is (in opzet) geregeld dat actuele functie eisen worden gesteld ten aanzien van opleiding, kennis en ervaring in lijn met de taken, verantwoordelijkheden en bevoegdheden.

2.2 Additionele maatregelen moeten getroffen worden om beheerprocessen in lijn te brengen met de normstelling

Incidentmanagement

Zowel I&S als DICT hanteren beide een eigen incidentmanagementproces. Het proces van I&S heeft betrekking op het operationele deel van het interceptieproces waar I&S de uitvoering voor doet, het proces van DICT heeft betrekking op het technische (ICT) deel van het interceptieproces in beheer bij de DICT.

De normen aangaande het incidentmanagement zijn naar verschillende thema's onder te verdelen. Deze thema's gaan in op hetgeen in het incidentproces moet zijn beschreven, bewustwordingsactiviteiten, rapportages over incidenten, schriftelijke registratie en analyse van incidenten en de centrale melding daarvan. Wij hebben opmerkingen bij de wijze waarop de politie maatregelen heeft getroffen om in opzet en bestaan te voldoen aan de normen bij de thema's. Dit geldt bij alle thema's. Uit ons onderzoek is onder meer gebleken dat bewustwording, incidentenrapportages en potentiele risico's niet in de incidentenprocedures zijn beschreven.

In het concept incidentmanagementproces van de DICT is opgenomen dat de periodieke registratie van incidenten worden geanalyseerd of geëvalueerd. In de incidentmanagementprocedure van I&S is de analyse en evaluatie niet beschreven. Voor beide processen vindt ook in de praktijk de analyse en evaluatie van incidenten niet plaats. De registratie van incidenten bevat niet alle kenmerken die wel vanuit de norm worden vereist. De procesbeschrijving Incidentmanagement van I&S dateert uit 2015 en is sindsdien niet meer geactualiseerd.

Changemanagement

De politie hanteert voor het changemanagementproces in de interceptieketen twee procesbeschrijvingen: één beschrijving heeft betrekking op de technische wijzigingen bij de DICT en de tweede beschrijving heeft betrekking op het wijzigingsbeheer bij I&S[2].

De normen aangaande het changemanagement zijn naar verschillende thema's onder te verdelen. Deze gaan in op het hebben van een wijzigingsproces, eisen ten aanzien van een wijziging zoals betrokkenheid van de systeemeigenaar bij goedkeuring, functiescheidingen binnen het proces, testproces en testomgeving, back-out procedure en beheerkalender. Wij hebben opmerkingen bij de wijze waarop de politie maatregelen heeft getroffen om in opzet te voldoen aan de normen bij de thema's. Dit geldt bij alle thema's.

Uit ons onderzoek is onder meer gebleken dat functiescheiding tussen het aanvragen, goedkeuren en doorvoeren van wijzigingen niet in de wijzigingsprocedures zijn beschreven. In de wijzigingsprocedures is ook niet beschreven dat 10.2.c [redacted] 10.2.c [redacted] 10.2.c [redacted]. De politie geeft aan dat 10.2.c [redacted] 10.2.c [redacted]. Niet duidelijk is wie formeel de systeemeigenaar is van de

[2] Voor de normstelling gelden de wijzigingsprocedures van de DICT en van I&S in tegenstellig tot het convenant waarvoor alleen die van de DICT geldt.

interceptieketen. De formele status van de wijzigingsprocedure van de DICT is onbekend. Alhoewel niet beschreven in de wijzigingsprocedures hanteert de politie in de praktijk wel een kalender (planning) van beheeractiviteiten.

Patchmanagement

De normen aangaande het patchmanagement zijn naar verschillende thema's onder te verdelen. Deze gaan in op hetgeen in het patchmanagementproces moet zijn beschreven (zoals periodieke penetratietests en risicoanalyse van kwetsbaarheden en patching) en over het inplannen van beveiligingsupdates als onderdeel van changemanagement. Wij hebben opmerkingen bij de wijze waarop de politie maatregelen heeft getroffen om in opzet en bestaan te voldoen aan de normen bij de thema's. Dit geldt bij alle thema's.

Uit ons onderzoek is onder meer gebleken dat er voor de objecten van onderzoek sprake is van verouderde software en ontbreekt een patchprocesbeschrijving voor de interceptieketen dat onder meer ingaat op het periodiek uitvoeren van penetratietesten. Resultaten van penetratietesten zijn niet aangetroffen. Beheerders maken wegens het ontbreken van een patchbeleid zelf een inschatting van de kans en impact van een kwetsbaarheid. Men laat zich daarbij leiden door de NCSC-classificatie van uitgebrachte alerts.

In de uitvoeringsregeling wordt Operationeel Beheer verantwoordelijk gehouden voor het patchmanagementproces terwijl dit een verantwoordelijkheid moet zijn voor de DICT.

Autorisatiebeheer

De normen aangaande het autorisatiebeheer zijn naar verschillende thema's onder te verdelen. Deze gaan in op het specifiek inrichten van een identificatie- en authenticatieproces voor de interceptieketen, dat toegang herleidbaar moet zijn naar een uniek persoon, organisatie of geautomatiseerd systeem, (technische) eisen die worden gesteld aan de toegang (zoals two-factor authenticatie, principes 'need-to-know' en 'least privilege' en functiescheidingen), ontoegankelijkheid van de toegang tot de data met geheimhouders en bewaartermijnen conform wet- en regelgeving. Wij hebben opmerkingen bij de wijze waarop de politie maatregelen heeft getroffen om in opzet en bestaan te voldoen aan de normen bij de thema's. Dit geldt bij alle thema's.

Uit ons onderzoek is onder meer gebleken dat een identificatie- en authenticatieprocesbeschrijving in opzet niet specifiek is uitgewerkt voor de interceptieketen. Hierbij kan bijvoorbeeld worden gedacht aan een autorisatiematrix en een beschrijving van de gewenste functiescheidingen. De politie steunt op het generieke identificatieproces van de afdeling HRM van het PDC.

Wegens het ontbreken van een autorisatiematrix en een beschrijving van de gewenste functiescheiding zijn de beheerautorisaties hebben we niet onderzocht of deze conform toegangsbeleid zijn ingericht. Wel hebben we vastgesteld dat beheerders gebruik maken van een naar een persoon te herleiden account[3]. Verder hebben wij voor de coldstore vastgesteld dat beheerders geauthentiseerd worden op basis van een gebruikersnaam en wachtwoord.

Monitoring en Logging

De normen aangaande de monitoring en logging zijn naar verschillende thema's onder te verdelen. Deze gaan in op de eis dat alle systemen van de interceptiefaciliteit voorzien moeten zijn van een logfunctie, de eisen aan de toegang tot de logbestanden, de eisen aan de logregistratie met bewaar- en

[3] Het *uniek* herleidbaar zijn naar een persoon is niet onderzocht.

vernietigingstermijnen, een tijdbron van voldoende kwaliteit, een (centrale) voorziening voor de opslag en analyse van logging, de lograpportages en de eisen aan de monitoring van de logging. Bij de thema's 'dat alle systemen van de interceptiefaciliteit voorzien moeten zijn van een logfunctie' en 'de beschikking over een tijdbron van voldoende kwaliteit' hebben we geen opmerkingen.
Bij de andere thema's hebben wij opmerkingen op de wijze waarop de politie maatregelen heeft getroffen om in opzet en bestaan te voldoen aan de normen.

Uit ons onderzoek is onder meer gebleken dat de documentatie over de monitoring en logging niet volledig de eisen uit de normering afdekken. Zo is gebleken dat, alhoewel systemen van de interceptieketen zijn voorzien van een logfunctie, er geen drempelwaarden zijn beschreven voor het alarmeren van de beheerorganisatie wanneer beleidsregels en prestatieniveaus zijn of dreigen te worden overschreden. Dat logging tot leesrechten moet zijn beperkt is niet beschreven maar is in de praktijk wel zo ingericht. 10.2.c [redacted]

Hierbij merken we op dat vanwege het ontbreken van een autorisatiematrix de uitgegeven beheerautorisaties ten aanzien van de verstrekte toegang tot logbestanden niet door ons zijn onderzocht.

2.3 Normen Convenant Nummerherkenning nog verder vertalen in maatregelen

In het convenant Nummerherkenning zijn specifieke eisen opgenomen met betrekking tot geheimhouderscommunicatie. Deze eisen hebben betrekking op de thema's het melden van de verwerking van persoonsgegevens bij de Autoriteit Persoonsgegevens (AP), incidentmanagement, wissen van geheimhouderscommunicatie, changemanagement, systeemdocumentatie, procedures voor het beheer en het gebruik van het systeem versleuteling van de informatie voor het systeem van nummerherkenning voor transport en opslag, logische toegangsbeveiliging en procedures voor de beoordeling van logging.

Bij het thema 'het melden van de verwerking van persoonsgegevens bij de Autoriteit Persoonsgegevens (AP)' hebben we geen opmerkingen. Bij de overige thema's hebben wij opmerkingen op de wijze waarop de politie maatregelen heeft getroffen om in opzet en bestaan te voldoen aan de normen.

<u>Incidentmanagementproces</u>
Zowel I&S als DICT hanteren beide een eigen incidentmanagementproces. Het proces van I&S heeft betrekking op het operationele deel van het interceptieproces waar I&S de uitvoering voor doet, het proces van DICT heeft betrekking op het technische (ICT) deel van het interceptieproces in beheer bij de DICT.

Het convenant stelt diverse eisen zoals een incidentenmanagementproces waarin een adequate reactie is georganiseerd bij verstoringen inclusief het identificeren en vernietigen van geheimhouderscommunicatie. Deze eisen wijken op onderdelen af van de eisen uit de normstelling 2017.

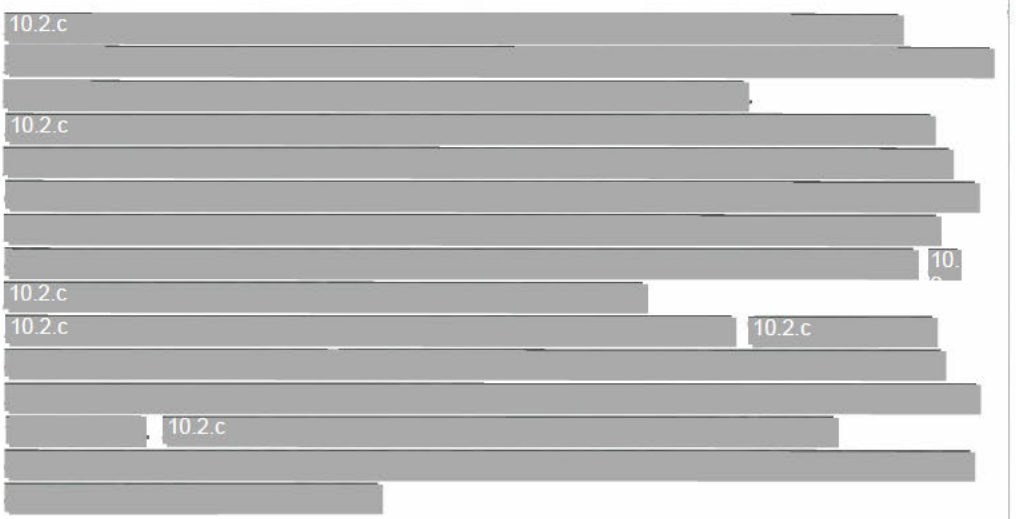
Uit ons onderzoek is onder meer gebleken dat niet alle in de normen gestelde vereisten zijn ook daadwerkelijk in beide incidentenprocedures zijn beschreven, zoals: bewustwording, incidentenrapportages en potentiele risico's.

In de incidentmanagementprocedure van I&S is de analyse en evaluatie van incidenten niet beschreven. Dit document is overigens sinds de transitie in 2016 niet meer geëvalueerd en aangepast. Hoewel in het concept incidentmanagementproces van DICT wel is opgenomen dat periodiek de registratie van incidenten moet worden

geanalyseerd of geëvalueerd vindt dit in de praktijk bij zowel de DICT als I&S niet plaats.

Gedurende de onderzoeksperiode hebben zich geen incidenten ten aanzien van ons object van onderzoek voorgedaan. Incidenten met betrekking tot het object van onderzoek hebben we dus niet kunnen onderzoeken.

Naschrift ten aanzien van het incident uit 2018 wat zich na de onderzoeksperiode heeft voorgedaan:



Wissen van geheimhouderscommunicatie

Het convenant stelt onder meer eisen aan wie geheimhouderscommunicatie mag wissen, op welke wijze dit moet plaatsvinden en de archivering. Uit ons onderzoek is onder meer gebleken dat het programma voor de overschrijving van geheimhoudercommunicatie sinds 2013 niet gewijzigd is.

We hebben kunnen vaststellen dat operationeel beheerders geautoriseerd zijn om geheimhouderscommunicatie te wissen. We hebben niet onderzocht of het wissen van geheimhouderscommunicatie door anderen dan operationeel beheerders kan plaatsvinden.

Changemanagement

Het convenant stelt onder meer eisen aan hetgeen in het changemanagementproces moet zijn opgenomen over de afstemming van wijzigingen met de NOvA en versiebeheer.

De politie hanteert voor het systeem van nummerherkenning het changemanagementproces van de DICT. Dit changemanagementproces heeft betrekking op de technische wijzigingen bij de DICT. Uit ons onderzoek is onder meer gebleken dat de rol van I&S richting de NOvA niet is beschreven en dat er geen melding wordt gemaakt van het feit dat wijzigingen aan de NOvA moeten worden gemeld in de concept changemanagementprocesbeschrijving van de DICT. Niet is beschreven hoe wordt gewaarborgd dat alleen de laatste goedgekeurde systeemversie in productie draait (versiebeheer).

Wijzigingsverzoeken (RFC's) m.b.t. de objecten van onderzoek zijn niet aangetroffen en derhalve hebben we het naleven van deze norm in de praktijk niet kunnen vaststellen.

Systeemdocumentatie en procedures

Het convenant stelt eisen aan systeemdocumentatie, zoals functionele en technische

documentatie en beheerprocedures. Uit ons onderzoek is onder meer gebleken dat deze documentatie op onderdelen ontbreekt dan wel niet formeel is vastgesteld. Zo is in 2012 het systeem van nummerherkenning functioneel- en technisch gedocumenteerd maar zijn deze documenten niet formeel vastgesteld. Dit geldt ook voor procedures voor (handmatige) handelingen ten behoeve van het beheer en het gebruik van het systeem inclusief het bestand van geheimhoudernummers. Ten aanzien van de technische documentatie heeft de politie aangegeven dat deze documentatie nog actueel is.

Technische- en organisatorische maatregelen ter beveiliging van het systeem zijn niet specifiek gemaakt voor het geheimhouderfilter dan wel het systeem voor nummerherkenning.

Logische toegangsbeveiliging
Het convenant stelt eisen aan de logische toegangsbeveiliging van het bestand.

Uit ons onderzoek is onder meer gebleken dat inrichtingsprincipes op hoofdlijnen zijn beschreven. Een nadere (technische) vertaling is echter niet aanwezig. We hebben in kaart gebracht welke accounts toegang hebben tot het systeem maar we hebben niet kunnen vaststellen of dit op basis van de principes 'need to know' of 'least privilege' is gebeurd door het ontbreken van bijvoorbeeld een logisch toegangsbeleid en/of een autorisatiematrix. Wij hebben vastgesteld dat één functioneel account en de domain administratoren toegangsrechten hebben op de map waarin het bestand wordt geplaatst. Logging van toegang vindt plaats maar wordt niet periodiek geanalyseerd.

Beveiligde verbinding
10.2.c [redacted]

10.2.c [redacted]

- 10.2.c [redacted]
- 10.2.c [redacted]
- 10.2.c [redacted]

Logging
Het convenant stelt eisen aan het logbestand en de analyse hiervan.

Uit ons onderzoek is onder meer gebleken dat, alhoewel er events worden gelogd, op basis van deze events 10.2.c [redacted]
10.2.c [redacted]

2.4 Aanbevelingen

Gegeven de hiervoor beschreven bevindingen adviseren wij om:

- *De politie een traject te laten starten om invulling te geven aan de vereisten uit het convenant en de normstelling, dit door verder maatregelen*

te ontwerpen en te realiseren. Houd daarbij rekening met het belang van de normen, dat wil zeggen de risico's die worden gelopen door het niet voldoen aan de norm, en de middelen (tijd, geld) dat het kost om deze maatregelen te treffen. Een deel van de afwijkingen kunnen onzes inziens relatief eenvoudig worden opgelost door bijvoorbeeld procedures en documenten aan te vullen en te formaliseren, andere afwijkingen vergen een grotere inspanning.

- *De DGPenV de voortgang van het traject te monitoren bijvoorbeeld op basis van periodieke rapportages en, indien nodig, tijdig bij te sturen.*
- *De politie om de normstelling kritisch te bezien en indien nodig aan te passen. Tijdens ons onderzoek bleken een aantal normen multi-interpretabel en/of niet realiseerbaar. Sluit, voor zover mogelijk, aan op gangbare standaarden zoals ISO of BIR. Doe dit op korte termijn, zodat eventuele wijzigingen kunnen worden meegenomen in het traject om de afwijkingen op te lossen.*
- *De politie om het convenant evenzo te evalueren op het multi-interpretabel en/of niet realiseerbaar zijn van normen, en de resultaten van deze evaluatie te bespreken met de NOvA.*
- *De politie om door interne controle of interne audit vast te stellen dat de maatregelen zijn gerealiseerd.*

3 Verantwoording onderzoek

3.1 Doelstelling

De doelstelling van het onderzoek is de opdrachtgever en de politie inzicht te geven in de informatiebeveiligingsmaatregelen die zijn getroffen op basis van de normstelling en de afspraken in het convenant, zodat de politie waar nodig aanvullende maatregelen kan treffen. Over de afwijkingen wordt in deze rapportage feitelijk en op hoofdlijnen gerapporteerd. Om de doelstelling te realiseren is onderzoek uitgevoerd bij de betrokken afdelingen van de politie, te weten de Dienst Informatiemanagement (DIM), de DICT en de afdeling I&S.

Op verzoek van de opdrachtgever is deze rapportage voorzien van aanbevelingen om handelingsperspectief te bieden.

3.2 Werkzaamheden en periode van uitvoering

Voor dit onderzoek zijn gedurende de periode maart 2018 t/m mei 2019 documenten geanalyseerd, zijn interviews gehouden en zijn waarnemingen ter plaatse uitgevoerd.

De ADR heeft de opzet en het bestaan van de maatregelen onderzocht voor de onderzoeksperiode van 1 april t/m 5 juni 2018. Dit geldt niet voor de maatregelen met betrekking tot het eerste thema 'de sturing op de informatiebeveiliging' en de maatregelen met betrekking tot het tweede thema 'verantwoordelijkheden' die alleen in opzet zijn onderzocht. Dit is een afwijking ten opzichte van de opdrachtbevestiging en is met de opdrachtgever afgestemd.

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). Peildatum voor vaststelling van de opzet en het bestaan is 5 juni 2018.

Hieronder volgt in tabelvorm de uitgevoerde werkzaamheden in relatie tot de objecten van onderzoek.

Thema's bevindingenmatrix	**Audit diepgang en objecten van onderzoek**		
	Coldstore 10.2.c	**Geheimhouders filter**	**Niet onderzocht**
1.Sturing op de informatiebeveiliging	- Opzet	- Opzet	Een procedure die onder meer maatregelen borgt bij ontwikkelingen of inkoop van informatiesystemen.
2.Verantwoordelijkheden	- Opzet	- Opzet	Een (actuele) functieomschrijving met duidelijk beschreven taken voor (beheer) medewerkers. Een actuele vervangingsregeling die zodanig is dat de functiescheiding

			gehandhaafd blijft en wordt toegepast.
3.Incidentmanagement	- Opzet - Bestaan (deels: een aantal algemene maatregelen zoals preventiemaatregelen en rapportages.	- Opzet - Bestaan (deels: een aantal algemene maatregelen zoals preventiemaatregelen en rapportages).	De afhandeling van incidenten m.b.t.: - de coldstore - het geheimhoudersfilter
4.Changemanagement	- Opzet - Bestaan (voor wat betreft de aanwezigheid van een beheerkalender)	- Opzet - Bestaan (voor wat betreft de aanwezigheid van een beheerkalender)	De afhandeling van changes m.b.t.: - de coldstore - het geheimhoudersfilter
5.Patchmanagement	- Opzet - Bestaan	- Opzet - Bestaan	
6.Autorisatiebeheer	- Opzet - Bestaan	- Opzet - Bestaan	Een identificatieproces voor de interceptieketen. Toegang interceptieketen is uniek herleidbaar tot een persoon, organisatie of systeem. De verleende toegang aan gebruikers van de interceptieketen middels two-factor authenticatie. Het onderscheid in drie niveaus operationeel beheergroepen bij operationeel beheer en de toegang voor technisch beheer. De archivering op een permanent medium.
7.Logging en monitoring	- Opzet - Bestaan	- Opzet	
8.Convenant Nummerherkenning	Niet van toepassing	- Opzet - Bestaan	De archivering na verwijdering van de geheimhoudercommunicatie. De afhandeling van incidenten en wijzigingen m.b.t. het geheimhoudersfilter.

De ADR heeft voor dit onderzoek een normenkader ontwikkeld gebaseerd op de Normstelling Interceptieketen 2017 en de afspraken zoals die zijn opgenomen in het Convenant tussen het Ministerie van Justitie, de politie en de Nederlandse Orde van

Advocaten (NOvA). Het voor dit onderzoek gehanteerde normenkader is voorafgaand aan het onderzoek afgestemd met de opdrachtgever.

De concept bevindingen uit ons onderzoek zijn in het kader van hoor wederhoor op 29 april 2019, 13 mei 2019 en 23 mei 2019 besproken met de politie. Voor zover de opmerkingen van de politie betrekking hadden op feitelijke onjuistheden zijn deze aangepast in de bevindingenmatrix en vervolgens op 25 juni 2019 aan de politie aangeboden.

Conform de opdrachtbevestiging bevat dit rapport de feitelijke bevindingen op hoofdlijnen van het onderzoek. Voor een volledig en gedetailleerd overzicht van de bevindingen verwijzen we naar de bevindingenmatrix. Deze is in te zien op locatie bij de politie.

3.3 Gehanteerde Standaard en Kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (IIA).

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.

3.4 Verspreiding rapport

De opdrachtgever, dhr. mr. W.F. Saris MPA, Directeur-Generaal Politie en Veiligheidsregio's, 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

Dan Haag, 12 december 2019

10.2.e

10.2.e

IT-Auditor
Auditdienst Rijk

Bijlage 1 Managementreactie opdrachtgever

Onderwerp
Managementreactie politie
Onderzoeksrapport Normstelling
Inrichting Interceptieketen 2017

De Directeur van de Auditdienst Rijk

Organisatieonderdeel
LE en PDC dienst ICT

Behandeld door
10.2.e

Functie

Telefoon

E-mail

Ons kenmerk

Uw kenmerk

In afschrift aan

Datum
5 december 2019

Bijlage(n)
0

Pagina
1

Met veel belangstelling heb ik kennis genomen van het Onderzoeksrapport Normstelling Inrichting Interceptieketen 2017 van de Auditdienst Rijk (ADR). De politie herkent en onderschrijft zowel de bevindingen als de aanbevelingen en neemt deze over. Reeds ten tijde van het onderzoek is hiertoe een taskforce ingericht onder leiding van de dienst ICT.
Deze taskforce heeft zich primair gericht op de actualisatie van documentatie over de sturing op informatiebeveiliging en verantwoordelijkheden op de naleving van de Normstelling. Voorts is gestart met de analyse en evaluatie van incidenten en de implementatie van drempelwaarden gekoppeld aan logging. Het patchproces is beschreven, verouderde software geüpdate en de autorisatiematrix vastgesteld.
De voortgang van de taskforce wordt ook de komende periode nauwlettend gemonitord door de Stuurgroep Interceptie, waar ik voorzitter van ben.

De politie heeft die Stuurgroep, samengesteld uit vertegenwoordigers van zowel de operatie als de PDC diensten ICT en IM, ingesteld om te sturen op continuïteit, verbetering en vernieuwing van het (beheer van het) interceptiesysteem. Interceptie is een belangrijk opsporingsmiddel waarbij operatie en techniek nauw met elkaar verbonden zijn. Dat vergt eenzelfde verbinding in de aansturing van het onderwerp in de volle breedte.

De politie onderkent de constateringen van de ADR ten aanzien van de multi interpretabiliteit en niet realiseerbaarheid van een aantal normen uit de normstelling, ondanks dat deze in 2017 is geactualiseerd. Daarom is aan concernaudit de opdracht gegeven om de normstelling kritisch te bezien op interpretatie en realiseerbaarheid en hierover een (aanpassings)advies te geven.
Ook de vaststelling van de ADR dat het normenkader gebaseerd op het convenant evaluatie behoeft onderschrijft de politie. In overleg met de NOvA zal een traject worden gestart om te komen tot een eenduidig en realiseerbaar normenkader voor het systeem van nummerherkenning. Of en in hoeverre het Convenant dient te worden gewijzigd zal in dat traject worden meegenomen.
Onderdeel van dat traject is ook de afhandeling van 10.2.c
10.2.c
10.2.e

10.2.e W.H. Woelders
Plv. Politiechef Landelijke Eenheid
Voorzitter stuurgroep interceptie

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