Samen werken, samen beveiligen

INFORMATIEBEVEILIGING BIJ DE NEDERLANDSE POLITIE

Inspectie
OPENBARE ORDE
EN VEILIGHEID

Samen werken, samen beveiligen

INFORMATIEBEVEILIGING BIJ DE NEDERLANDSE POLITIE

Inspectie Openbare Orde en Veiligheid

Den Haag

maart 2007

INSPECTIE OPENBARE ORDE EN VEILIGHEID

Inspectie Openbare Orde en Veiligheid (Inspectie OOV)
Bezoekadres: Juliana van Stolberglaan 148, 2595 CL Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
Telefoon: (070) 426 62 61
Telefax: (070) 426 69 90
Website: www.ioov.nl

COLOFON

Uitgave: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Inspectie Openbare Orde en Veiligheid
Lay out: Grafisch Buro van Erkelens
Drukwerk: drukkerij Hega, Den Haag
ISBN: 978-90-5414-125-9

maart 2007

Inhoudsopgave

NB (Bijlagen II t/m VIII zijn terug te vinden op de bijgeleverde cd-rom)

Onze missie

De Inspectie OOV levert een bijdrage aan de veiligheid van de samenleving. Zij oefent daartoe toezicht uit op besturen en organisaties die verantwoordelijk zijn voor de openbare orde en veiligheid en stelt hen daarmee in staat de veiligheid te verbeteren.

De Inspectie OOV houdt, onder de verantwoordelijkheid van de ministers van BZK en van Justitie, toezicht op de kwaliteit van de taakuitvoering van zowel de verantwoordelijke bestuursorganen als de operationele diensten die op de verschillende onderdelen van het OOV-terrein actief zijn (politie, brandweer, GHOR).

De Inspectie OOV laat zich leiden door enerzijds de inschatting van maatschappelijke veiligheids-risico's en anderzijds door de vraag waar zij met haar toezicht maximaal kan bijdragen aan het realiseren van beoogde beleidseffecten. In haar werkplannen, jaarverslagen en rapportages worden de gemaakte keuzes en gevolgde werkwijzen verantwoord.

Het oordeel van de Inspectie OOV komt onafhankelijk tot stand.

De Inspectie OOV draagt haar bevindingen actief uit. Zij geeft daarmee de ministers en de onder toezicht staande organisaties inzicht in hun bijdragen aan de kwaliteit van het veiligheidsniveau en de praktische uitwerking van het gevoerde beleid. De Inspectie OOV beoogt daarmee bij betrokkenen een oriëntatie op permanente aandacht voor verbetering tot stand te brengen.

De Inspectie OOV zoekt actief samenwerking met andere partijen van beleid, uitvoering en toezicht, zowel op het OOV-domein als op aanverwante terreinen.

De Inspectie OOV weet wat er leeft en toetst of het werkt.

Betreffende dit rapport

Samen werken, samen beveiligen

Door het samen met haar partners uitvoeren van een inspectiebrede risico-analyse wordt jaarlijks bepaald welke thema's, passend binnen de hoofdlijnen van het Meerjarenbeleidsplan Progressie in toezicht, binnen het politiedomein in het bijzonder zullen worden onderzocht.

De richtinggevende thema's voor 2006-2008 zijn:
- maatschappelijke oriëntatie van de korpsen;
- professie van het vak;
- informatiehuishouding;
- bestuurlijke verantwoordelijkheden (met name ketensamenwerking).

Dit rapport 'Samen werken, samen beveiligen' maakt onderdeel uit van onderzoeken binnen het thema informatiehuishouding.

Eerder verscheen binnen dit thema:
- Landelijke coördinatie en uitwisseling van politie-informatie – Ontwikkelingen sinds rapportage 2004 (december 2006)
- Landelijke Informatiecoördinatie en uitwisseling van politie-informatie – Een evaluatie van het project Landelijke Informatiecoördinatie DNP (2004)

Binnenkort zullen verschijnen binnen dit thema:
- Informatie Gestuurde Politie (najaar 2007)

Samenvatting, conclusies en aanbevelingen

Zonder betrouwbare informatiesystemen en accurate gegevensvoorziening is politiewerk vandaag de dag niet denkbaar. Vanuit het vitale belang van goede informatie voor de politie is informatiebeveiliging daarom evenzeer belangrijk. Informatiebeveiliging is meer dan enkel het afschermen van vertrouwelijke gegevens. Doorgaans wordt bij informatiebeveiliging gedacht aan de BEI-eisen, waarbij de B staat voor beschikbaarheid (doen de informatiesystemen het als het erop aankomt?), de E voor exclusiviteit (is informatie voldoende afgeschermd?) en de I voor integriteit (kloppen de gegevens/cijfers?). In dit licht is informatiebeveiliging dan ook niet iets waar 'ook aandacht voor moet zijn', maar een essentiële voorwaarde voor een goed verloop van alle werkprocessen bij de politie. Het feit dat steeds meer informatie binnen de Nederlandse politie wordt uitgewisseld en gedeeld, leidt er bovendien toe dat informatiebeveiliging bij alle korpsen van gelijk niveau dient te zijn. Immers een korps moet er op kunnen vertrouwen dat zijn informatie bij de buren ook veilig is.

In deze samenvatting wordt eerst ingegaan op de implementatie van informatiebeveiliging bij de politiekorpsen en de actualiteit van het huidige Stelsel voor Informatiebeveiliging, gevolgd door conclusies en aanbevelingen. Daarna wordt het thema informatiebeveiliging bij interceptie belicht. Beide paragrafen bestaan uit een korte samenvatting met conclusies en aanbevelingen.

IMPLEMENTATIE VAN DE RIP EN HET STELSEL

In 1997 stelden de ministers van BZK en Justitie de Regeling Informatiebeveiliging Politie (RIP) vast. In de RIP werd de verantwoordelijkheid van de korpsbeheerders om een beveiligingsbeleid te formuleren en beveiligingsplannen op te stellen verwoord. De drie politieberaden (OM-Politieberaad, Korpsbeheerdersberaad en de Raad van Hoofdcommissarissen) onderschreven destijds de Regeling Informatiebeveiliging Politie en gaven opdracht voor de ontwikkeling van een Stelsel voor Informatiebeveiliging. Ook gaven ze aan dat een en ander door de korpsen in 2005 geïmplementeerd zou moeten zijn.

Aanvankelijk verliep de aanpak met het Stelsel voortvarend, vooral waar het ging om het formuleren van korpsbeleid, de opleiding van Informatiebeveiligingsfunctionarissen (IBF-ers) en inrichting van de regionale beveiligingsorganisatie (met portefeuillehouders, IBF-ers, taakaccenthouders en auditors). In een tijd dat informatiebeveiliging, ook bij de politie, nog in de kinderschoenen stond, sloeg de aanpak van uitgewerkte en praktische producten uit het Stelsel aan. Veel korpsen gingen aan de slag met onderdelen uit het

Stelsel. Opbrengsten van het Stelsel lagen onder meer op het terrein van beveiligingsorganisatie en verantwoordelijkheidstoedeling, bewustwording van het belang van informatiebeveiliging, deskundigheidsbevordering en netwerkontwikkeling. Vooral bij de rechercheonderdelen is de informatiebeveiliging goed aangeslagen.

De implementatie van het Stelsel voor Informatiebeveiliging door de korpsen leidde echter slechts bij enkele korpsen tot een systematische aanpak van het onderwerp in de managementcyclus. Het algemene beeld dat naar voren komt uit de documentatie en korpsbezoeken is dat de politie een organisatie is die actief met informatiebeveiliging bezig is. Wel blijken de politiekorpsen op het gebied van informatiebeveiliging vooral uitvoerings- en taakgericht te zijn. Op incidenten wordt over het algemeen uiterst adequaat gereageerd. Wat echter ontbreekt, is een duidelijke planmatige en structurele aanpak van informatiebeveiliging. En juist voor dit onderwerp is een planmatige, systematische benadering essentieel. In termen van de INK-stadia lijken de meeste korpsen zich, voor het onderwerp informatiebeveiliging, nog in de 'activiteit georiënteerde' fase te bevinden.
Hieronder worden kort de onderdelen beleid, organisatie, maatregelen en evaluatie belicht, aangevuld met twee paragrafen over verantwoording en samenwerking. In hoofdstuk 5 komen deze uitgebreider aan de orde.

BELEID

Het niet planmatig oppakken van het onderwerp informatiebeveiliging heeft als consequentie dat op dit moment in een aantal korpsen een door de korpsbeheerder en korpsleiding geaccordeerd beleid ontbreekt. Als er al informatiebeveiligingsbeleid wordt aangetroffen, is dit vaak verouderd en sluit het niet goed meer aan op de huidige organisatie van het korps en de politieorganisatie in het algemeen. Ontwikkelingen als de overdracht van taken naar ISC (ICT-Service Coöperatie Politie, Justitie en Veiligheid en later de voorziening tot samenwerking Politie Nederland, vtsPN), de introductie van C2000 en een andere aanpak bij interceptie (tapkamers) zijn niet of slechts beperkt in het beleid verwerkt. In dit verband is ook de mate waarin sprake is van geïntegreerd beveiligingsbeleid van belang (onder meer fysieke-, personele- en informatiebeveiliging).

ORGANISATIE

Niet alle korpsen hebben een informatiebeveiligingsfunctionaris die zorgt voor de coördinatie van alle informatiebeveiligingsactiviteiten. Deze functie wordt in het Stelsel als belangrijk beschouwd binnen de zogenaamde 'hulporganisatie'. Bovendien is er een opvallend verband tussen korpsen met een goed bezette informatiebeveiligingsorganisatie en de mate van succes bij het implementeren van een planmatige en structurele aanpak van informatiebeveiliging. Voorts is in dit verband de functiescheiding, de verantwoordelijkheidsverdeling en het verkrijgen van zekerheid na uitbesteding van belang.

MAATREGELEN

Ook op het niveau van informatiebeveiligingsmaatregelen blijken de korpsen veelal niet planmatig te werken aan de implementatie. Vaak worden maatregelen pas geïmplementeerd als dit door incidenten of door verhoogde aandacht voor informatiebeveiliging noodzakelijk blijkt. De actualiteit van de dag krijgt dan voorrang boven een structurele aanpak van het onderwerp. Belangrijke aspecten van dit onderwerp zijn voorts: het hebben van overzicht van de informatiesystemen, mede als basis voor de beveiligingsclassificatie, A&K-analyses, incidentenregistratie en het beveiligingsbewustzijn van de medewerkers.

EVALUATIE

De evaluatiecyclus van informatiebeveiliging blijkt slechts in enkele gevallen verankerd in de brede management- en in de INK-cyclus. De evaluatie van het informatiebeveiligingsbeleid vindt nog veel op ad hoc-basis plaats. Daarnaast maken de korpsen nog maar beperkt gebruik van audits als evaluatie-instrument. Een aantal korpsen past het instrument van de interne audit wel toe en incidenteel wordt ook aan andere korpsen gevraagd om een audit bij het eigen korps uit te voeren. Externe audits worden slechts beperkt toegepast. Het aspect evaluatie scoort over het algemeen het slechtst. Tevens is bij dit aspect van belang of de evaluaties zijn ingebed in de reguliere beleidsevaluatiecycli.

VERANTWOORDINGSINFORMATIE

Vaak kunnen korpsen wel laten zien dat ze een informatiebeveiligingsmaatregel hebben genomen, maar kunnen ze hierbij niet aantonen dat deze maatregelen ook op operationeel niveau werken. Ook ontbreekt het aan actuele vastleggingen van maatregelen en aan het afleggen van verantwoording over het daadwerkelijk gerealiseerde beveiligingsniveau. Hierdoor is het voor het korps moeilijk om een buitenstaander (collega-korpsen of zoals in dit geval de Inspectie OOV) inzicht te geven in de stand van zaken met betrekking tot de informatiebeveiliging en daarmee van het gerealiseerde beveiligingsniveau. Het ontbreekt kortom vaak aan verantwoordingsinformatie en aan een systeem van monitoring.

SAMENWERKING

De afgelopen jaren zijn, mede door de inrichting van de zogenaamde ISC-verzorgingsgebieden, veel samenwerkingsverbanden ontstaan op het terrein van politiële informatievoorziening en informatiebeveiliging. Deze actieve samenwerking vindt op diverse niveaus plaats en draagt in belangrijke mate bij aan een meer consistente en professionele wijze van informatiebeveiliging bij de Nederlandse politie.

Op 1 juli 2006 is de voorziening tot samenwerking Politie Nederland (vtsPN) opgericht. Een publiekrechtelijk samenwerkingsverband van alle politiekorpsen, dat gestalte geeft aan de gemeenschappelijke informatiehuishouding van de politie. In de vtsPN zijn de voormalige CIP (Concern Informatiemanagement Politie) en ISC opgegaan, alsmede de baten lastendienst ITO en het Nederlands Politie Instituut.

ACTUALITEIT VAN HET STELSEL

In 2002 werd de ontwikkeling van het Stelsel afgerond en werd het beheer van het Stelsel overgedragen aan het CIP (Concern Informatiemanagement Politie) en waar het de opleidingen betreft aan de Politieacademie. De Inspectie constateert dat deze er niet in zijn geslaagd het Stelsel en de opleidingen tussen 2002 en 2006 actueel te houden. Door achterstallig onderhoud en doordat de ontwikkelingen (zowel technisch als bestuurlijk) op het gebied van informatie en automatisering erg snel gaan, is er nu in de visie van de korpsen niet langer sprake van een actueel stelsel. In politiekringen is er momenteel discussie over de vraag of het huidige BBNP (basisbeveiligingsniveau Nederlandse politie) groot onderhoud zou moeten krijgen of dat een nieuw BBNP zou moeten worden opgesteld uitgaande van de Code voor Informatiebeveiliging. Het bestaande BBNP is echter onder andere gebaseerd op (een eerdere versie van) de Code voor Informatiebeveiliging. De conclusie dat het Stelsel, met enige regelmaat, geactualiseerd dient te worden wordt breed onderschreven.

CONCLUSIES

Is 2005, zoals destijds voorzien, inderdaad het oogstjaar geworden voor wat betreft de implementatie van de informatiebeveiliging bij de Nederlandse politie? De Inspectie stelt vast dat dit niet het geval is. Hoewel een beperkt aantal korpsen veel onderdelen van het Stelsel goed heeft geïmplementeerd, is er niet één die op álle punten goed scoort. Bovendien is de variatie tussen de korpsen nog erg groot. Dit vormt een algemeen risico door de toename van informatie-uitwisseling tussen de korpsen en het groeiend gebruik van landelijk werkende systemen; zwakke korpsen zijn daarin de ‘zwakste schakel’. Het jaar 2005 en ook 2006 hebben dus niet de oogst gebracht waarop had mogen worden gerekend.

Binnen kringen van de politie wordt de mening gedeeld dat het Stelsel niet meer actueel is en dat deze onderhoud behoeft.

De Inspectie OOV onderschrijft de mening dat het Stelsel geactualiseerd dient te worden en vervolgens met enige regelmaat onderhouden moet worden.

De Inspectie constateert dat gelet op de bovenregionale ontwikkelingen (zoals de voorziening tot samenwerking) er veranderingen zijn opgetreden in de verdeling van taken

en verantwoordelijkheden ten aanzien van de informatiebeveiliging. Duidelijk is dat de korpsbeheerder verantwoordelijk is voor die onderdelen van informatiebeveiliging die binnen zijn eigen korps plaatsvinden. Ook voor de andere onderdelen is de korpsbeheerder verantwoordelijk. Sommige onderdelen van informatiebeveiliging zijn door de korpsbeheerder uitbesteed of overgedragen aan de vtsPN, een organisatie met rechtspersoonlijkheid waarvan de korpsbeheerders het bestuur vormen. De RIP is ook van toepassing op de vtsPN. Dit betekent onder meer dat ten aanzien van de informatiebeveiliging op het bestuur van de vtsPN dezelfde verplichtingen rusten als op de korpsbeheerders van de afzonderlijke korpsen. De korpsbeheerder kan van de vtsPN zekerheden verlangen (Sevice Level Agreements en dergelijke) op het gebied van informatiebeveiliging voor de geleverde diensten. De minister heeft daarenboven de bevoegdheid om algemeen geldende regels te stellen aan de informatiebeveiliging die dan ook voor de vtsPN gelden.

AANBEVELINGEN TEN AANZIEN VAN IMPLEMENTATIE RIP EN STELSEL

De Inspectie doet op basis van bovenstaande constateringen de volgende aanbevelingen voor verbetering van de implementatie van het Stelsel voor Informatiebeveiliging binnen de Nederlandse politie:

Systeem, organisatie en uitvoering

De Inspectie OOV doet doorgaans aanbevelingen op verschillende niveaus.
Op systeemniveau zijn de aanbevelingen vaak gericht aan de betrokken minister(s), aan de Raad van Hoofdcommissarissen of aan het Korpsbeheerdersberaad. Op organisatieniveau zijn ze gericht aan de korpsbeheerder of korpschef, dit geldt ook voor aanbevelingen op uitvoeringsniveau. Veel van de aanbevelingen zijn gericht op aspecten van organisatie en uitvoering. Het lijkt daardoor of er op systeemniveau geen aanbevelingen te doen zouden zijn; niets is minder waar. De politie kent momenteel een periode waarin er bovenregionaal enorm veel in ontwikkeling is op het terrein van ICT en informatiebeveiliging (het instellen van de voorziening tot samenwerking met daarin CIP en ISC, de samenwerking in de verzorgingsgebieden, de implementatie van onderdelen uit 'wenkend perspectief', et cetera) en waarin regionale taken op het gebied van informatiebeveiliging deels worden overgenomen of uitgevoerd door bovenregionale organen. Een complexe bestuurlijke organisatie die ook nog voortdurend in ontwikkeling is.
Direct aansluitend op deze paragraaf komen de aanbevelingen op organisatieniveau aan de orde. Deze zijn vooral gebaseerd op de bevindingen uit de korpsbezoeken (hoofdstuk 5). Daarna worden aanbevelingen op systeemniveau gedaan, deze gaan vooral over het actueel maken en houden van het Stelsel, het bevorderen van een planmatige aanpak bij implementatie en de opzet van verantwoordingsrapportages.

BELEID

Samenhangend beveiligingsbeleid (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie van vtsPN)

Zorg voor het formaliseren en actualiseren van samenhangend beveiligingsbeleid. Dit beleid dient de verschillende veiligheidsgebieden (personele aspecten van beveiliging, facilitaire en fysieke beveiliging en informatiebeveiliging) onder één paraplu te brengen, waardoor de maatregelen binnen deze gebieden beter op elkaar kunnen worden afgestemd.

MAATREGELEN

Risicoanalyse (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Zorg voor het uitvoeren van risicoanalyses (Afhankelijkheids- en Kwetsbaarheids-analyses) voor informatiesystemen om vast te stellen of voldoende informatie-beveiligingsmaatregelen zijn getroffen (uitgaande van het BBNP) en integreer dit in de reguliere planning- en controlcyclus. Hierbij kan een afhankelijkheidsanalyse worden uitgevoerd om te bepalen of het gewenste beveiligingsniveau gelijk of onder het basis-beveiligingsniveau ligt. Voor informatiesystemen waarbij het beveiligingsniveau boven het basisbeveiligingsniveau ligt, dienen met een kwetsbaarheidsanalyse aanvullende maatregelen te worden bepaald.

Incidentenregistratie (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Zorg voor een integrale registratie van (informatie)beveiligingsincidenten als onderdeel van de evaluatiecyclus. Deze centrale registratie dient alle incidenten te bevatten en dient daarvoor op regelmatige basis te worden gevoed vanuit de verschillende incidenten-registraties op het gebied van interne onderzoeken, ICT-helpdesk, fysieke toegangs-beveiliging en dergelijke. De incidenten in de centrale registratie dienen vervolgens regelmatig te worden geanalyseerd. Deze analyse is vervolgens weer input voor de evaluatie van beveiligingsbeleid en -maatregelen.

Beveiligingsbewustzijn (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Bevorder op een planmatige wijze het beveiligingsbewustzijn van politiemedewerkers. Het gedrag van politiemedewerkers bepaalt in hoge mate welke risico's het korps loopt op het gebied van informatiebeveiliging. Ook bepaalt dit het gedrag van politie-medewerkers in hoge mate de effectiviteit van de informatiebeveiligingsmaatregelen. Daarom is het zeer belangrijk om pro-actief te sturen op het juiste gedrag van de politiemedewerkers.

ORGANISATIE

Voldoende personeel (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Maak voldoende personeel vrij voor de coördinatie van informatiebeveiligingsactiviteiten om een adequate implementatie van het Stelsel mogelijk te maken. Op basis van de onderzoeksgegevens lijken korpsen met goed opgeleide, enthousiaste en actieve IBF-ers (die voldoende tijd kunnen besteden aan informatiebeveiligingstaken) succesvoller te zijn bij het implementeren van het Stelsel voor Informatiebeveiliging, dan korpsen zonder of met beperkte inzet van IBF-ers.

EVALUATIE

Audits (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Maak systematisch gebruik van het instrument van interne (en externe) audits om zekerheid te verkrijgen over de implementatie van (onderdelen van) het Stelsel voor Informatiebeveiliging. Interregionale (interne) audits zijn hierbij een effectieve werkwijze.

Beleidsevaluatie en INK (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Evalueer het (informatie)beveiligingsbeleid en maak dit onderdeel van de beleids-evaluatie- en INK-cyclus.

Geen activiteit maar een proces

Algemeen aandachtspunt hierbij is dat de implementatie van bovengenoemde aanbevelingen niet als een op zichzelf staande activiteit moet worden gezien; informatie-beveiliging is boven alles een proces, dat dient te zijn ingebed in de managementcyclus van de politiekorpsen.

AANBEVELINGEN OP SYSTEEMNIVEAU

Planmatige aanpak (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Realiseer een planmatige implementatie van het BBNP door het opstellen van informatie-beveiligingsplannen en het monitoren van de uitvoering daarvan mede door het (laten) uitvoeren van interne en externe audits.

Samenwerking (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Zorg in het hele land voor verdergaande interregionale samenwerking op het gebied van informatiebeveiliging en zorg dat de in samenwerking tot stand gekomen producten snel in de korpsen kunnen worden geïmplementeerd.

Rapportage korpsbeheerders (geadresseerd aan de korpsbeheerders en bestuur en directie vtsPN)

Zorg dat de korpsen en de vtsPN vierjaarlijks rapporteren aan de korpsbeheerders over de werking en effectiviteit van de informatiebeveiliging in hun korpsen en bij de vtsPN. Het Korpsbeheerdersberaad zou deze rapportage kunnen agenderen voor overleg met de ministers van BZK en van Justitie. De Inspectie geeft de korpsbeheerders in overweging om deze rapportage een gezamenlijke te laten zijn om zodoende het belang van gezamenlijkheid bij informatiebeveiliging te onderstrepen. Gezien de huidige stand van zaken met betrekking tot de informatiebeveiliging bij de Nederlandse politie beveelt de Inspectie verder aan om in eerste instantie de frequentie van deze rapportages te verhogen, zodat de eerste rapportage voor het eind van 2008 beschikbaar is.

Actualiteit van het Stelsel (geadresseerd aan de korpsbeheerders)

Zorg voor een actueel Stelsel voor Informatiebeveiliging met een basisbeveiligingsniveau dat rekening houdt met de huidige technische en bestuurlijke context van het politiewerk en met de actuele ontwikkelingen op het gebied van informatiebeveiliging. De opleidingen dienen hierbij aan te sluiten. Bekijk, in het licht van de huidige bestuurlijke ontwikkelingen, ook of de toedeling van taken en verantwoordelijkheden ten aanzien van de informatiebeveiliging aanpassing behoeft. Zorg er intussen voor dat de implementatie van het huidige Stelsel en BBNP krachtig ter hand worden genomen.

INTERCEPTIE

SAMENVATTING EN CONCLUSIES

De Normstelling Inrichting interceptiefaciliteiten is in 2004 aan de RIP toegevoegd. Hierin wordt bepaald dat de korpsbeheerder het beheer van de interceptiefaciliteiten dient te beleggen in het beleidsdocument over informatiebeveiliging. In het onderzoek is een aantal aspecten uit de Normstelling belicht. Een deel van het interceptieproces vindt centraal plaats (bij de Unit Landelijke Interceptie (ULI) van het Korps Landelijke Politiediensten (KLPD)), een ander deel ter plekke bij de korpsen.
Een zeer beperkt aantal korpsen heeft in zijn informatiebeveiligingsbeleid een concrete verwijzing naar het interceptiebeveiligingsbeleid opgenomen.
De taken, verantwoordelijkheden en bevoegdheden van het management en de medewerkers die betrokken zijn bij het gebruik en beheer van de interceptiefaciliteiten zijn

niet door alle korpsen vastgelegd. Verwijzing naar procesbeschrijvingen over de interactie tussen de korpsen en de ULI laat onverlet dat de korpsen ter zake zelf afspraken moeten maken en vastleggen.
De functiescheiding binnen de interceptieorganisatie laat een divers beeld zien. Voor kleinere korpsen lijkt het vaak lastig om dat in voldoende mate te realiseren, maar er zijn ook grote verschillen in de mate waarop aan de functiescheiding in plannen, procedures en werkinstructie(s) invulling is gegeven.
De korpsen dienen voldoende informatiebeveiligingsmaatregelen te treffen met betrekking tot de inrichting, de logische toegangsbeveiliging en de fysieke toegangsbeveiliging van de interceptiefaciliteiten. Veel korpsen hebben op dit moment nog moeite om volledig aan de Normstelling te voldoen. Als redenen noemen de korpsen onder meer het gebrek aan mogelijkheden in het ULI-systeem om het gewenste niveau van functiescheiding te realiseren en aanstaande verbouwingen of verhuizingen om de fysieke toegangsbeveiliging tot de interceptiefaciliteiten conform de Normstelling in te kunnen richten.
Een beperkte bezetting van de interceptieafdeling (vaak slechts één interceptiecoördinator) en de piketdiensten bieden ook niet altijd de mogelijkheid om adequaat toezicht te houden op het gebruik van de interceptiefaciliteiten.
De korpsen hebben nog slechts in beperkte mate uitvoering gegeven aan de auditing van de interceptiefaciliteit en de interne uitwerking daarvan. Achttien korpsen hebben in het geheel geen audits laten uitvoeren op de interceptiefaciliteiten.
Concluderend kan worden gesteld dat de meeste korpsen nog moeite hebben om op alle onderdelen te voldoen aan de Normstelling. Maatregelen worden wel genomen, maar van een planmatige aanpak is daarbij doorgaans geen sprake.

AANBEVELINGEN

Beleidskader (geadresseerd aan de korpsbeheerders en korpschefs)

Formuleer een beleidskader voor een gestructureerde en planmatige aanpak van de interceptiebeveiliging en beleg de verantwoordelijkheid voor de uitvoering daarvan op strategisch niveau binnen het korps.

Audits (geadresseerd aan korpsbeheerders en korpschefs)

Zorg dat op korte termijn de voorgeschreven interne en externe audits worden uitgevoerd, zodat kan worden vastgesteld welke hiaten er (nog) zijn in de implementatie van de Normstelling (toegespitst op het uitluisteren).

Overeenkomsten (geadresseerd aan de korpsbeheerders)

Leg de relatie van het politiekorps met het KLPD/ULI over het interceptieverkeer vast in een geformaliseerde overeenkomst.

Inleiding en aanleiding

1

Informatie wordt door de Nederlandse politiekorpsen als een van de belangrijke productiefactoren beschouwd. Hierbij wordt een toenemend beroep gedaan op informatie van buiten het eigen korps. Vanuit het vitale belang van goede informatie voor de politie is informatiebeveiliging belangrijk. Informatiebeveiliging is meer dan enkel het afschermen van vertrouwelijke gegevens. Doorgaans wordt bij informatiebeveiliging gedacht aan de BEI-eisen, waarbij de B staat voor beschikbaarheid (is de informatie er als het erop aankomt?), de E voor exclusiviteit (is informatie voldoende afgeschermd?) en de I voor integriteit (kloppen de gegevens/de cijfers?).
Informatiebeveiliging is niet iets waar 'ook aandacht voor moet zijn', maar een essentiële voorwaarde voor een goed verloop van alle werkprocessen bij de politie.
Het feit dat steeds meer informatie binnen de Nederlandse politie wordt uitgewisseld en gedeeld, leidt er bovendien toe dat informatiebeveiliging bij alle korpsen van gelijk niveau dient te zijn. Immers een korps moet er op kunnen vertrouwen dat zijn informatie bij 'de buren' ook veilig is.
Informatiebeveiliging, in al zijn facetten, is een belangrijk onderdeel van de uitvoering van de justitiële politietaak. Een adequate naleving van de regelgeving op dit gebied is derhalve noodzakelijk als schakel in de strafrechtelijke keten.

De Inspectie Openbare Orde en Veiligheid (Inspectie OOV) heeft in het najaar van 2005 zeven prioriteiten voor het toezicht op de politie vastgesteld: professionaliteit, integriteit, ketengerichtheid, omgevingsgerichtheid, verantwoording, paraatheid en informatie. Het kernthema informatie heeft ook in het werkplan 2006 en 2007 van de Inspectie een plaats gekregen.
In eerdere onderzoeken heeft de Inspectie al aandacht aan het kernthema informatie geschonken. In het onderzoek naar de politiële jeugdtaak (februari 2004), in het onderzoek naar de coördinatie en uitwisseling van politie-informatie (december 2004), in het onderzoek naar de kwaliteit van de politiële opsporingstaak ('Opsporing bezocht', maart 2006) en een vervolgrapport op het thema informatie-uitwisseling (december 2006).

INFORMATIEBEVEILIGING

Het Inspectie onderzoek naar de politiële opsporingstaak, 'Opsporing bezocht', richtte zich op vier thema's. Eén daarvan was informatie en informatiebeveiliging. De informatiesystemen die bij de opsporing worden gebruikt zijn kwetsbaar en vragen een goede beveiliging. Er werd voor dit onderzoek informatie verzameld over het beveiligingsbeleid van de korpsen, het gebruik van risicoanalyse, de genomen beveiligingsmaatregelen, de verantwoordelijkheidstoedeling binnen de organisatie en de toepassing van audits. Kortom alle fasen van de beleidscyclus. Geconcludeerd werd 'Over het algemeen heeft de informatiebeveiliging bij de Nederlandse politie nog niet het beoogde niveau.

Van systematische aandacht voor het onderwerp is slechts bij enkele korpsen sprake .... sommige korpsen hebben wel beleid en plannen, maar geen risicoanalyse gedaan of maatregelen genomen; andere korpsen hebben op diverse vlakken beveiligingsmaatregelen genomen, maar hebben nauwelijks beleid op dit gebied'. De diepgang van dit onderdeel van 'Opsporing bezocht' was echter beperkt. Deze conclusie was slechts gebaseerd op ingevulde vragenlijsten en meegestuurde (ondersteunende) documentatie. De behoefte om een meer gefundeerd oordeel te kunnen geven over de stand van informatiebeveiliging bij de Nederlandse politie, heeft geleid tot het voorliggende onderzoek. Anders dan in 2006 werden de korpsen ditmaal niet 'op hun blauwe ogen' geloofd, maar leidden ontbrekende bewijzen tot een onvoldoende score.

VIR EN RIP

Nadat in 1994 voor de rijksoverheid het Voorschrift Informatiebeveiliging Rijksdienst (VIR) van kracht werd, werd in 1997 door de ministers van BZK en Justitie voor de politie een vergelijkbaar voorschrift vastgesteld, te weten de Regeling Informatiebeveiliging Politie (RIP). Sinds die tijd is de politie gericht aan de gang gegaan met informatiebeveiliging. De RIP geeft aan dat de korpsbeheerders moeten zorgen voor beveiligingsbeleid en beveiligingsplannen. In 1997 werd ook het Expertisecentrum Informatiebeveiliging Nederlandse politie (ECIB) ingesteld. Om de invoering van de informatiebeveiliging te ondersteunen heeft het Expertisecentrum een Stelsel voor Informatiebeveiliging ontwikkeld. Dit stelsel bevatte onder meer leidraden, handleidingen en hulpmiddelen. Eén van de leidraden was het Basis Beveiligingsniveau Nederlandse Politie (BBNP).

2005 OOGSTJAAR

In de systematiek van het Stelsel is voorzien in een audit op de informatiebeveiliging in het jaar voorafgaand aan de algemene INK-audit. De INK-audits vonden in 2006/2007 plaats. De korpsen hebben daarmee impliciet aangegeven dat 2005 het oogstjaar zou zijn voor de implementatie van het BBNP. Voor de Inspectie Openbare Orde en Veiligheid was dit aanleiding om onderzoek te doen naar de mate waarin de RIP, het Stelsel en het BBNP zijn ingevoerd door de korpsen. De Inspectie OOV wil met dit onderzoek een bijdrage leveren aan (de verbetering van) de informatiebeveiliging bij de Nederlandse politie. Enerzijds door de mate van implementatie per korps in beeld te brengen, maar ook door succesvolle initiatieven van korpsen te belichten.

SAMENWERKING EN UITBESTEDING

De directie Strategie en de directie Politie van het directoraat-generaal Veiligheid (DGV) van het ministerie van BZK zijn beleidsmatig betrokken bij het onderwerp informatiebeveiliging bij de Nederlandse politie. Deze directies hadden de behoefte om een evaluatie uit te voeren naar de implementatie van de regelgeving die in 1997 werd

vastgesteld (RIP) en de daadwerkelijke informatiebeveiliging binnen de korpsen volgens de eisen die in de periode 2000 tot 2002 zijn vastgelegd (het Stelsel voor Informatiebeveiliging bij de Nederlandse politie, waaronder het BBNP). De Inspectie OOV heeft in overleg met de beide directies besloten dit onderzoek uit te voeren.

EXTERNE DESKUNDIGHEID

De Inspectie heeft besloten het toetsende gedeelte van het onderzoek bij de korpsen uit te besteden aan een externe deskundige. PricewaterhouseCoopers (PwC) heeft dit gedeelte van het onderzoek in de 25 regiokorpsen uitgevoerd. De departementale Auditdienst heeft volgens dezelfde methodiek en gebruik makend van hetzelfde normenkader, het onderzoek bij het KLPD uitgevoerd. Het toetsende deel van het onderzoek is begeleid door een begeleidingsgroep onder leiding van de Inspectie OOV en met participatie van de Auditdienst, de directie Strategie en de directie Politie van het ministerie van BZK.
De begeleidingsgroep heeft ook de Inspectie in verschillende fasen van het onderzoek geadviseerd. Voor wat betreft het centrale deel van de interceptie is gebruik gemaakt van een recent afgesloten audit door de Auditdienst van het ministerie van BZK. Alhoewel sprake is van samenwerking en uitbesteding is de Inspectie OOV verantwoordelijk voor de eindrapportage en de oordeelsvorming daarin.

ONDERZOEKSVRAAG EN –AANPAK

De Inspectie OOV heeft willen vaststellen of de uit de RIP en het Stelsel voortvloeiende verplichtingen door de korpsen zijn geïmplementeerd. Om zo een beeld te krijgen van de wijze en het niveau van informatiebeveiliging zowel bij de Nederlandse politie als geheel als bij de individuele korpsen. De huidige regelgeving is hierbij de basis voor het gebruikte normenkader. De Inspectie had reden om aan te nemen dat de informatiebeveiliging bij de korpsen nog niet overal norm-conform is. Het onderzoek had niet het karakter van een audit en er is geen gedetailleerd onderzoek verricht naar de implementatie van de afzonderlijke maatregelen van het Stelsel. Wel is gekeken of de korpsen aannemelijk kunnen maken dat ze het basisbeveiligingsniveau (BBNP) hebben ingevoerd. Daarnaast is, zoals al aangegeven, meer specifiek gekeken naar een aantal aspecten van informatiebeveiliging rond de tapkamers.

INTERCEPTIE

Naast de algemene vraagstelling heeft de Inspectie specifiek gekeken naar de informatiebeveiliging rond interceptie (tapkamers). Uitgangspunt voor dit deel van het onderzoek is de Normstelling Inrichting Interceptiefaciliteiten die sinds 2003 onderdeel is van de RIP. Een deel van het interceptieproces vindt centraal plaats (bij het Korps Landelijke Politiediensten (KLPD)), een ander deel ter plekke bij de korpsen. Omdat het Korps Landelijke Politiediensten, als onderdeel van het ministerie van BZK in de departemen-

tale Auditdienst een reguliere toezichthouder kent, heeft deze dienst het onderzoek naar het centrale deel bij het KLPD uitgevoerd. De Auditdienst heeft in hoofdstuk 6, naar aanleiding van een door haar uitgevoerde audit, tevens een korte bijdrage geschreven over het centrale deel van de interceptie. In datzelfde hoofdstuk wordt door de Inspectie OOV gerapporteerd over de decentrale interceptieprocessen.

REIKWIJDTE

Het onderzoek richtte zich op de verplichtingen die voortvloeien uit de RIP en het Stelsel. Daarbij gaat het om de vraag of korpsen op een planmatige manier omgaan met informatiebeveiliging en invulling geven aan de plan-do-check-act-cyclus. Uitgaande van het normenkader is vooral bewijs verzameld vanuit de management-cyclus van de korpsen.
Voor onderzoek naar de tapfaciliteiten is gebruik gemaakt van de 'Normstelling Inrichting Interceptiefaciliteiten'
Het onderzoek was (behoudens de speciale aandacht voor interceptie) níet gericht op de meer gevoelige, kritische systemen die een hoger beveiligingsniveau vergen dan het BBNP. De Inspectie geeft derhalve geen antwoord op de vraag of deze systemen afdoende zijn beveiligd. Het gegeven dat nauwelijks Afhankelijkheids- & Kwetsbaarheidsanalyses (A&K analyses) zijn uitgevoerd maakt dat ook hier vraagtekens bij kunnen worden geplaatst. Het zou daarbij even goed kunnen dat het gerealiseerde beveiligingsniveau niet te laag maar juist te hoog is. Bovendien vragen kritische systemen doorgaans maatregelen die voortbouwen op de basisbeveiliging. Als de basisbeveiliging niet volledig is geïmplementeerd is er derhalve sprake van een zeker inherent risico.

Het onderzoek is vervolgens toegespitist op de volgende onderzoeksvragen:

1. In hoeverre hebben de korpsen de maatregelen getroffen die in de RIP en het van de RIP afgeleide Stelsel Informatiebeveiliging Politie zijn aangegeven?
2. Hebben de 26 korpsen informatiebeveiligingsbeleid?
3. Wanneer hebben de 26 korpsen het BBNP ingevoerd?
4. Hoe is de informatiebeveiligingsfunctie verankerd in de organisatie van de korpsen?
5. Welke uit de RIP voortvloeiende en via A&K-analyses benoemde, aanvullende maatregelen bovenop het niveau van het BBNP hebben de korpsen genomen?
6. Welke maatregelen hebben de 26 korpsen genomen met betrekking tot de beveiliging van de lokale faciliteiten voor de toegang tot de centrale interceptiefaciliteiten?
7. Is de aanpak van informatiebeveiliging centraal bij ULI (Unit Landelijke Interceptiefaciliteiten) voldoende en zijn afdoende beveiligingsmaatregelen getroffen? NB. Hierover wordt door de Auditdienst van het ministerie van BZK op basis van een eigen audit kort gerapporteerd.
8. Op welke wijze en in welke vorm dragen ISC (ICT-Service Coöperatie Politie, Justitie en Veiligheid) en CIP (Concern Informatiemanagement Politie) bij aan het Stelsel voor Informatiebeveiliging? Hoe actueel is het BBNP?
9. Welke good practices zijn er en welke lessons to learn?

Tijdens het onderzoek bleek de deelvraag over de positie van ISC en CIP bijzonder actueel. Mede als gevolg van de oprichting van de voorziening tot samenwerking Politie Nederland (vtsPN) in 2006 en het onderbrengen van ISC en CIP bij de voorziening, is een dermate dynamische situatie ontstaan dat de Inspectie in deze rapportage volstaat met een korte, beschrijvende, aanduiding van de nu ontstane situatie en zich onthoudt van een oordeel. De Inspectie zal wel een conclusie en een aanbeveling wijden aan de actualiteit van het Stelsel als zodanig.

Onderzoeksmethoden en uitvoering van het onderzoek

Het onderzoek werd bij alle 26 korpsen uitgevoerd. De externe deskundige heeft het onderzoek bij de 25 regiokorpsen uitgevoerd, terwijl de Auditdienst van het ministerie van BZK, aan de hand van hetzelfde normenkader en dezelfde vragenlijst, het onderzoek uitvoerde bij het KLPD. Daarnaast heeft de Auditdienst, uitgaande van haar auditplan voor 2006, onderzoek gedaan naar de centrale interceptiefaciliteit bij het KLPD. De Inspectie OOV heeft de Auditdienst gevraagd een korte schets te geven van de uitkomsten van dit onderzoek voor het centrale deel van de interceptie. Daardoor ontstaat in dit rapport een zo compleet mogelijk beeld van de informatiebeveiliging bij interceptie.

Het onderzoek kende verschillende fasen:

Voorbereiding

Allereerst werden de verplichtingen die voortvloeien uit de RIP en het Stelsel (al dan niet uitgewerkt in de leidraden en handreikingen) geïnventariseerd. Deze inventarisatie was het uitgangspunt bij het vaststellen van het normenkader. Naast meer 'algemene' normen werd ook expliciet gekeken naar normen ten aanzien van de tapkamers (de Normstelling inrichting interceptiefaciliteiten). Het normenkader is vertaald in een vragenlijst. Normenkader en vragenlijst zijn als bijlagen op cd-rom bij deze rapportage gevoegd.

Bestuderen documentatie en houden interviews

Bestuderen van beschikbare documentatie (onder meer de korpsantwoorden en -documentatie uit het Inspectie onderzoek naar kwaliteit van opsporing (2005/2006) en eerdere evaluaties van het Stelsel) en houden van interviews bij ISC en CIP. Omdat een deel van de informatiebeveiliging buiten de korpsen plaatsvindt was een oriëntatie bij ISC (gericht op dienstenniveaubeheer in termen van beveiligingsmaatregelen en afspraken (zoals Service Level Agreement (SLA)) daaromtrent met de korpsen) en het CIP (gericht op (verdere) ontwikkeling en onderhoud van een Stelsel voor Informatiebeveiliging) nodig.

Schriftelijke vragenlijsten

Schriftelijke vragenlijst voor de regiokorpsen en het KLPD met betrekking tot naleving van de RIP en implementatie van het Stelsel voor Informatiebeveiliging Politie, waaronder het BBNP. In deze vragenlijst werden ook vragen opgenomen met betrekking tot beveiliging van de lokale faciliteiten die toegang geven tot de interceptiefaciliteiten.

Verificatie bij de korpsen door middel van interviews en aan de hand van beschikbare documentatie

De antwoorden van de korpsen werden tijdens een korpsbezoek geverifieerd. Als bewijsstukken ontbraken werd de voorstelling van zaken gecorrigeerd. De interviews waren in de meeste gevallen met de Chief Information Officer (CIO), de informatiebeveiligingsfunctionaris (IBF-er) en de verantwoordelijke voor de interceptie. De vragenlijsten en de ontvangen antwoorden werden door of namens de korpschef ondertekend. De korpsbeelden die PwC maakte werden voor hoor en wederhoor aan de korpsen voorgelegd.

Inventariseren good practices

Op basis van de beschikbare informatie is tijdens de korpsbezoeken bijzonder gelet op good practices en lessons to learn. Deze zijn in aparte tekstblokken in hoofdstuk 4 opgenomen.

LEESWIJZER

Hoofdstuk 2 bevat een kort overzicht van de geschiedenis van ICT bij de politie. Hoofdstuk 3 geeft vervolgens kort uitleg over het Stelsel voor Informatiebeveiliging en de ontwikkelingen die tot het Stelsel hebben geleid. In hoofdstuk 4 wordt geschetst hoe het nu is gesteld met het Stelsel en de actualiteit daarvan. Na dit hoofdstuk wordt gerapporteerd over de inspanningen en prestaties van de korpsen op het gebied van informatiebeveiliging. Daarin is aandacht voor de aspecten beleid, organisatie, maatregelen en evaluatie. Ook is in hoofdstuk 5 een aantal zogenaamde good practices belicht. Hoofdstuk 6 gaat over informatiebeveiliging ten aanzien van interceptie. De bijlagen, die overigens op de bijgevoegde cd-rom zijn te vinden, bevatten naast het normenkader en de gebruikte vragenlijst, ook 26 korpsbeelden waarin per korps de prestaties en de inspanningen worden geschetst. Als peildatum geldt daarbij het derde kwartaal van 2006.

ICT bij de politie, een terugblik

2

In dit hoofdstuk wordt in vogelvlucht de ontwikkeling naar één informatiehuishouding voor de Nederlandse politie sinds 1999 beschreven.

BELEIDSPLAN NEDERLANDSE POLITIE 1999-2002

Sinds de vorming van de politieregio's in 1993 zijn op ICT-gebied bij de Nederlandse politie vooral de instelling van de Regieraad ICT Politie en de door haar ingezette Bestek-operatie van belang geweest. Aan de basis daarvan stonden het Beleidsplan Nederlandse Politie 1999-2002 uit 1998 en het Convenant Politie 1999.
Met het Beleidsplan Nederlandse Politie 1999-2002 werd de wens naar meer samenwerking op het gebied van ICT verwoord. De minister van BZK stelde vast dat in de voorafgaande jaren veel in beweging was gezet om de informatievoorziening van de Nederlandse politie te verbeteren, in eerste instantie vooral binnen de korpsen. Het is geleidelijk steeds duidelijker geworden dat ook de bovenregionale informatievoorziening verbetering behoeft. Vooral aan duidelijkheid en slagvaardigheid in de besluitvorming op dit punt had het ontbroken. Wanneer dit probleem niet werd opgelost achtte hij het gevaar groot dat afspraken zouden blijven verzanden en dat de voortgang zou stagneren. De minister concludeerde dat er nog veel moest gebeuren om de ontstane achterstanden in te lopen en een niveau te bereiken waarop de beschikbare ICT hulpmiddelen het primaire proces ondersteunen.

CONVENANT

Het Convenant Politie 1999[1] vormde de basis voor het inlopen van de achterstanden op het gebied van ICT. Op 24 augustus 1999 heeft de minister van BZK de Tweede Kamer hierover schriftelijk geïnformeerd[2]. Uit het oogpunt van doelmatigheid was in zijn visie de regionale maat te klein voor ICT-beleid. Om de noodzakelijke vernieuwingen grootschalig te kunnen invoeren en beheren was het nodig de kwaliteit van die ICT-functie te verbeteren en de organisatie ervan aan te passen. In voorafgaande jaren hadden verschillende regiokorpsen de samenwerking op het gebied van beheer van gezamenlijke informatiesystemen en rekencentra al gezocht en gevonden. Echter, nog lang niet overal was de meest efficiënte schaal bereikt. Op 9 november 1999 werd het Convenant Politie 1999 getekend door de minister en de korpsbeheerders. Vervolgens werd op 22 november 1999 de Regieraad ICT Politie ingesteld.

1 Tweede Kamer, 1998-1999, 26 3445, nr. 15.
2 Beleidsplan Nederlandse politie 1999-2002; brief minister van BZK over het inlopen van achterstanden op het gebied van ICT, Tweede Kamer 1998-1999, 26345, nr. 19.

MOTIE RIETKERK

Op 21 november 2000 heeft de Tweede Kamer de motie-Rietkerk[3] aangenomen. In deze motie wordt geconstateerd dat de politie een zorgwekkende achterstand heeft op ICT-gebied en dat er nog veel belemmeringen moeten worden weggewerkt. De Tweede Kamer uitte de wens dat er binnen vier jaar één informatiesysteem voor het politiewerk zou komen en heeft aan de minister van BZK verzocht om jaarlijks te rapporteren over de voortgang. De minister van BZK heeft toegezegd om deze motie uit te voeren.

OPDRACHT REGIERAAD ICT POLITIE

De minister van BZK heeft in 1999 de Regieraad ICT Politie ingesteld met als taak het realiseren van één samenhangende, robuuste en toekomstvaste informatiehuishouding voor de Nederlandse politie. Het standaardiseren van informatie- en ICT-voorzieningen staat hierbij centraal. Volgens de instellingsregeling draagt de Regieraad zorg voor:

- ontwikkeling, uitvoering, evaluatie en bijstelling van het ICT-beleid van de Nederlandse politie;
- realisatie van één gelijkwaardig basisniveau van ICT-voorzieningen en een homogene basisinformatievoorziening bij de korpsen;
- ontwikkeling van standaarden voor netwerkvoorzieningen, hardware en software voor de korpsen en voor de aansluiting tussen de politiekorpsen en de door de Regieraad aangewezen derden.

MASTERPLAN

De Regieraad stelde in de eerste helft van 2000 haar Masterplan op. Doel was om één robuuste, gebruiksvriendelijke, veilige, beheersbare en toekomstvaste informatievoorziening voor het politiewerk te ontwikkelen. Een voorziening die bovendien informatie-uitwisseling in de keten en in het kader van de internationale verplichtingen mogelijk zou maken. De minister bood het Masterplan op 23 augustus 2000 aan aan de Tweede Kamer. Het plan schetst wat de Regieraad in de periode tot en met 2005 wilde realiseren. Als basis voor de inhaalslag noemde de Regieraad de volgende vier pijlers:

- vernieuwing van de informatievoorziening;
- professionaliseren van het ICT-proces;
- optimaliseren van de P&O component;
- sturing door de Regieraad en de organisatie daarvan.

Deze resultaten zouden voor het eind van 2005 bereikt moeten zijn. De Regieraad wilde beginnen met het ontsluiten van gegevens in de bestaande interne en externe databestanden met behulp van moderne technologie. Dit zou onmiddellijk de informatie en samenwerking verbeteren. Het belangrijkste risico dat in het Masterplan werd onderkend was de implementatie. De Regieraad kondigde aan hier extra alert op te zijn.

3 Tweede Kamer, 2000-2001, nr. 48

BESTEK 2001-2005

Het Masterplan werd uitgewerkt in het Bestek 2001-2005. De concepten vraagsturing en aanbodverzorging staan hierin centraal. Vraagsturing is de onderlinge afstemming van de uiteenlopende behoefte van de korpsen en de bundeling van deze behoeften tot eenduidige opdrachten. Aanbodverzorging is de gecoördineerde ontwikkeling van applicaties, technische infrastructuur en levering van diensten, zoals applicatiebeheer en netwerkdiensten.

De opdracht aan de Regieraad luidde:

1. organiseer de ICT voor de politie langs lijnen van vraag en aanbod;
2. zorg dat de technische infrastructuur homogeen wordt;
3. concentreer de rekencentra van de korpsen in zes verzorgingsgebieden;
4. ontwikkel een architectuur voor het informatiehuis van de politie;
5. standaardiseer/uniformeer de toepassingen langs lijnen van die architectuur;
6. zorg voor een beter en professioneler informatiehuis van de politie.

OPRICHTING CIP EN ISC

In 2002 zijn de CIP (Concern Informatiemanagement Politie) en de ISC (ICT-Service Coöperatie Politie, Justitie en Veiligheid) opgericht. De Regieraad functioneert als Raad van Toezicht. De minister van BZK heeft destijds aan de Tweede Kamer aangegeven dat hij voornemens is om deze privaatrechtelijke organisaties om te vormen naar publiek-rechtelijke rechtspersonen. Dit is inmiddels gebeurd met de oprichting van vtsPN op 1 juli 2006.

MIDTERM REVIEW

Medio 2003 heeft het Expertisecentrum (ECIB) een midterm review uitgevoerd naar de voortgang van de uitvoering van Bestek 2001-2005[4]. De meest opvallende conclusie was dat eind 2005 de doelstelling van het Bestek voor niet meer dan 70% zou worden gehaald.

RAPPORT ALGEMENE REKENKAMER 2003

In 2003 verscheen ook een rapport van de Algemene Rekenkamer over de ICT bij de Nederlandse politie. De Algemene Rekenkamer deed het onderzoek op verzoek van de Tweede Kamer. Daarbij is gekeken naar de uitgaven, het functioneren van toepassingen, samenwerking en naar de coördinerende rol van de minister van BZK. Ook de Bestek-operatie onder leiding van de Regieraad is betrokken in dit onderzoek. De Algemene Rekenkamer proefde bij de politieregio's een bereidheid tot samenwerken. Die bereidheid tot samenwerken werd echter danig op de proef gesteld door de grote

4 Tweede Kamer, vergaderjaar 2000-2001, 26 345, nr. 62

tekortkomingen in de informatiehuishouding. Ook de Algemene Rekenkamer meende dat voor 2006 niet één gezamenlijke informatiehuishouding tot stand zou zijn gebracht. De Algemene Rekenkamer uitte verder haar zorgen over de betaalbaarheid van de Bestek-operatie.

VERZORGINGSGEBIEDEN

Sinds 2002 verzorgt ISC voor de regiokorpsen een groeiend aantal automatiseringstaken. In principe zijn vanaf de overgangsdatum de systemen overgegaan van het regiokorps naar het regionale rekencentrum van het ISC-verzorgingsgebied. Daarvan zijn er zeven in Nederland (zes regionale en een landelijke). Er bestaan verschillen tussen de verzorgingsgebieden op het gebied van producten en diensten. De bedoeling is om deze verschillen in de komende jaren weg te nemen.

HERIJKT BESTEK

Op basis van de midterm review en het onderzoek van de Algemene Rekenkamer heeft een herijking van het Bestek 2001-2005 plaatsgevonden. Het herijkte Bestek is in het najaar van 2004 bestuurlijk geaccepteerd als richtinggevend document voor komende jaren. De belangrijkste koerswijzigingen ten opzichte van het oorspronkelijke Bestek waren:

- het vervangen van de 'big-bang' strategie - waarbij oude systemen in hoog tempo volledig vervangen worden door nieuwe - door een strategie waarin wordt voortgebouwd op de bestaande situatie. De meest urgente functionaliteiten worden snel gerealiseerd via verbeteringen aan bestaande systemen;
- het jaarlijkse volume aan veranderingen wordt begrensd. Hierbij wordt rekening gehouden met: financiële middelen, de beperkingen van korpsen bij het implementeren van processen en systemen en de beheer- en ontwikkelcapaciteit van de vraag- en aanbodorganisatie (CIP en ISC), die als nieuwe organisaties zelf nog in ontwikkeling zijn;
- onderkenning van het feit dat het Bestek een meerjarige, zeer complexe grootschalige transitie is met een doorlooptijd van vele jaren;
- een besturingswijze, waarbij flexibel en stapsgewijs het onveranderde einddoel (de gezamenlijke uniforme informatiehuishouding) wordt behaald. De inhoud van iedere stap wordt bepaald door de op dat moment geldende omstandigheden en prioriteiten. De Regieraad is ervan overtuigd dat gezamenlijkheid de cruciale voorwaarde is voor het realiseren van één uniforme informatiehuishouding. De Bestek-operatie is niet alleen een technologisch traject maar vooral ook een pad van cultuurverandering: bij de korpsen moet regiodenken plaatsmaken voor concerndenken en moet de bereidheid groeien om informatie te delen.

RESULTATEN ICT BESTEK 2001 - 2005

De minister van BZK heeft eind 2005 de Tweede Kamer geïnformeerd over de resultaten van de uitvoering van het Bestek 2001 – 2005 tot dusver.
Op het gebied van de infrastructuur wordt gemeld dat de zes bovenregionale rekencentra de ICT-organisatie hebben overgenomen van de korpsen en dat de landelijke netwerkinfrastructuur (Nutsvoorziening) is ontwikkeld en uitgerold. Met betrekking tot de ICT-organisatie worden gemeld dat het concerndenken zichtbaar is geworden in de doorontwikkeling van de vraag- en aanbodorganisatie en de centrale rol die deze spelen in de ICT-organisatie van de politie.
De resultaten op het gebied van uniformering van ICT-toepassingen (applicaties) zijn echter ernstig achtergebleven. Er is nog steeds sprake van verschillende toepassingen voor belangrijke werkprocessen. Een belangrijke stap vooruit is de ontsluiting van de regionale informatiesystemen voor handhaving en opsporing door middel van de invoering van het systeem Blue View. Hierdoor is het delen van informatie tussen de korpsen sterk verbeterd.

COMMISSIE LEEMHUIS

In juni 2005 verscheen het rapport van de Stuurgroep Evaluatie Politieorganisatie, 'Lokaal verankerd, nationaal versterkt'. In het rapport van de stuurgroep (ook wel de Commissie Leemhuis genoemd) wordt over ICT gesteld: 'Het is voor de Stuurgroep, ..., niet verwonderlijk dat het ICT-dossier van de politie door velen als minder gelukkig wordt gezien. In de afgelopen tien jaar is er zeker het een en ander bereikt in de stroomlijning van de ICT bij de politie, maar er is nog steeds geen sprake van een eenduidige en werkende ICT-structuur.' (pag. 90). En: 'De ontwikkelingen om te komen tot een landelijk uniforme en eenduidige informatiehuishouding voor de Nederlandse politie zijn niet verlopen in het tempo dat vooraf was uitgedacht. De operatie om de ICT van 26 onafhankelijke politiekorpsen tot één geheel te smeden is lastig gebleken.' (pag. 94). Een en ander leidt de Stuurgroep tot de volgende constatering: 'Op dit moment hebben de ontwikkelingen op het gebied van ICT en innovatie de aandacht van het topmanagement van de Nederlandse politie. Op het gebied van innovatie neemt de politie een vooraanstaande positie in. Het besef is gegroeid dat een goede doorontwikkeling hiervan van groot belang is voor de prestaties, effectiviteit en efficiency van de politie in de (nabije) toekomst. Deze effectiviteit en efficiency zouden verder kunnen worden gestimuleerd als het informatiebeheer op landelijk niveau wordt belegd, zodat een aantal bestaande organisatorische en culturele barrières kan worden beslecht.'(pag. 95).

VERLENGING INSTELLINGSPERIODE REGIERAAD ICT POLITIE

De instellingsperiode van de Regieraad ICT Politie is vlak voor 1 januari 2006 verlengd, waarbij de opheffing is gekoppeld aan de oprichting van de rechtsopvolgers van CIP en ISC en de formele ontbinding van deze coöperaties.

WENKEND PERSPECTIEF

Een werkgroep heeft in de eerste helft van 2006 in opdracht van de Raad van Hoofdcommissarissen het document 'Wenkend Perspectief, strategische visie op politieel informatiemanagement en technologie 2006-2010' opgesteld. De aanleiding van het opstellen van deze visie was het gereedkomen van een aantal voorzieningen waarmee de korpsen alle huidige regionale systemen voor handhaving en opsporing kunnen raadplegen. Met deze voorzieningen werd een belangrijke stap gezet in de verbetering van de informatie-uitwisseling tussen de korpsen. De Raad van Hoofdcommissarissen en het Korpsbeheerders Beraad hebben ingestemd met deze visie als richting en uitwerking van het Herijkte Bestek 2005-2008.

VOORZIENING TOT SAMENWERKING POLITIE NEDERLAND

Op 1 juli 2006 is de voorziening tot samenwerking Politie Nederland (vtsPN) opgericht, waarin op 1 augustus 2006 de organisaties Coöperatie Informatiemanagement Politie (CIP), de ICT Service Coöperatie voor politie, justitie en veiligheid (ISC) en het agentschap Organisatie Informatie- en communicatietechnologie OOV (ITO) van het ministerie van BZK zijn opgegaan. Ook het Nederlands Politie Instituut is opgegaan in de vtsPN. De minister van BZK heeft bij de oprichting van de vtsPN een aantal criteria gesteld op basis waarvan hij het functioneren van vtsPN zal beoordelen. Deze criteria zijn vastgelegd in het zogenaamde Referentiekader. Er is door het opgaan van de vraagorganisatie en de aanbodorganisatie in de vtsPN geen sprake meer van een strikte organisatorische scheiding van vraag en aanbod. De Regieraad is nog niet opgeheven, maar functioneert alleen nog als Raad van Toezicht voor CIP en ISC.

UITWERKING WENKEND PERSPECTIEF

De vtsPN heeft het Wenkend Perspectief geconcretiseerd in het document Hoofdlijnen van het ICT-programma voor 2007 – 2010. Het bestuur van de vtsPN heeft dit document geaccordeerd. Dit programma is onlangs verder geconcretiseerd met een jaarplan en een begroting voor 2007.

Het Stelsel voor de aanpak van de informatiebeveiliging

3

In dit hoofdstuk wordt in vogelvlucht de ontwikkeling beschreven van informatiebeveiliging bij de Nederlandse politie en de stappen die sinds 1994 zijn ondernomen om een uniform niveau van beveiliging bij de 26 korpsen te bereiken.

AANLEIDING

De ontwikkeling van de informatiebeveiliging bij de politie kent een lange ontstaansgeschiedenis en gaat terug tot het rapport van de Algemene Rekenkamer 'Computerbeveiliging van gegevens in geautomatiseerde systemen bij de ministeries (1988)'. In 1994 publiceerde het Beleidsadviescollege voor de Politiële Informatievoorziening (BPI) het Beveiligingskader politiële informatievoorziening. Het BPI heeft in 1994 geadviseerd om één beveiligingskader in te richten, dat eenduidige uitgangspunten vastlegt voor het informatiebeleid van alle partijen die betrokken zijn bij het bewerken of uitwisselen van politie-informatie. Dit werd noodzakelijk geacht vanwege de onderlinge afhankelijkheid van te treffen beveiligingsmaatregelen (het principe van de zwakste schakel) en de bovenregionale infrastructuren. Het beveiligingskader richtte zich op de formulering, planning, uitvoering en evaluatie van informatiebeveiligingsbeleid en werd op bruikbaarheid getoetst in de politieregio's Brabant-Zuid-Oost en Flevoland.

VIR EN RIP

Op basis van de overeenstemming met het politieveld over de noodzakelijke eenduidigheid van een beveiligingskader is door de ministers van BZK en van Justitie op 1 april 1997 de Regeling Informatiebeveiliging Politie (RIP) vastgesteld. De RIP legt de verantwoordelijkheid bij de korpsbeheerders om een beveiligingsbeleid te formuleren en beveiligingsplannen op te stellen. Het uitgangspunt van de RIP is dat de korpsen ieder zelf verantwoordelijk zijn voor de beveiliging van hun eigen informatievoorziening, maar dat ze de informatiebeveiliging wel zodanig inrichten dat dit gebeurt op basis van 'uniforme, gemeenschappelijke betrouwbaarheidseisen en –maatregelen'. Het is dus van groot belang dat de korpsen samenwerken bij het vormgeven van de informatiebeveiliging.
De RIP bouwt in grote lijnen voort op het Voorschrift Informatiebeveiliging Rijksdienst (VIR) van 1 januari 1995. Het VIR beschrijft de noodzaak van informatiebeveiliging voor de gehele rijksoverheid. De RIP doet dit ten aanzien van de politie. Het VIR is niet van toepassing voor de regionale politiekorpsen. De RIP (en niet het VIR) is wel van toepassing op het KLPD als agentschap van het ministerie van BZK.

De RIP verstaat onder informatiebeveiliging het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van de informatievoorziening. Hierbij zijn aspecten van Beschikbaarheid (doen de systemen het als het erop aankomt?), Exclusiviteit (is informatie voldoende afgeschermd?) en Integriteit (kloppen de gegevens?) van belang (de zogenaamde BEI-eisen).
In de (toelichting op de) RIP wordt een scala aan maatregelen genoemd die kunnen bijdragen aan een effectieve informatiebeveiliging. Genoemd worden het invullen van verantwoordelijkheden binnen het korps, het beleggen van verantwoordelijkheden bij leidinggevenden en lijnmanagers, het integreren van informatiebeveiliging in de politiële bedrijfsprocessen, het bevorderen van het beveiligingsbewustzijn bij het personeel, et cetera.

STELSEL VOOR DE AANPAK VAN DE INFORMATIEBEVEILIGING

De uitwerking van de RIP is bij ministeriële regeling door de ministers van BZK en van Justitie belegd bij het Expertisecentrum Informatiebeveiliging Nederlandse Politie (ECIB). Bij beschikking (nr. EIB97/u258) van de ministers van BZK en van Justitie werd per 1 mei 1997, voor een periode van maximaal vijf jaar het ECIB ingesteld. Het bestuur van het ECIB werd gevormd door vertegenwoordigers van de drie politieberaden (Korpsbeheerdersberaad, OM-politieberaad en de Raad van Hoofdcommissarissen) en de ministeries van BZK en van Justitie. Het Expertisecentrum heeft zorg gedragen voor een uitwerking van de regelgeving in de vorm van het Stelsel voor de Politiële Informatiebeveiliging met eenduidige uitgangspunten voor de implementatie van het informatiebeveiligingsbeleid bij de korpsen.
De uitwerkingen van het ECIB zijn voorgelegd aan c.q. goedgekeurd door de drie beraden en het bestuur van het ECIB. Het ECIB heeft op 10 april 2002 de werkzaamheden afgerond en het Stelsel (en de daarmee samenhangende producten) opgeleverd aan haar opdrachtgevers, de ministers van BZK en van Justitie. Het overzicht van de producten van het ECIB is in bijlage V bij dit rapport (op cd-rom) opgenomen.

De opdracht van het ECIB was drieledig:

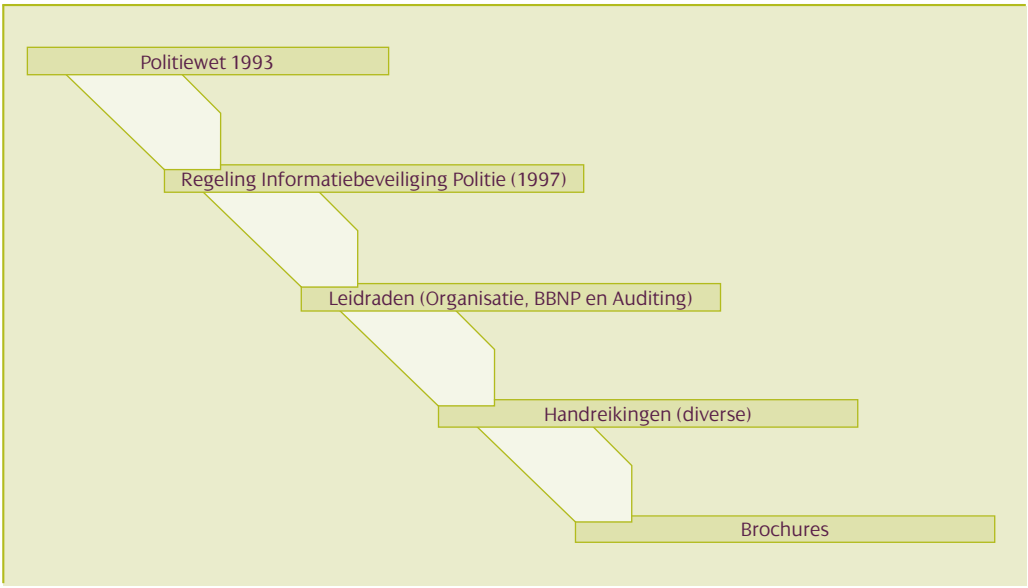
- het ontwikkelen van het Stelsel voor de aanpak van de informatiebeveiliging: een uniforme, gemeenschappelijke aanpak van informatiebeveiliging bij de politie die de gehele managementcyclus van beleid, plan, uitvoering en evaluatie dekt;
- het leveren van hulpmiddelen voor het toepassen van het Stelsel: bij het Stelsel horende methoden en instrumenten ontwikkelen gericht op de implementatie van het Stelsel;
- het scheppen van de randvoorwaarden voor de implementatie van het Stelsel: het organiseren van de noodzakelijke kwantitatieve en kwalitatieve randvoorwaarden om de implementatie van het Stelsel mogelijk te maken.

De werkzaamheden van het ECIB zijn zowel tussentijds (november 1999) als aan het eind (december 2001) geëvalueerd. In het evaluatierapport van 2001 werd door een onafhankelijk deskundige (M&I, evaluatierapport 20 december 2001) ten aanzien van het opgeleverde Stelsel en de daarbij horende methoden en instrumenten

geconcludeerd: ‘het Stelsel is, mede op basis van internationaal erkende normen en standaards, van goede (inhoudelijke) kwaliteit en door de korpsen goed toepasbaar. Tevens sluit het Stelsel goed aan bij het door de korpsen gehanteerde INK-model. Hiermee kan de ontwikkeling van het Stelsel als afgerond worden beschouwd. Er zijn door de korpsen hulporganisaties ingericht en veel van de functionarissen hebben de door het ECIB ontwikkelde opleidingen gevolgd’.

PUBLICATIES

Het Stelsel voor de aanpak van de informatiebeveiliging bestaat uit een set samenhangende publicaties in de vorm van ‘leidraden’, ‘handreikingen’, ‘brochures’ en ‘folders’. Leidraden zijn vastgesteld met instemming van de hiervoor genoemde politieberaden. Handreikingen zijn nadere uitwerkingen van de RIP of één van de leidraden. Brochures geven nadere informatie op de hiervoor genoemde publicaties of belichten een specifiek onderwerp. Het Stelsel is gebaseerd op de managementcyclus en bevat criteria, normen en instrumenten voor zowel beleid en planning als uitvoering en auditing. Daarnaast zijn in het Stelsel hulpmiddelen opgenomen gericht op de bewustwording en een opleidingprogramma ten behoeve van de functionarissen van de hulporganisatie. De samenhang in de publicaties van het Stelsel is tot stand gebracht door steeds aansluiting te zoeken bij een ‘hoger’ document te weten een wet, de RIP of een leidraad. Zo is de RIP gebaseerd op de artikelen 38, derde lid, 46 en 48, eerste lid van de Politiewet 1993. Leidraden vloeien rechtstreeks voort uit de RIP. Leidraden hebben, door de wijze waarop hiervoor bestuurlijk draagvlak is gevonden in de politieberaden, een landelijke geldigheid. Delen van leidraden zijn, voor operationele doeleinden, uitgewerkt in handreikingen en brochures.



De basisbeveiligingsmaatregelen zijn (als Leidraad) uitgewerkt in het Basisbeveiligingsniveau Nederlandse Politie (BBNP). Het BBNP is de uitwerking van de artikelen 3 en 5 van de RIP waarin vastligt dat moet worden gestreefd naar uniforme en gemeenschappelijk betrouwbaarheidseisen en -maatregelen. Naast het formuleren van informatiebeveiligingsbeleid, het inrichten van de (hulp)organisatie, het volgens een vaststaand schema auditen, is het implementeren van het BBNP een belangrijk onderdeel van het hele implementatieproces van de RIP.
Tot slot bevat het Stelsel publicaties gericht op het organiseren van de noodzakelijke kwantitatieve en kwalitatieve randvoorwaarden om de implementatie van het Stelsel mogelijk te maken. Daartoe behoort de handreiking voor het inrichten van de hulporganisatie voor de informatiebeveiliging en een compleet opleidingsprogramma voor de functionarissen van die hulporganisatie.
Bij de ontwikkeling van de publicaties en producten heeft het ECIB gebruik gemaakt van nationale en internationale standaards zoals de British Standard BS 7799s en de Code voor Informatiebeveiliging (versie 2000).

VERANTWOORDELIJKEN

De normstelling op het gebied van de informatiebeveiliging is op hoog abstractieniveau vastgelegd in de RIP en in opdracht van de beide politieministers nader uitgewerkt in het Stelsel.

De RIP is opgesteld vanuit de gedachte dat de korpsbeheerder verantwoordelijk is voor de informatiebeveiliging in zijn korps. De korpsbeheerder zorgt voor de implementatie van het Stelsel inclusief de controle erop door middel van audits. De verantwoordelijkheid voor het bewaken van de algehele voortgang bij de implementatie van de RIP en het Stelsel en daarmee van de effectiviteit van beleid en regelgeving ligt bij de minister van BZK.

De korpsen zijn zelf verantwoordelijk voor de invoering en uitvoering van het Stelsel. De Regieraad ICT, die door de minister van BZK was belast met het beheer van het door ECIB overgedragen Stelsel, heeft het beheer van het Stelsel en de ondersteuning van de korpsen bij de implementatie ervan belegd bij het Concern Informatiemanagement Politie (CIP).

HET INK-MODEL VAN DE POLITIE

De Nederlandse politie gebruikt het model van het Instituut Nederlandse Kwaliteit (INK) om periodiek de eigen bedrijfsvoering en prestaties te meten en te verbeteren. In lijn met dit INK-model wordt bij elk van de korpsen eens in de vier jaar de totaalbalans opgemaakt en verbeterpunten geformuleerd voor de volgende periode. De eerste INK-cyclus was van 1998-2001. De tweede cyclus startte in 2002 en eindigde in 2006.

In het Stelsel voor de aanpak van de informatiebeveiliging is in overeenstemming met de korpsen bepaald dat de implementatie van het informatiebeveiligingsbeleid bij de korpsen de agenda van het INK-model volgt. In het INK-model ligt vast dat het jaar voorafgaand aan het laatste jaar van een INK cyclus, het jaar is waarin de informatiebeveiliging dient te worden geaudit. Met als gevolg dat 2005 het jaar was waarin elk korps overeenkomstig artikel 6 van de RIP een audit heeft moeten uitvoeren op de implementatie van het gehele Stelsel (dat wil zeggen een onafhankelijk oordeel over de kwaliteit van de getroffen maatregelen en over het handhaven en het naleven ervan).

Nadat het Stelsel is overgedragen

4

DOEL EN OPZET

De vorige twee hoofdstukken waren vooral historisch, beschrijvend en feitelijk van aard. Dit hoofdstuk is wat meer beschouwend van opzet: er wordt ingegaan op de overdracht van het Stelsel. De nu ontstane situatie wordt kort geschetst en er wordt summier ingegaan op de actualiteit van het Stelsel voor Informatiebeveiliging.

DE OVERDRACHT IN 2002

In 2002 heeft het Expertisecentrum (ECIB) de uitwerking van de RIP in het Stelsel voor Informatiebeveiliging overgedragen aan de opdrachtgevers, de ministers van BZK en van Justitie. Deze hebben (samen met de korpsbeheerders en korpschefs) het beheer van het Stelsel in handen gegeven van de Regieraad ICT politie. Deze heeft het feitelijk beheer belegd bij het Concern Informatiemanagement Politie. De opleidingen zijn in beheer gegeven bij de Politieacademie.

Hieronder volgt een korte schets van wat er sinds 2002 met het (beheer van het) Stelsel is gebeurd en de betrokkenheid van het CIP en de Politieacademie daarbij.

CIP EN HET STELSEL VOOR INFORMATIEBEVEILIGING

Toen in 2002 het CIP het onderhoud en het beheer van het Stelsel werd toebedeeld, werd dit ondergebracht bij het onderdeel informatiebeveiliging. Bij de overgang van het Stelsel van het Expertisecentrum naar het CIP was het de bedoeling dat hiervoor vijf formatieplaatsen beschikbaar zouden zijn, drie voor het functioneel beheer en twee voor architectuur. Momenteel zijn er bij het CIP twee formatieplaatsen voor informatiebeveiliging (en beheer van het Stelsel) bezet.

ONDERZOEK NAAR KOSTEN

Bij het gereedkomen van de (concept) leidraad BBNP heeft de voorzitter van de ICT-board van de Raad van Hoofdcommissarissen aan het Expertisecentrum en het CIP in een brief (d.d. 4 januari 2002) zijn zorg geuit over de kosten van invoering van BBNP door de korpsen. ‘Ik merk op dat de invoering van de concept leidraad behoorlijke financiële en organisatorische implicaties zal hebben voor de politiekorpsen. De consequenties van deze implicaties zijn vooralsnog slechts indicatief te benoemen.

Wij hechten daarom belang aan een nader onderzoek zodat inzicht ontstaat op de werkelijke kosten en capaciteit die hiermee gemoeid zijn.' De Inspectie OOV stelt vast dat er geen onderzoek is verricht naar de kosten van implementatie van BBNP.

INITIATIEVEN EN RESULTATEN

Als onderdeel van het beheer van het Stelsel heeft het CIP de volgende initiatieven genomen:

- in 2002 is het accountmanagement voor de korpsen opgezet;
- intensief overleg met ISC, onder meer om het BBNP te verduidelijken;
- een handreiking Telewerken is gemaakt;
- er wordt momenteel gewerkt aan een rubriceringsregeling, die de status van leidraad moet krijgen;
- samen met PricewaterhouseCoopers is een nieuw Wegingsinstrument gemaakt;
- korpsen zijn geassisteerd bij het gebruik van het Wegingsinstrument;
- advies is gegeven aan de Politieacademie over opleidingen;
- binnen CIP-projecten wordt nu in een vroeg stadium de inbreng van de informatiebeveiligingsafdeling gevraagd.

De Inspectie OOV constateert op basis van de gevoerde gesprekken en de bestudeerde stukken dat het Stelsel tussen 2002 en 2006 niet actueel is gehouden.

POLITIEACADEMIE EN HET STELSEL VOOR INFORMATIEBEVEILIGING

Voorafgaand aan de overdracht van de opleidingen aan de Politieacademie zijn door het ECIB vier opleidingen verzorgd voor de functie van Informatiebeveiligingsfunctionaris (IBF-er). Deze cursussen werden verzorgd door docenten van de Politieacademie en van PricewaterhouseCoopers en waren voor de korpsen kosteloos.

In 2002 is het cursusmateriaal overgedragen aan de Politieacademie. Het betreft materiaal voor cursussen ten behoeve van IBF-ers, portefeuillehouders, taakaccenthouders en auditors. De Politieacademie kreeg de verantwoordelijkheid het cursusmateriaal actueel te houden en de cursussen aan te bieden en te verzorgen. Met de verantwoordelijkheid is niet ook een budget daarvoor overgeheveld. Het was de Politieacademie bij overdracht niet geheel duidelijk welke verantwoordelijkheden werden overgedragen. Van eventuele afspraken die destijds gemaakt zijn is niets terug te vinden. De Politieacademie kreeg de opdracht de opleiding te verzorgen conform het Stelsel.

Het cursusaanbod voor informatiebeveiliging werd ondergebracht bij het onderdeel Maatwerk van de Politieacademie. Voor de Politieacademie is de IBF-cursus, qua onderhoud, een dure cursus, omdat deze slechts eenmaal per twee jaar kan worden verzorgd. Immers, een korps heeft meestal maar één IBF-er (de grotere korpsen hebben er doorgaans meer), die de functie gemiddeld zo'n twee á drie jaar uitoefent. De Politieacademie biedt de cursus niet, zoals indertijd bij ECIB wel het geval was, kosteloos aan; het cursusgeld bedraagt 5000 euro per cursist. In 2003/2004 is door de Politieacademie een IBF-cursus verzorgd. Het minimumaantal van twaalf deelnemers werd met elf aanmeldingen niet gehaald; het CIP heeft de lege cursusplaats toen betaald. Van de elf cursisten hebben negen ook examen gedaan en zijn geslaagd. Om te stimuleren dat cursisten ook daadwerkelijk examen doen betaalt het CIP 4000 euro terug aan het korps als de kandidaat slaagt voor het examen.

Na de overdracht van de opleidingen heeft de Politieacademie alleen zogenaamd staand onderhoud gepleegd. Het volledig actueel houden van de opleiding werd door de Politieacademie als te duur en economisch niet rendabel beschouwd.

De cursus van 2003/2004 is uitgebreid geëvalueerd, omdat deze niet goed is verlopen. De cursisten gaven aan dat het materiaal verouderd was. Dit had deels te maken met het feit dat het Stelsel als zodanig gedateerd was (materiaal uit 1999), dat CIP en ISC een rol gingen spelen bij de informatiebeveiliging van de politie en dat onvoldoende aandacht was voor de gedragscomponent van informatiebeveiliging. Naar aanleiding van de evaluatie is de cursus aangepast. Ze wordt nu verzorgd en actueel gehouden door een commercieel bureau. De Politieacademie treedt op als makelaar. De opleiding wordt afgesloten met twee erkende EXIN-examens op HBO-niveau: ISF (Information Security Foundation) en ISMA (Information Security Management Advanced). De opleiding is zowel bedoeld voor IBF-ers als voor auditors en heeft een minimumaantal van zes deelnemers, waardoor de kans dat de cursus doorgaat aanzienlijk groter is. In 2006 is weer een IBF-cursus verzorgd. Ook is de doelgroep uitgebreid: Immigratie en Naturalisatiedienst (IND), ISC, Dienst Justitiële Inrichtingen (DJI) en Algemene Inlichtingen- en Veiligheidsdienst (AIVD) kunnen ook cursisten aanmelden.
De andere opleidingen (portefeuillehouder, taakaccenthouder en auditor) zijn wel aan de korpsen aangeboden, maar hier bleek nauwelijks interesse voor te zijn. De oorspronkelijke opleidingen werden eveneens met een examen afgesloten. De oorspronkelijke opleidingen gingen in op alle aspecten van het Stelsel. De huidige opleiding is in principe algemener van aard, maar wel toegespitst op de politie.

De Inspectie OOV constateert op basis van de gevoerde gesprekken en bestudeerde stukken dat de opleidingen binnen het Stelsel voor Informatiebeveiliging tussen 2002 en 2006 niet voldoende zijn onderhouden. Hierbij past echter wel de kanttekening dat de Politieacademie een lastige taak had om opleidingen te verzorgen conform het Stelsel, terwijl delen van het Stelsel niet langer actueel waren.

DE ACTUALITEIT VAN HET STELSEL VOOR INFORMATIE-BEVEILIGING

De Inspectie OOV is geïnteresseerd in de vraag naar de actualiteit van het Stelsel. Immers, ontworpen in de periode 1999 tot 2002, gecombineerd met het ontbreken van adequaat onderhoud in de jaren tussen 2002 en 2006, is de kans op veroudering groot, zeker gelet op de snelle ontwikkelingen op het gebied van ICT en de bovenregionale voorzieningen. In vrijwel alle gesprekken in het kader van het onderzoek was de actualiteit van het Stelsel een thema van belang.
De volgende vragen kwamen in de verschillende gesprekken aan de orde:

- wat heeft het Stelsel opgeleverd?
- welke relevante veranderingen zijn van invloed geweest op de actualiteit van het Stelsel?
- welke onderdelen van het Stelsel zijn op dit moment nog wel bruikbaar en welke niet meer?
- wat heeft de komst van CIP en ISC betekend voor de actualiteit van het Stelsel?
- heeft de politie een eigen Stelsel nodig of is een meer universele aanpak beter?

In het algemeen wordt de mening gedeeld dat het Stelsel in 2002 een prima instrument was om de informatiebeveiliging bij de politie te bevorderen. Het feit dat het ging om, soms tot in detail, uitgewerkte leidraden, handreikingen en maatregelen paste goed bij het toenmalige 'volwassenheidsniveau' van veel van de korpsen, waar het de informatiebeveiliging betreft. Deze nadruk op uitwerking en detail in het Stelsel wordt anno 2006 echter vaak gezien als een argument om het Stelsel in te ruilen voor een meer algemene en wat globalere systematiek voor informatiebeveiliging. Hierbij wordt dan steevast gewezen op de ontwikkeling die de korpsen hebben doorgemaakt bij het beveiligen van informatie; het huidige 'volwassenheidsniveau' van de korpsen zou een minder bedillerige aanpak van informatiebeveiliging mogelijk maken.

De Inspectie OOV constateert dat er op het terrein van de ICT bij de politie veel in beweging is. De belangrijkste recente ontwikkelingen daarbij zijn, naast technische en werkinhoudelijke ontwikkelingen, de oprichting van ISC en CIP, de overgang van veel automatiseringstaken van de regio's naar de ISC-verzorgingsgebieden, de oprichting van de voorziening tot samenwerking en het feit dat ISC en CIP daarin zijn opgegaan. De conclusie dat het Stelsel geactualiseerd dient te worden wordt binnen de politie breed onderschreven. De Inspectie OOV deelt deze mening en is van oordeel dat actualisatie van het BBNP (en mogelijk enkele andere onderdelen van het Stelsel) gewenst is en dat actuele ontwikkelingen op technisch, bestuurlijk en vakinhoudelijk (het vak informatiebeveiliging) gebied hierbij betrokken dienen te worden. Het niet langer actueel zijn van het Stelsel mag in de visie van de Inspectie OOV echter geen reden zijn om te stoppen met implementeren van het huidige Stelsel.

OPBRENGST VAN HET STELSEL

De opbrengsten van het Stelsel zijn:

- de meeste korpsen hebben hun beveiligingsorganisatie ingericht en leidinggevenden verantwoordelijk gemaakt;
- er is veel gerealiseerd op het gebied van bewustwording van het belang van informatiebeveiliging bij het personeel;
- een fors aantal informatiebeveiligingsmaatregelen is door de korpsen ingevoerd;
- er is sprake van een cultuuromslag sinds 2002;
- vooral bij de rechercheonderdelen is informatiebeveiliging goed aangeslagen;
- de deskundigheidsbevordering is groot geweest (door de (gratis) opleidingen die het ECIB verzorgde);
- er is een goed werkend netwerk van informatiebeveiligingsfunctionarissen, waardoor de regio's volop communiceren met elkaar over informatiebeveiliging; het samenwerken in de verzorgingsgebieden van ISC bevordert dit;
- standaardisatie is bevorderd door het BBNP en het Stelsel.

WAT IS NIET GELUKT?

Waar in het Stelsel is voorzien in een planmatige en complete aanpak van informatiebeveiliging, hebben veel korpsen slechts elementen uit het Stelsel ingevoerd, zonder voor een meer planmatige aanpak te kiezen. Populaire elementen waren: het inrichten van de hulporganisatie, het schrijven van een informatiebeveiligingsdocument en de deelname aan opleidingen voor de functie van informatiebeveiligingsfunctionaris. Het ontbreken van een planmatige aanpak van informatiebeveiliging is daarmee waarschijnlijk het belangrijkste faalpunt bij de implementatie van het Stelsel.
Andere zaken die minder succesvol zijn verlopen:

- de uitrol van het Stelsel is te veel overgelaten aan de werkvloer (de IBF-ers) en er is te weinig aandacht geweest voor de positie van de korpsleiding, die dit proces meer had kunnen ondersteunen; ook is de functie van portefeuillehouder niet overal goed van de grond gekomen;
- door de korpsen werd de verplichting het BBNP te implementeren als erg zwaar ervaren, gezien het grote aantal maatregelen en het detailniveau van het BBNP; bovendien is het BBNP nogal activiteitengeoriënteerd en sluit daarom steeds minder aan bij de ambitie van de politie om procesgeoriënteerd te werken;
- de samenwerking tussen korpsen op het gebied van informatiebeveiliging is nog niet voldoende van de grond gekomen;
- het beheer van het Stelsel en de opleidingen is onvoldoende geweest om het Stelsel actueel en effectief te houden.

RELEVANTE VERANDERINGEN

- Het veld en de spelers op het gebied van ICT zien er sinds 2002 heel anders uit. Toen het Stelsel werd geïntroduceerd was er sprake van 26 korpsen die zelfstandig over hun eigen informatie en automatisering gingen. Het Stelsel was gebaseerd op de verantwoordelijkheid van de korpsbeheerder voor informatiebeveiliging en voor de systemen. Momenteel vindt veel uitwisseling van informatie plaats en zijn systemen aan elkaar 'geknoopt'. Iedere korpsbeheerder is verantwoordelijk voor de informatiebeveiligingsactiviteiten die binnen zijn korps plaatsvinden. Voor de activiteiten die zijn uitbesteed (bijvoorbeeld aan vtsPN) kan de korpsbeheerder zekerheden eisen (bijvoorbeeld in de vorm van SLA's). De korpsbeheerders vormen tevens het bestuur van de vtsPN.
- Het CIP en vooral het ISC hebben een belangrijke positie ingenomen op het terrein van ICT. Veel van de uitvoerende automatiseringswerkzaamheden van de korpsen vinden plaats in de rekencentra van de ISC-verzorgingsgebieden. Voor de informatiebeveiliging betekent dit dat de meer technische beveiligingsmaatregelen door ISC worden genomen en dat de korpsen hierover met ISC afspraken moeten maken. De eigen taak van de regio's op het gebied van informatiebeveiliging verschuift daarmee steeds meer naar maatregelen op het personeel, organisatorisch en gebouwelijk vlak en de gedragsaspecten van beveiliging. Daarbij zouden korpsen wel alle aspecten van informatiebeveiliging (inclusief de beveiliging die wordt 'ingekocht' bij het ISC) in onderling verband moeten blijven zien (integrale beveiliging).
- Het delen van informatie is veel belangrijker geworden; dit geldt voor uitwisseling tussen korpsen onderling en tussen de verschillende politieprocessen (zoals handhaving, opsporing, gebiedsgebonden politiewerk via een systeem van Informatie-Gestuurde Politie), maar ook voor uitwisseling met externe partners, zoals het Openbaar Ministerie, de jeugdzorg, gemeentelijke diensten, et cetera.
- Er is veel veranderd in de informatiehuishouding van de politie, in de technologische mogelijkheden en in de kosten van automatisering.
- ICT is, nadat Bestek 2001 - 2005 niet heeft opgeleverd wat was beoogd, nu een zeer actueel onderwerp voor de Nederlandse politie. De Raad van Hoofdcommissarissen heeft intussen 'Wenkend perspectief' gepubliceerd, een nieuwe visie op ICT-ontwikkelingen bij de politie. Momenteel wordt hard gewerkt om 'Wenkend perspectief' nader uit te werken en in te voeren.
- Samenwerking tussen korpsen op allerlei vlak, ook ICT en informatiebeveiliging, is veel normaler geworden. De ISC-verzorgingsgebieden, met de regio Zuid als aansprekend voorbeeld, hebben hieraan een positieve impuls gegeven.
- De oprichting van de voorziening tot samenwerking Politie Nederland en het onderbrengen van de ICT-taken bij de voorziening.

BBNP

Het BBNP bevat een groot aantal beveiligingsmaatregelen. Het merendeel van de korpsen kan niet aantonen dat het BBNP volledig is ingevoerd (zie hoofdstuk 4). Veel korpsen vinden het BBNP overigens erg uitgebreid en gedetailleerd en bovendien nogal activiteiten-georiënteerd. Zelfs het volledig implementeren van het BBNP leidt volgens een aantal korpsen niet tot een afdoende beveiliging, omdat in 2002 niet, op maatregelniveau, kon worden geanticipeerd op ontwikkelingen in de jaren daarna; kritiek dus op de actualiteit. Het aspect van risicomanagement zou ook ontbreken in het BBNP. Een ander punt van kritiek op het BBNP is dat het niet consistent is: hier is het beveiligingsniveau te hoog, daar te laag. Overigens is het de korpsen, binnen de contouren van het Stelsel toegestaan om beredeneerd af te wijken van het BBNP.
Toch is het BBNP bedoeld als een minimum beveiligingsniveau, waar alle korpsen aan zouden moeten voldoen. Dat minimum niveau is de basis voor het onderling vertrouwen tussen korpsen, wanneer ze informatie met elkaar delen.

ROLVERDELING

ICT (en daarmee ook sommige aspecten van de informatiebeveiliging) zijn sinds 2006 georganiseerd onder de vtsPN. De individuele korpsen hebben in deze constructie betrekkelijk weinig te kiezen als 'klant'; zo wordt het althans ervaren door de korpsen. Enerzijds is dit positief omdat het landelijk leidt tot meer uniformering, waar, ook door de Inspectie OOV al geruime tijd op wordt aangedrongen. Anderzijds ontstaat de situatie dat niet de lokale omstandigheden bij de korpsen bepalend zijn voor de wijze van ICT-ondersteuning, maar dat de ICT-producten leidend zijn met als gevolg dat de korpsen hun werkprocessen daaraan moeten aanpassen.

ACTUALISEREN MAAR OOK DOORGAAN MET IMPLEMENTEREN

Dat het Stelsel niet meer op alle punten actueel is en dat er op dit punt wat moet gebeuren is duidelijk. Beantwoording van de vraag of beter gekozen kan worden voor een geheel nieuw, en mogelijk wat globaler Stelsel of dat het huidige Stelsel geactualiseerd kan worden, past niet binnen het kader van het onderhavige onderzoek. Die ontwikkeling zal gezien alle hierboven geschetste veranderingen toch wel worden ingezet. Daarbij is van belang dat zoveel mogelijk gekozen wordt voor één lijn voor de gehele Nederlandse politie en dus zo veel mogelijk wordt afgezien van regionaal maatwerk. Het niet meer 100% actueel zijn van het Stelsel mag in de visie van de Inspectie geen reden zijn om het niet te implementeren. Een korps dat het BBNP heeft ingevoerd heeft bepaald wel iets om trots op te zijn.

Implementatie van informatie-beveiliging bij de Nederlandse politie

5

In dit hoofdstuk wordt het landelijk beeld van de informatiebeveiliging bij de Nederlandse Politie per oktober 2006 geschetst. Dit is gebaseerd op de ingevulde vragenlijsten, de interviews en de bestudeerde documentatie van de 25 regiokorpsen en het KLPD. Niet in het onderzoek is betrokken de informatiebeveiliging van de technische voorzieningen welke niet in beheer van de korpsen zijn (zoals de voorzieningen aangeboden door ISC, de nutsvoorziening).

Na een algemeen beeld van de implementatie van het Stelsel voor Informatiebeveiliging zoals afgeleid van de Regeling Informatiebeveiliging Politie (RIP), zal meer gedetailleerd worden ingegaan op de onderdelen van de informatiebeveiligingsmanagementcyclus:

- Beleid
- Organisatie
- Maatregelen
- Evaluatie

Per onderdeel is de situatie beschreven zoals deze bij de 26 korpsen is aangetroffen. Tevens is per onderdeel een overzicht met daarin de score per korps opgenomen. In bijlage IV is aangegeven op welke wijze de score is bepaald.

ALGEMEEN BEELD

Het algemene beeld dat naar voren komt uit de documentatie en korpsbezoeken is dat de politie een organisatie is die actief met informatiebeveiliging bezig is. Wel blijken de politiekorpsen op het gebied van informatiebeveiliging nogal uitvoerings- en taakgerichte organisaties te zijn. Op incidenten wordt over het algemeen uiterst adequaat gereageerd. Wat echter ontbreekt, is een duidelijke planmatige en structurele aanpak van de informatiebeveiliging. En juist voor dit onderwerp is een planmatige, systematische benadering essentieel. In termen van de INK-stadia blijken de meeste korpsen zich, voor het onderwerp informatiebeveiliging, nog in de ‘activiteit georiënteerde’ fase te bevinden.

BELEID

Het niet planmatig oppakken van het onderwerp informatiebeveiliging heeft als consequentie dat op dit moment in een aantal korpsen een door de korpsbeheerder en korpsleiding geaccordeerd beleid ontbreekt. En als er al informatiebeveiligingsbeleid aanwezig is, is dit vaak verouderd en sluit niet goed meer aan op de huidige organisatie van het korps en de politieorganisatie in het algemeen. Ontwikkelingen als de over-

dracht van taken naar ISC (ICT-Service Coöperatie Politie, Justitie en Veiligheid en later de voorziening tot samenwerking Politie Nederland, vtsPN), de introductie van C2000 en een andere aanpak bij interceptie (tapkamers) zijn niet of slechts beperkt in het beleid verwerkt. Ook is in dit verband van belang de mate waarin sprake is van geïntegreerd beveiligingsbeleid (onder meer fysieke-, personele- en informatiebeveiliging).

ORGANISATIE

Niet alle korpsen hebben een informatiebeveiligingsfunctionaris die zorgt voor de coördinatie van alle informatiebeveiligingsactiviteiten. Deze functie wordt in het Stelsel als belangrijk beschouwd binnen de zogenaamde 'hulporganisatie'. Bovendien is er een opvallend verband tussen korpsen met een goed bezette informatiebeveiligingsorganisatie en de mate van succes bij het implementeren van een planmatige en structurele aanpak van informatiebeveiliging. Voorts is in dit verband van belang de functiescheiding, de verantwoordelijkheidsverdeling en het verkrijgen van zekerheid na uitbesteding.

SAMENWERKING

De afgelopen jaren zijn, mede door de inrichting van de zogenaamde ISC-verzorgingsgebieden, veel samenwerkingsverbanden ontstaan op het terrein van politiële informatievoorziening en informatiebeveiliging. Deze actieve samenwerking vindt op diverse niveaus plaats en draagt in belangrijke mate bij aan een meer consistente en professionele wijze van informatiebeveiliging bij de Nederlandse politie. Op 1 juli 2006 is de voorziening tot samenwerking Politie Nederland (vtsPN) opgericht: een publiekrechtelijk samenwerkingsverband van alle politiekorpsen, dat belast is met de realisatie van de gemeenschappelijke informatiehuishouding van de politie. In de vtsPN zijn de voormalige CIP (Concern Informatiemanagement Politie) en ISC opgegaan, alsmede de baten/lastendienst ITO en het Nederlands Politie Instituut.

MAATREGELEN

Ook op het niveau van informatiebeveiligingsmaatregelen blijken de korpsen veelal niet planmatig te werken aan de implementatie daarvan. Vaak worden maatregelen pas geïmplementeerd als dit door incidenten of door verhoogde aandacht voor informatiebeveiliging noodzakelijk blijkt. De actualiteit van de dag krijgt dan voorrang boven een structurele aanpak van het onderwerp. Belangrijke aspecten bij dit onderwerp zijn: het hebben van overzicht van de informatiesystemen mede als basis voor de beveiligingsclassificatie, A&K-analyses, incidentenregistratie en het beveiligingsbewustzijn van de medewerkers.

EVALUATIE

De evaluatiecyclus van informatiebeveiliging blijkt slechts in enkele gevallen verankerd in de brede managementcyclus en in de INK-cyclus. De evaluatie van het informatie-

beveiligingsbeleid vindt nog veel op ad hoc-basis plaats. Daarnaast maken de korpsen nog maar beperkt gebruik van audits als evaluatie-instrument. Een aantal korpsen past wel het instrument van de interne audit toe en incidenteel wordt ook aan andere korpsen gevraagd om een collegiale audit bij het eigen korps uit te voeren. Externe audits worden slechts beperkt toegepast. Het aspect evaluatie scoort over het algemeen het slechtst. Tevens is bij dit aspect van belang of de evaluaties zijn ingebed in de reguliere beleidsevaluatiecycli.

VERANTWOORDINGSINFORMATIE

Vaak kunnen korpsen wel laten zien dat ze een informatiebeveiligingsmaatregel hebben genomen, maar kunnen ze hiermee niet aantonen dat deze maatregelen ook op operationeel niveau werken. Ook ontbreekt het aan actuele vastleggingen van maatregelen en het rapporteren over het daadwerkelijk gerealiseerde beveiligingsniveau. Hierdoor is het voor het korps moeilijk om een buitenstaander (collega-korpsen of zoals in dit geval de Inspectie OOV) inzicht te geven in de stand van zaken met betrekking tot de informatiebeveiliging en daarmee van het gerealiseerde beveiligingsniveau. Het ontbreekt kortom vaak aan verantwoordingsinformatie en aan een systeem van monitoring.

Dit algemene beeld komt duidelijk terug als we de 26 korpsen naast elkaar zetten. De korpsen hebben een score gekregen op de onderdelen van informatiebeveiliging: beleid, organisatie, maatregelen en evaluatie. Hierbij is gebruik gemaakt van een vijfpuntsschaal op basis van een op de RIP gebaseerd normenkader (zie hiervoor de bijlagen). Daarbij is een 5 gegeven als geheel werd voldaan aan de norm en een 1 als niet werd voldaan aan de norm. Hierbij moet worden opgemerkt dat de in dit onderzoek gebruikte norm niet het maximaal haalbare is wat bereikt kan worden. Een score van 5 laat zich dus niet lezen als een ‘10 op het rapport’. Bij het onderdeel ‘maatregelen’ gaat het bijvoorbeeld om het ingevoerd hebben van het BBNP, hetgeen een minimumniveau van beveiliging is dat voor alle systemen en processen geldt. Als de score daar onder de 5 is, wordt zelfs dit minimumniveau niet gehaald. Tegelijkertijd is het goed mogelijk dat een korps wel een hoger niveau van beveiliging heeft voor meer kritische systemen; daarin voorziet de cijferwaardering van het op de RIP gebaseerd normenkader niet en worden in dit onderzoek daarom geen uitspraken gedaan.

Op de vier onderdelen wordt voor alle 26 korpsen gezamenlijk als volgt gescoord:

Tabel 1 Score van de 26 korpsen (op vijfpuntsschaal) per onderwerp

Onderdeel	Score
Beleid	3,24
Organisatie	3,79
Maatregelen	3,13
Evaluatie	2,45
Totaal (gemiddelde van de scores)	3,16

Over het algemeen wordt een score, iets boven het gemiddelde behaald. Op het onderdeel organisatie wordt de hoogste score aangetroffen. Dit valt te verklaren uit het feit dat de meeste korpsen de functies die met informatiebeveiliging te maken hebben, hebben benoemd of beschreven en dat op die functies ook functionarissen zijn aangesteld. De lagere score op het onderdeel maatregelen is met name te verklaren doordat bijna geen enkel korps kan aantonen dat daar het BBNP is geïmplementeerd of binnenkort zal zijn geïmplementeerd. Daarnaast zijn bij een beperkt aantal korpsen Afhankelijkheids- & Kwetsbaarheidsanalyses uitgevoerd. Zoals al eerder aangegeven, is het onderdeel evaluatie slecht ontwikkeld binnen de korpsen. Dit is dan ook waarneembaar in een beduidend lagere score op dit onderdeel.

De totaalscore maar nu per korps geeft het volgende beeld:

Tabel 2 Score per korps (op vijfpuntsschaal) alle onderwerpen bij elkaar genomen

Rang	Korpsnaam	Score
1	Amsterdam-Amstelland	4,10
2	Noord- en Oost-Gelderland	4,07
3	IJsselland	3,70
4	Rotterdam-Rijnmond	3,65
5	Brabant-Zuid-Oost	3,54
6	Zaanstreek-Waterland	3,49
7	Groningen	3,48
8	Kennemerland	3,45
9	KLPD	3,44
10	Noord-Holland Noord	3,39
11	Haaglanden	3,32
12	Midden- en West-Brabant	3,20
13	Fryslân	3,17
14	Zuid-Holland-Zuid	3,16
15	Flevoland	3,13
16	Brabant-Noord	3,10
17	Hollands Midden	3,03
18	Twente	2,96
19	Drenthe	2,86
20	Zeeland	2,85
21	Gelderland-Zuid	2,69
22	Utrecht	2,63
23	Limburg-Noord	2,58
24	Gelderland-Midden	2,55
25	Limburg-Zuid	2,50
26	Gooi en Vechtstreek	2,02
	Totaal	3,16

ALGEMEEN BEELD C2000

C2000 communicatie loopt via de (regionale) meldkamers. De inrichting van deze meldkamers is divers en varieert van het delen van huisvesting van politie met brandweer en ambulance tot geheel geïntegreerd ingerichte multidisciplinaire meldkamer-

processen. Ook de organisatorische ophanging van de (multidisciplinaire) meldkamer varieert. Op basis van de door de korpsen verstrekte informatie over C2000-verantwoordelijkheid heeft de Inspectie de indruk dat de korpsen C2000 veelal puur zien als een zaak voor de meldkamer. Op basis van het huidige onderzoek zijn de verantwoordelijkheden ten aanzien van randapparatuur beperkt in beeld te brengen, evenals de verantwoordelijkheden ten aanzien van gelieerde organisaties. Hierdoor heeft de Inspectie een onvolledig beeld van wat wel en wat niet door de korpsen is opgepakt als onderdeel van het totale C2000-beveiligingsproces.
De afgelopen twee jaar zijn alle korpsen overgegaan op C2000. Sommige korpsen zijn nog bezig met afrondende implementatieactiviteiten. Maatregelen voor een betrouwbaar C2000 liggen deels bij de gebruikers. De korpsen hebben de invoering van C2000 – beveiliging en ingebruikname - over het algemeen als een geïsoleerd project uitgevoerd. Beveiligingsmaatregelen zijn verwoord in (multidisciplinaire) C2000-beveiligingsplannen. De Inspectie heeft geen duidelijke relatie aangetroffen van deze plannen met een overkoepelend beveiligingsbeleid. Daardoor blijft C2000 een geïsoleerd onderwerp. De Inspectie heeft geen aanwijzingen gevonden voor overdracht van C2000-beveiligingsplannen aan Informatiebeveiligingsfunctionarissen. Daardoor rijst de vraag wie C2000 in het kader van interne beheersing belast is met de vereiste periodieke bijstelling van beveiligingsplannen en de daaraan gerelateerde rapportage-activiteiten.

Maatregelen voor een betrouwbaar C2000 liggen voor een deel bij directie Mobiele Diensten, de centrale beheerder van de C2000-infrastructuur. Van de 26 korpsen spreekt slechts één korps van een dienstenovereenkomst met directie Mobiele Diensten. Afspraken over beveiligingsmaatregelen maken in het algemeen onderdeel uit van een dienstenovereenkomst. De Inspectie heeft beperkt zicht óf en hoe de korpsen het dienstenniveaubeheer met directie Mobiele Diensten hebben ingericht - inclusief toets op naleving. De Inspectie zal in 2007 twee verdiepingsonderzoeken uitvoeren in het kader van C2000. Een onderzoek richt zich op de vereiste beveiligingsplannen en rapportages bij de openbare orde en veiligheidsdiensten en bij de centrale beheerder C2000-infrastructuur. Het tweede onderzoek richt zich op beveiligd gebruik, opslag, programmering (inclusief encryptie) en registratie van randapparatuur.

In de volgende alinea's wordt het algemene, landelijke beeld verder uitgewerkt in de onderdelen beleid, organisatie, maatregelen en evaluatie.

BELEID

Bij dit onderdeel is getoetst of het beleid voldoet aan de daaraan gestelde eisen in de RIP. Over het algemeen kan worden gesteld dat de meeste beleidsdocumenten voldoen aan de RIP en de noodzakelijke elementen bevatten. Negentien van de 26 korpsen hebben een vastgesteld beleid. Bij acht daarvan is dit het afgelopen jaar nog geactualiseerd. Twee korpsen hebben in het geheel geen beleidsdocument en de overige korpsen hebben een beleidsdocument met een conceptstatus.

Mede ingegeven door de vorming van de ISC-verzorgingsgebieden ontstaan veel nieuwe vormen van samenwerking en overleg. Binnen elk verzorgingsgebied blijken op diverse niveaus (korpsleiding, CIO's, service liaisons en informatiebeveiligingsfunctionarissen) aspecten van informatiebeveiliging te worden besproken. In de zuidelijke zes regio's (Zeeland en de regio's in Brabant en Limburg) heeft dit zelfs geleid tot diverse concrete plannen en adviezen met betrekking tot informatiebeveiliging, die via het CIO-beraad en het beraad van plaatsvervangend korpschefs, hebben geleid tot concrete eenduidige regels voor alle zes korpsen. Dit bevordert het bundelen van kennis en een consistente aanpak van informatiebeveiliging binnen de samenwerkende korpsen. Dat dit niet onmiddellijk bij alle korpsen leidt tot een hoge score is ook zichtbaar in de tabel: de korpsen in Zeeland en Limburg blijven wat achter bij de korpsen in Brabant.

Visie op informatiebeveiliging in Twente.
Om de bewustwording op het gebied van informatiebeveiliging bij het lijnmanagement en de medewerkers te verbeteren is de controle op het internetgebruik belegd bij de bureau- en afdelingschefs. Zij krijgen maandelijks een overzicht met het internetgebruik van de medewerkers van hun afdelingen. Op deze wijze kunnen zij buitensporig internetgebruik detecteren. Vervolgens kunnen ze indien nodig maatregelen nemen. Op deze wijze worden zij expliciet gewezen op de verantwoordelijkheid die zij hebben voor het internetgebruik door hun medewerkers.

Dit is een voorbeeld van de visie die binnen het korps is geformuleerd over informatiebeveiliging. Deze visie is eerder ontwikkeld door een aantal IBF-ers in Nederland en gaat over de richting van informatiebeveiliging[5]. De visie stelt dat informatiebeveiliging moet zijn gericht op de mensen die ongewenst gedrag vertonen en incidenten veroorzaken. Deze medewerkers vormen in de regel maar een paar procent van alle medewerkers. Het overgrote deel van de medewerkers doet alles goed en heeft geen gerichte aandacht nodig.

VEROUDERDE BELEIDSDOCUMENTEN

Opvallend is dat veel van de – niet-actuele en concept – beleidsdocumenten eind van de jaren negentig zijn opgesteld. Naar aanleiding van de RIP en de introductie van het Stelsel voor Informatiebeveiliging zijn de – veelal nieuw aangestelde – informatiebeveiligingsfunctionarissen aan de slag gegaan met het opstellen van het informatiebeveiligingsbeleid. Zoals nu wordt geconstateerd, zijn deze initiële beleidsdocumenten in die gevallen nooit geformaliseerd en vaak ook niet actueel gehouden.
Dit is te meer opmerkelijk omdat door het ontstaan van het CIP en de ISC, en meer recent het opgaan daarvan in de voorziening tot samenwerking Politie Nederland, de uitvoering van de geautomatiseerde gegevensverwerking is gewijzigd. Deze wijziging in de uitvoering van de geautomatiseerde gegevensverwerking heeft uiteraard gevolgen voor het beleid en de organisatie van informatiebeveiliging van de korpsen. Weliswaar blijven de korpsbeheerders integraal verantwoordelijk voor alle aspecten van informatie-

5 Grip op Betrouwbaarheid, Een nieuwe visie op informatiebeveiliging, G. Alberts (NOG), B. Dodde (CIP), R. Klein Obbink (CIP, Redactie), W. Kroeze (TWN), G. van Rheenen (UTR), 5 maart 2004.

beveiliging, door het instellen van de vtsPN is de manier waarop invulling wordt gegeven aan die verantwoordelijkheid (door outscourcing en de mogelijkheid om zekerheden te verkrijgen door middel van SLA's) wel veranderd. Actualisering van het beleid en de beleidsdocumenten zou alleen al om deze reden voor de hand liggen. Daarnaast hebben zich nog twee belangrijke ontwikkelingen voorgedaan betreffende informatiebeveiliging: de 'normstelling inrichting interceptiefaciliteiten' en het 'beveiligingsbeleid C2000', die eveneens actualisering van het beleid noodzakelijk maken.

GEÏNTEGREERD BEVEILIGINGSBELEID

Het hebben van een actueel beleidsdocument is van belang omdat beleid het begin en de basis vormt voor de gehele managementcyclus voor informatiebeveiliging. Het niet hebben van zo'n document kan ertoe leiden dat informatiebeveiligingsinitiatieven niet conform een eenduidig beleid worden uitgevoerd en dat het gewenste niveau van beveiliging niet wordt gerealiseerd.
Slechts een beperkt aantal korpsen heeft een geïntegreerd beveiligingsbeleid waarbij de fysieke (o.m. aan het gebouw) en personele aspecten van beveiliging en informatiebeveiliging zijn samengebracht onder een totaal samenhangend beveiligingsbeleid. Door deze integratie kunnen initiatieven op het gebied van beveiliging beter op elkaar worden afgestemd, waardoor effectieve en efficiënte beveiligingsmaatregelen kunnen worden geïmplementeerd.

De korpsen hebben een score gekregen op een vijfpuntsschaal voor informatiebeveiligingsbeleid. Daarbij zijn de aanwezigheid van een actueel en vastgesteld beleidsdocument evenals de integratie van het interceptie- en C2000-beleid in het beleidsdocument in de score meegenomen. Hieruit ontstaat het beeld per korps op het onderdeel beleid zoals weergegeven in tabel 3:

Tabel 3 Score per korps (op vijfpuntsschaal) op het onderwerp beleid

Rang	Korpsnaam	Score	Rang	Korpsnaam	Score
1	Noord- en Oost-Gelderland	4,33	5	Kennemerland	3,00
	Zaanstreek-Waterland	4,33		Rotterdam-Rijnmond	3,00
	Amsterdam-Amstelland	4,33		Zeeland	3,00
2	Fryslân	4,00		Flevoland	3,00
3	Groningen	3,67	6	Drenthe	2,67
	IJsselland	3,67		Gelderland-Midden	2,67
	Noord-Holland Noord	3,67		Utrecht	2,67
	Zuid-Holland-Zuid	3,67	7	Gelderland-Zuid	2,33
	KLPD	3,67		Limburg-Noord	2,33
4	Twente	3,33	8	Gooi en Vechtstreek	1,00
	Haaglanden	3,33		Gemiddeld	3,24
	Hollands Midden	3,33			
	Midden- en West-Brabant	3,33			
	Brabant-Noord	3,33			
	Brabant-Zuid-Oost	3,33			
	Limburg-Zuid	3,33			

ORGANISATIE

Als onderdeel van het Stelsel is de handreiking 'Hulporganisatie voor informatiebeveiliging' gepubliceerd. Deze hulporganisatie had ten doel de politiekorpsen te ondersteunen bij het implementeren van het Stelsel. Als onderdeel van de hulporganisatie werden de volgende functionarissen benoemd:

- de portefeuillehouder Informatiebeveiliging;
- de informatiebeveiligingsfunctionaris;
- de taakaccenthouder informatiebeveiliging;
- de auditor Informatiebeveiliging.

De IB-gerelateerde overlegvormen van de zuidelijke regio's.

De zes zuidelijke regio's werken intensief samen op het gebied van informatiebeveiliging. Op diverse niveaus wordt op regelmatige basis overlegt over bedrijfsvoeringvraagstukken, waar informatiebeveiliging een onderdeel van is. De informatiebeveiligingsfunctionarissen van de zes zuidelijke regio's overleggen regelmatig over informatiebeveiligingsaspecten. Bij dit overleg zit de CIO die informatiebeveiliging in zijn portefeuille heeft. Tevens zijn de IBF-ers van het ISC verzorgingsgebied Zuid en een vertegenwoordiger van het CIP bij dit overleg aanwezig. De activiteiten van dit IBF-overleg vindt plaats op basis van een meerjarenplan voor 2006-2008. In het kader van dit plan worden door werkgroepen van het IBF-overleg beleids- en adviesproducten vervaardigd. Voorbeelden hiervan zijn de Adviesnota gebruik Multifunctionele apparatuur, het Autorisatiebeleid Zuid-Nederland en het Beleid draagbare (elektronische) media. Deze producten worden vervolgens ingebracht in het CIO-overleg van de zuidelijke zes regio's. Vervolgens worden producten na goedkeuring door de CIO's ingebracht in het zogenaamde 'Board VIP overleg' (Veiligheid en Informatie Politie). In dit overleg zijn de plaatsvervangend korpschefs van de zes zuidelijke regio's vertegenwoordigd. Na accordering van producten in dit overleg zijn het in feite officiële beleidsstukken voor alle zes zuidelijke regio's geworden. Op deze wijze worden veel in gemeenschappelijk zuidelijk verband ontwikkelde beleidsproducten tot beleid voor alle zes zuidelijke korpsen en ontstaat een consistente wijze van omgaan met informatiebeveiligingsbeleid en maatregelen. Het IBF-overleg evalueert regelmatig haar activiteiten.

ADEQUATE BEVEILIGINGSORGANISATIE

In dit verband constateert de Inspectie dat de meeste korpsen een adequate informatiebeveiligingsorganisatie hebben geïmplementeerd. Zeven korpsen hebben een goed ontwikkelde hulporganisatie met een portefeuillehouder, een informatiebeveiligingsfunctionaris en taakaccenthouders voor informatiebeveiliging in de lijn. Bij vijf korpsen is geen informatiebeveiligingsfunctionaris aanwezig of is deze gedurende lange tijd niet aanwezig geweest. De meeste korpsen hebben in ieder geval een informatiebeveiligingsfunctionaris die is belast met de coördinatie van de informatiebeveiliging. Het korps IJsselland heeft aangegeven geen hulporganisatie meer nodig te hebben, omdat informatiebeveiliging volgens de leiding voldoende is ingebed in de organisatie.

PERSONEEL

Hoewel dit onderzoek niet ten doel had na te gaan hoeveel fte's noodzakelijk zijn voor een goed functionerende informatiebeveiligingsorganisatie, kan wel worden geconstateerd dat de meeste korpsen die relatief goed presteren op het gebied van informatiebeveiliging, vaak één of meer fte beschikbaar hebben voor informatiebeveiliging. Ook hebben deze korpsen vaak betrokken taakaccenthouders Informatiebeveiliging in de lijn. Korpsen die geen informatiebeveiligingsfunctionaris hebben, of er langere tijd geen gehad hebben, presteren over het algemeen minder goed op het gebied van informatiebeveiliging.

Werkende hulporganisatie Noord- en Oost-Gelderland.
Sinds eind 2003 functioneert binnen het korps Noord- en Oost-Gelderland een taakaccenthoudersplatform. Iedere taakaccenthouder informatiebeveiliging (TIB) heeft een adviesrelatie met zijn/haar lijnchef. Dit platform komt een keer per twee maanden bijeen. De onderwerpen die ter vergadering behandeld worden hebben te maken met planning en evaluatie van beveiligingsmaatregelen. Deze taakaccenthouders werken binnen hun team aan de coördinatie van de informatiebeveiligingsactiviteiten. Zo zijn per team informatiebeveiligingsplannen geschreven om de implementatie van het BBNP te realiseren. Verder worden er door de taakaccenthouders regelmatig zelfevaluaties uitgevoerd op de implementatie van het BBNP, welke resulteren in adviesrapporten aan de teamchefs ter verbetering van de informatiebeveiligingsmaatregelen. Binnen de organisatie zijn eisen gesteld met betrekking tot de taakaccenthouders en er is overleg met een opleidingsinstantie om hieraan invulling te geven. Door dit actieve taakaccenthoudersplatform wordt op een effectieve en efficiënte wijze gerealiseerd dat de implementatie van het BBNP zoveel mogelijk in de lijn wordt opgepakt en uitgevoerd.

FUNCTIESCHEIDING

Met betrekking tot de functiescheiding op de Infodesk en binnen de interceptieorganisatie komt een divers beeld naar voren. Allereerst is te constateren dat het voor kleinere korpsen lastiger is om in voldoende mate functiescheiding te realiseren. Ook constateert de Inspectie dat er grote verschillen zijn in de mate waarin is vastgelegd (in plannen, procedures en werkinstructies) op welke wijze invulling is gegeven aan de functiescheiding binnen de Infodesk en interceptieorganisatie. Over het algemeen kan worden gesteld dat de functiescheiding bij de meeste korpsen adequaat is geregeld.

TAKEN, VERANTWOORDELIJKHEDEN EN BEVOEGDHEDEN EN C2000

Naast een specifieke verantwoordelijkheid van de minister van BZK maakt het beveiligingsbeleid C2000 onderscheid tussen de beheerder van de technische infrastructuur en gebruikers van die infrastructuur - waaronder de politiekorpsen. Bij de gebruikers

berust het zogenoemde Lokaal Beheer[6] dat zowel betrekking heeft op meldkamers als op randapparatuur. Beheerder en gebruikers zijn ketenpartners en dragen samen met derden[7] zorg voor een betrouwbaar communicatiesysteem.
Op algemeen bestuurlijk niveau zijn de korpsbeheerders van de regionale politiekorpsen verantwoordelijk voor de uitvoering van het Beveiligingsbeleid C2000. Zij dragen het Beveiligingsbeleid C2000 binnen hun organisatie uit en dienen hiertoe beveiligingsplannen op te stellen. Daarnaast heeft de politie een bijzondere verantwoordelijkheid voor de door haar aangevraagde en door het ministerie toegelaten gelieerde organisaties[8]. Tevens is de politie verantwoordelijk voor het opstellen van een calamiteitenplan voor de (eigen) operationele processen voor het kunnen omgaan met ernstige verstoringen van C2000. Op operationeel niveau vloeien de verantwoordelijkheden voort uit het voor het korps opgestelde (multidisciplinaire) beveiligingsplan.

De ingebruikname van C2000 is een regionale verantwoordelijkheid. Hiertoe zijn destijds regionale (multidisciplinaire) projecten opgestart. Vijf korpsen spreken van een nog lopende implementatie. De Inspectie heeft de indruk dat - los van de bekende lopende projecten - een aantal andere regionale projecten nog niet formeel is afgesloten, waardoor overdracht naar de lijn nog moet plaatsvinden alsmede de inbedding binnen de reguliere planning en controlcyclus.

De korpsen geven verschillend antwoord op de vraag naar de verantwoordelijke functionaris voor de beveiliging van C2000. Vier korpsen beperken zich tot een verwijzing naar het beveiligingsplan. Acht korpsen hebben de verantwoordelijke functionaris voor informatiebeveiliging van C2000 bij de meldkamer ondergebracht. Een mogelijke verklaring hiervoor is dat voor de korpsen C2000 in eerste instantie alleen voelbaar werd in de (gemeenschappelijke) meldkamer. Immers, bij de bouw van het digitale netwerk waren er diverse technische voorzieningen binnen de meldkamer nodig. Bovendien moesten alle meldkamers een acceptatie procedure doorlopen voor aansluiting op het C2000-netwerk. Na dit voorwerk kon randapparatuur in de districten in gebruik worden genomen en werd C2000 dagelijkse praktijk. De Inspectie heeft beperkt zicht op de wijze van invulling van (lijn)verantwoordelijkheden met betrekking tot decentrale registratie van randapparatuur en incidenten, fysieke beveiliging, programmering (inclusief encryptie) en toets op naleving van het beveiligingsplan door gelieerden. Daarop richtte dit onderzoek zich niet primair.

Beveiliging C2000 wordt door de korpsen over het algemeen als geïsoleerde activiteit ingevuld. Geen van de korpsen noemt een relatie tussen C2000 en de informatiebeveiligingsfunctionaris of de beveiligingsfunctionaris. In het landelijke beveiligingsbeleid vervult de IBF-er een belangrijke rol. Naast controle[9] op de implementatie van

6 Lokaal Beheer omvat functioneel beheer, technisch beheer en beveiligingsbeheer
7 Toeleveranciers, onderhoudsorganisaties, inbouworganisaties
8 Gelieerdenbeleid
9 Door de beveiligingsfunctionaris van de gebruikersorganisatie namens de verantwoordelijke van de gebruikersorganisatie

het beveiligingsbeleid dient conform dat beleid de controle op de implementatie van beveiligingsmaatregelen (conform Beveiligingsplan) te worden uitgevoerd door de informatiebeveiligingsfunctionaris[10].

ZEKERHEID NA UITBESTEDING

Als gevolg van de uitbesteding van de automatiseringsorganisaties van de korpsen naar de verzorgingsgebieden van het ISC, valt het daadwerkelijk treffen van maatregelen (binnen de kaders van het BBNP) die te maken hebben met de automatiserings-organisatie nu voor een groot gedeelte onder de verzorgingsgebieden van het ISC. Conform de RIP dienen de korpsen met het ISC en andere politiekorpsen schriftelijke afspraken te maken over de informatiebeveiligingsnormen op basis van de in de RIP-bijlage genoemde criteria en bijbehorende normklassen en over de betrouwbaar-heid van informatiesystemen plus informatie en de wijze waarop hierover zekerheid wordt verkregen (realisatie).
Bijna alle korpsen hebben een Service Level Agreement (SLA) met ISC waarin de afspraken betreffende de uitbesteding zijn vastgelegd. Deze afspraken zijn dan nader uitgewerkt in een Dossier Afspraken en Procedures (DAP). De verzorgingsgebieden van het ISC hebben verder een Producten en Diensten Catalogus (PDC) waarin de (standaard) diensten zijn beschreven. Eén korps heeft nog geen SLA, maar al wel een DAP.

SLA EN AUDITS

Niet in alle SLA's is de mogelijkheid opgenomen om een audit uit te voeren op het verzorgingsgebied, waardoor lang niet overal (onafhankelijke) zekerheid kan worden verkregen over de feitelijke betrouwbaarheid van de informatiesystemen. Twee korpsen, Twente en Amsterdam-Amstelland, hebben nadere expliciete afspraken gemaakt op het gebied van betrouwbaarheidsniveaus en de beveiliging van informatiesystemen door hun verzorgingsgebied van ISC; ook het KLPD is hier druk mee doende. De stand van zaken met betrekking tot de informatiebeveiliging bij het ISC maakte overigens geen deel uit van het onderzoek.
De korpsen hebben een score gekregen op een vijfpuntsschaal voor de informatie-beveiligingsorganisatie. Daarbij is vastgesteld of er een adequate informatiebeveiligings-organisatie binnen de korpsen is geïmplementeerd, of er voldoende functiescheiding is geïmplementeerd op de Infodesk en interceptieorganisatie en of voldoende afspraken zijn gemaakt met interne en externe partijen. Hieruit ontstaat het volgende beeld per korps op het onderdeel organisatie in tabel 4:

Tabel 4	Score per korps (op vijfpuntsschaal) op het onderwerp organisatie				
Rang	Korpsnaam	Score	Rang	Korpsnaam	Score
1	Groningen	4,60	5	Fryslân	3,60
	Rotterdam-Rijnmond	4,60		Drenthe	3,60
2	Amsterdam-Amstelland	4,40		Gelderland-Midden	3,60
	Brabant-Noord	4,40		Gelderland-Zuid	3,60
	Brabant-Zuid-Oost	4,40		Haaglanden	3,60
3	IJsselland	4,20		Flevoland	3,60
	Noord- en Oost-Gelderland	4,20		KLPD	3,60
	Hollands Midden	4,20	6	Zeeland	3,40
4	Noord-Holland Noord	3,80	7	Utrecht	3,20
	Zaanstreek-Waterland	3,80	8	Twente	3,00
	Kennemerland	3,80		Gooi en Vechtstreek	3,00
	Zuid-Holland-Zuid	3,80		Limburg-Zuid	3,00
	Midden- en West-Brabant	3,80		Gemiddeld	3,79
	Limburg-Noord	3,80			

MAATREGELEN

Bij dit onderdeel is getoetst of de volgende maatregelen van het Stelsel zijn geïmplementeerd:

- het beheren van een overzicht van informatiesystemen en hun eigenaren;
- het hanteren van beveiligingsclassificaties;
- de status en planning van het implementeren van het BBNP;
- het uitvoeren van A&K-analyses;
- het treffen van maatregelen om te voldoen aan de Normstelling Inrichting Interceptiefaciliteiten;
- het melden, registreren en afhandelen van beveiligingsincidenten;
- het bevorderen van beveiligingsbewustwording van medewerkers.

Praktische aanpak van risicoanalyse en audits in IJsselland

Door het korps IJsselland is een aanpak voor risicoanalyses ontwikkeld die is gebaseerd op een A&K-analyse maar eenvoudiger van opzet is. Met deze aanpak streeft men na om het 'onbewust lopen van risico's' om te zetten in het 'bewust nemen van risico's'. Op een divers aantal items (integraal, zowel IB als fysiek) zijn risicoanalyses uitgevoerd en zijn maatregelen geïmplementeerd. De analyses bestaan uit de volgende componenten:

- Samenvatting inhoud;
- Motivatie (aanleiding/reden);
- Effecten personeel/financieel (voor- en nadelen);
- Maatregel;
- Beslispunten;
- Intern adviestraject.

Bij de uitvoering van de analyses wordt rekening gehouden met relevante wet- en regelgeving (RIP, BBNP, et cetera). Op deze wijze wordt een praktisch toepasbare methode gehanteerd om snel te kunnen bepalen of een object adequaat is beveiligd en/of aanvullende maatregelen nodig zijn. Naast deze methode voor risicoanalyse heeft het korps een quick-scan ontwikkeld om periodiek de implementatie van het BBNP te kunnen toetsen . Deze quick-scan wordt eens in de twee jaar uitgevoerd en levert managementinformatie op over in hoeverre maatregelen van het BBNP zijn geïmplementeerd.

CLASSIFICATIE

Bijna alle korpsen beschikken over een beheerd overzicht van informatiesystemen waaraan ook eigenaren zijn toegewezen. Eén korps gaf aan geen eigenaren te hebben toegewezen. Negen korpsen gaven aan dat eigenaren aan informatiesystemen waren toegewezen, maar dat dit (nog) niet expliciet was vastgelegd (Veel korpsen blijken geen officiële classificatie voor bepalen van het beveiligingsniveau) voor informatie-(systemen) te hanteren. Momenteel wordt door een landelijke werkgroep gewerkt aan een landelijke classificatie voor informatie. Bij een groot aantal korpsen wordt voor de classificatie van informatiesystemen gewerkt met de landelijke normklassen uit de bijlage van de RIP.

Informatiebeveiligingsbewustwording in Amsterdam-Amstelland

In het Informatiebeveiligingsbeleid van het korps Amsterdam-Amstelland is door middel van aparte blokken tekst relevante informatie opgenomen met betrekking tot informatiebeveiliging. Dit betreft wetenswaardigheden met betrekking tot risico's welke gelopen worden, ontwikkelingen met betrekking tot informatiebeveiliging, nieuwsberichten met betrekking tot informatiebeveiliging en kosten van gebrekkige informatiebeveiliging. Deze extra informatie maakt het Informatiebeveiligingsbeleid goed leesbaar en tevens leuk om te lezen.

De campagne van Amsterdam-Amstelland 'Weet wat je Weet' brengt op een sympathieke manier informatiebeveiliging onder de aandacht van de medewerkers. De campagne 'Weet wat je Weet' is gericht op bewustwording van de medewerkers en is opgezet in zogenaamde flights, bijvoorbeeld:

1. Weet wat je ZEGT
2. Weet wat je DOET
3. Weet wat je VRAAGT
4. Weet wat je ZOEKT

Deze thema's worden door middel van verschillend promotiemateriaal onder de aandacht van de medewerkers gebracht. De totale campagne duurt drie jaar, waarbij de drie eerste flights al uitgerold zijn. Daarna wordt gestart met het opzetten van de concepten voor het onderdeel ZOEKT. Door toetsing/audit na elke flight wordt ook duidelijk wat het resultaat is van de desbetreffende flight en op basis hiervan kan de campagne eventueel worden bijgestuurd.

IMPLEMENTATIE BBNP

Slechts acht korpsen kunnen aantonen dat zij het BBNP grotendeels of geheel hebben geïmplementeerd, of binnenkort zullen implementeren op basis van een actueel informatiebeveiligingsplan. Bij negen korpsen is de status van de implementatie van het BBNP onbekend omdat de implementatie niet planmatig ter hand wordt genomen of omdat de status niet kan worden aangetoond door middel van een interne of externe audit.

De Inspectie acht dit zorgelijk, zeker gezien het feit dat de korpsen hebben toegezegd om per 2005 het BBNP te implementeren en hierop een audit uit te (laten) voeren. Bijna alle korpsen geven bovendien aan dat een letterlijke implementatie van de maatregelen in het BBNP niet mogelijk en ook niet gewenst is. Men vindt het BBNP te gedetailleerd

en treft daarom waar mogelijk vervangende en compenserende maatregelen. Zo heeft het korps Amsterdam-Amstelland een eigen baseline ontwikkeld die is afgeleid van het BBNP.

AFHANKELIJKHEIDS- & KWETSBAARHEIDSANALYSE

Slechts een beperkt aantal korpsen heeft Afhankelijkheids- en Kwetsbaarheidsanalyses (A&K-analyses) uitgevoerd om het gewenste beveiligingsniveau voor een informatiesysteem vast te stellen. Vijf korpsen hebben A&K-analyses uitgevoerd voor kritische informatiesystemen, zoals RBS of andere recherche-informatiesystemen. Enkele korpsen, zoals IJsselland, gebruiken een eenvoudiger – van de A&K-analyse afgeleide – methode om risicoanalyses uit te voeren. Op enkele uitzonderingen na blijkt het gebruik van A&K-analyses of andere methodes voor risicoanalyse geen gewoongoed te zijn in de politieorganisaties.
De Inspectie acht dit zorgelijk, aangezien de korpsen zo onvoldoende inzicht hebben in de noodzakelijke gewenste mate van beveiliging om deze te vergelijken met het daadwerkelijk gerealiseerde niveau van beveiliging. Daarmee worden mogelijk informatiebeveiligingsrisico's gelopen die niet zichtbaar zijn voor de politiekorpsen.

MELDING VAN INCIDENTEN

Zestien korpsen hebben een beschreven procedure met betrekking tot de melding, registratie en afhandeling van beveiligingsincidenten. De meeste korpsen hebben echter alleen een beschrijving van het beleid ten aanzien van het melden, registreren en afhandelen van incidenten opgenomen in het beleidsdocument. Een groot aantal korpsen heeft daarmee geen adequaat uitgewerkte procedure voor het melden, registreren en afhandelen van informatiebeveiligingsincidenten. Dit uit zich bij veel korpsen in het niet of slechts beperkt registreren van informatiebeveiligingsincidenten. Verder bestaat er slechts in enkele gevallen een geïntegreerde registratie van informatiebeveiligingsincidenten; in de meeste gevallen zijn er meerdere registraties, bijvoorbeeld bij de informatiebeveiligingsfunctionaris, bij een bureau integriteit en bij de facilitaire dienst. Dit heeft consequenties voor (de volledigheid van) het beeld dat de korpsleiding zich kan vormen betreffende het optreden van inbreuken op de (informatie)beveiliging. Daarnaast zijn incidenten een goede indicatie voor de werking van informatiebeveiligingsmaatregelen en daarmee een nuttig instrument voor de evaluatie van informatiebeveiligingsbeleid en –maatregelen. Dit wordt nog te weinig als zodanig onderkend.

Kennemerland: nieuwsbrief informatiebeveiliging
De informatiebeveiligingsfunctionaris van Kennemerland stelt maandelijkse een nieuwsbrief samen met daarin nieuwsberichten op het gebied van informatiebeveiliging uit een groot aantal bronnen. Deze nieuwsbrief wordt per e-mail verspreid naar geïnteresseerden, die daardoor op de hoogte blijven van relevante ontwikkelingen en incidenten op het gebied van informatiebeveiliging.

Informatiebeveiliging okt. 2006

Een uitgave van bureau integriteit politie Kennemerland

Reacties en aanmelding voor digitale toezending: jos.van.rijn@kennemerland.politie.nl
Bronnen o.a. Webwereld, Planet, Het Net, Microsoft, Headliner, ZD Net,Telegraaf, Volkskran, Parool etc.

Landelijk loket voor aangifte cybercrime

Tweede Kamer steunt moties SP en PvdA

De Tweede Kamer schaart zich achter een initiatief om een centraal persoon aan te stellen voor de bestrijding van criminaliteit rond hoogwaardige technologie. Ook komt er een landelijk loket voor aangifte. De Tweede Kamer nam twee moties aan waarin deze voorstellen werden gedaan. De moties waren een gezamenlijk initiatief van SP en PvdA.
SP-Kamerlid Arda Gerkens toont zich tevreden met het besluit. "De bestrijding van internetcriminaliteit zal steeds belangrijker worden. Doordat politie, justitie, Economische Zaken en Binnenlandse Zaken zich allemaal apart met de bestrijding bezighouden, dreigde er versnippering te ontstaan. Door de aanstelling van een projectregisseur zal de 'high tech crime' volop bestreden kunnen worden."
Een derde motie, voor het heropstarten van het National High Tech Crime Center (NHTCC), haalde het niet. De NHTCC werd begin 2006, een jaar na de oprichting, weer gesloten nadat er politieke onenigheid was ontstaan over de opzet van de bestrijdingsdienst. Gerkens: "Dat is jammer, want dat was een goed project. Toch denk ik dat een projectregisseur ook een goede oplossing is."

6000 politiedossiers gewist in USA

Een politiedepartement in de Amerikaanse stad Saint Louis is dankzij een computercrash meer dan 6000 dossiers kwijtgeraakt. De dossiers, die allemaal van de afgelopen week waren, moeten opnieuw worden ingevoerd met behulp van notities die men eerder heeft gemaakt.Medewerkers vermoeden dat een netwerkbeheerder, die onlangs werd

BEVEILIGINGSBEWUST

Bijna alle korpsen ontplooien activiteiten op het gebied van de bevordering van de bewustwording op het gebied van informatiebeveiliging van hun medewerkers. In veel gevallen worden nieuwe medewerkers door informatiebeveiligers voorgelicht en geven informatiebeveiligers presentaties aan teams over het belang van informatiebeveiliging. Elf korpsen zijn daarmee op een actieve, intensieve en gestructureerde wijze bezig. Twee van deze elf hebben een specifiek communicatieplan om de bewustwording te verbeteren op het gebied van informatiebeveiliging. Zeven korpsen ontplooien slechts beperkt activiteiten op het gebied van bewustwording. De Inspectie acht dit opmerkelijk in het licht van het feit dat alle korpsen in de interviews en in hun beleidsdocumenten het gedrag van medewerkers als veruit de belangrijkste factor voor het succes van informatiebeveiliging zien. Het is in die zin opvallend dat dit belang niet in alle korpsen wordt vertaald in concrete acties gericht op het verhogen van de bewustwording voor informatiebeveiliging.

Aan de kaak stellen incidenten Rotterdam-Rijnmond

In de afhandeling van informatiebeveiligingsincidenten wordt in Rotterdam-Rijnmond aangesloten bij de activiteiten in het kader van het beleidsprogramma Kompas 2010 gericht op de beïnvloeding van gedrag van korpsmedewerkers. Deze aanpak is onder andere gevolgd in de 'Van Persie'-zaak. Daarbij wordt voor het reactieve deel een gedragslijn gehanteerd die in de loop der tijd op basis van praktijkvoorbeelden is ontwikkeld. Bij de 'Van Persie'-zaak bleek dat na het in het nieuws verschijnen van deze kwestie, gegevens over deze zaak veelvuldig werden opgevraagd door politiefunctionarissen. Deze politiefunctionarissen zijn door hun leidinggevenden bevraagd over hun motieven en de rechtmatigheid van hun bevraging. Waar nodig zijn door de korpsleiding disciplinaire maatregelen en straffen opgelegd.

De korpsen hebben een score gekregen op een vijfpuntsschaal voor informatiebeveiligingsmaatregelen. Dit geeft het volgende beeld per korps op het onderdeel maatregelen in tabel 5:

Tabel 5 Score per korps (op vijfpuntsschaal) op het onderwerp maatregelen

Rang	Korpsnaam	Score	Rang	Korpsnaam	Score
1	Amsterdam-Amstelland	4,17	7	Groningen	3,17
2	Noord- en Oost-Gelderland	4,00		Brabant-Noord	3,17
3	Haaglanden	3,83		Flevoland	3,17
4	IJsselland	3,67	8	Twente	3,00
	Midden- en West-Brabant	3,67	9	Hollands Midden	2,83
	Brabant-Zuid-Oost	3,67	10	Utrecht	2,67
5	Kennemerland	3,50		Zuid-Holland-Zuid	2,67
	Rotterdam-Rijnmond	3,50		Limburg-Noord	2,67
	KLPD	3,50	11	Zeeland	2,50
6	Fryslân	3,33	12	Gooi en Vechtstreek	2,33
	Gelderland-Zuid	3,33	13	Drenthe	2,17
	Noord-Holland Noord	3,33		Gelderland-Midden	2,17
	Zaanstreek-Waterland	3,33		Limburg-Zuid	2,17
				Gemiddeld	3,13

EVALUATIE

Bij de beoordeling van dit onderdeel is gekeken naar de volgende evaluatieaspecten:
- het evalueren van het informatiebeveiligingsbeleid;
- het inbedden van deze evaluatie in de reguliere beleidsevaluatiecyclus en in de INK-cyclus;
- het (laten) uitvoeren van interne en externe audits;
- het toetsen van de implementatie van informatiebeveiligingsmaatregelen in het kader van systeemverwerving.

De korpsen zonder beleidsdocument, met een concept beleidsdocument of met een verouderd beleidsdocument hebben geen evaluatie uitgevoerd. Elf korpsen evalueren het informatiebeveiligingsbeleid op ad hoc basis. Vier korpsen evalueren het informatiebeveiligingsbeleid als onderdeel van de reguliere beleidsevaluatiecyclus, en bij twee hiervan is de evaluatie van informatiebeveiligingsbeleid ook in de INK-cyclus geïntegreerd.

EVALUATIE EN C2000

Bij het merendeel van de korpsen ontbreekt een aanwijzing voor de verwevenheid van C2000 in de beleidsevaluatiecyclus en borging in het INK-proces.
Uit de ingevulde vragenlijsten komt het beeld naar voren dat de korpsen voor het onderwerp naleving samenwerken met CIP (coördinatie vraagorganisatie) en ISC (aanbodzijde). Geen van de korpsen heeft daarbij de directie Mobiele Diensten genoemd[11]. Dit is des te opvallender omdat de directie Mobiele Diensten de centrale beheerder van de C2000-infrastructuur is, waardoor er sprake is van uitbesteding van de korpsen aan deze directie Mobiele Diensten. Diensten kan men uitbesteden; de verantwoordelijkheid voor de bijbehorende informatiebeveiliging niet. In een dergelijke situatie brengen raamcontracten en Service Level Agreements – voorzien van een beveiligingsparagraaf – uitkomst.

AUDITS

Door de korpsen wordt weinig gebruikgemaakt van het auditinstrument als maatregel om de opzet, het bestaan en de werking van beveiligingsmaatregelen uit het BBNP te toetsen. Negen korpsen hebben geen audits laten uitvoeren naar de implementatie van het BBNP. Tien korpsen hebben alleen een interne audit uitgevoerd. Zeven korpsen hebben een externe audit laten uitvoeren; drie van deze audits vonden langer dan vier jaar geleden plaats. Door het ontbreken van interne en externe audits ontbeert de korpsleiding onpartijdige en onafhankelijke zekerheid over de implementatie van het BBNP. Hierdoor wordt het ook moeilijk voor de korpsen om zich richting de collega-korpsen en andere organisaties te verantwoorden over de implementatie van de maatregelen uit het BBNP.

RISICO'S

Het ontbreken van een structurele evaluatie van beleid en maatregelen op het gebied van informatiebeveiliging geeft aan dat er op het gebied van het afleggen van verantwoording over informatiebeveiliging nog veel te winnen is. Gecombineerd met het feit dat interne en externe audits nog slechts beperkt worden toegepast, leidt dit tot het risico dat korpsen beperkt inzicht hebben in de effectiviteit en doelmatigheid van het door hen geformuleerde beleid en de door hen getroffen maatregelen. Daarmee is het tevens onduidelijk of het gerealiseerde niveau van beveiliging toereikend is voor het gewenste niveau van beveiliging.

11 Ten tijde van het onderzoek onderdeel van het ministerie van BZK, thans ondergebracht bij de voorziening tot samenwerking Politie Nederland.

De korpsen hebben een score gekregen op een vijfpuntsschaal voor de evaluatie van informatiebeveiliging. Dit geeft het volgende beeld per korps op het onderdeel evaluatie in tabel 6:

Tabel 6 Score per korps (op vijfpuntsschaal) op het onderwerp evaluatie

Rang	Korpsnaam	Score	Rang	Korpsnaam	Score
1	Noord- en Oost-Gelderland	3,75	7	Utrecht	2,00
2	Kennemerland	3,50		Midden- en West-Brabant	2,00
	Amsterdam-Amstelland	3,50	8	Fryslân	1,75
	Rotterdam-Rijnmond	3,50		Gelderland-Midden	1,75
3	IJsselland	3,25		Gooi en Vechtstreek	1,75
4	Drenthe	3,00		Hollands Midden	1,75
	KLPD	3,00	9	Gelderland-Zuid	1,50
5	Noord-Holland Noord	2,75		Brabant-Noord	1,50
	Brabant-Zuid-Oost	2,75		Limburg-Noord	1,50
	Flevoland	2,75		Limburg-Zuid	1,50
6	Groningen	2,50		Gemiddeld	2,45
	Twente	2,50			
	Zaanstreek-Waterland	2,50			
	Haaglanden	2,50			
	Zuid-Holland-Zuid	2,50			
	Zeeland	2,50			

AANBEVELINGEN

De Inspectie OOV doet op basis van bovenstaande constateringen een aantal aanbevelingen voor verbetering van de implementatie van het Stelsel voor Informatiebeveiliging binnen de Nederlandse politie. Sommige aanbevelingen kunnen binnen de korpsen worden opgepakt, andere hebben betrekking op het systeem van informatiebeveiliging bij de Nederlandse politie en vragen een bovenregionale aanpak.

BELEID

Samenhangend beveiligingsbeleid (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie van vtsPN)

Zorg voor het formaliseren en actualiseren van samenhangend beveiligingsbeleid. Dit beleid dient de verschillende veiligheidsgebieden (personele aspecten van beveiliging, facilitaire en fysieke beveiliging en informatiebeveiliging) onder één paraplu te brengen waardoor de maatregelen binnen deze gebieden beter op elkaar kunnen worden afgestemd.

MAATREGELEN

Risicoanalyse (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Zorg voor het uitvoeren van risicoanalyses (Afhankelijkheids- en Kwetsbaarheids-analyses) voor informatiesystemen om vast te stellen of voldoende informatiebeveiligings-maatregelen zijn getroffen (uitgaande van het BBNP) en integreer dit in de reguliere planning- en controlcyclus. Hierbij kan een afhankelijkheidsanalyse worden uitgevoerd om te bepalen of het gewenste beveiligingsniveau gelijk of onder het basisbeveiligings-niveau ligt. Voor informatiesystemen waarbij het beveiligingsniveau boven het basis-beveiligingsniveau ligt, dienen met een kwetsbaarheidsanalyse aanvullende maat-regelen te worden bepaald.

Incidentenregistratie (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Zorg voor een integrale registratie van (informatie)beveiligingsincidenten als onderdeel van de evaluatiecyclus. Deze centrale registratie dient alle incidenten te bevatten en dient daarvoor op regelmatige basis te worden gevoed vanuit de verschillende incidenten-registraties op het gebied van interne onderzoeken, ICT-helpdesk, fysieke toegangs-beveiliging en dergelijke. De incidenten in de centrale registratie dienen vervolgens regelmatig te worden geanalyseerd. Deze analyse is vervolgens weer input voor de evaluatie van beveiligingsbeleid en –maatregelen.

Beveiligingsbewustzijn (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Bevorder op een planmatige wijze het beveiligingsbewustzijn van politiemedewerkers. Het gedrag van politiemedewerkers bepaalt in hoge mate welke risico's het korps loopt op het gebied van informatiebeveiliging. Ook bepaalt het gedrag van politiemedewer-kers in hoge mate de effectiviteit van de informatiebeveiligingsmaatregelen. Daarom is het zeer belangrijk om pro-actief te sturen op het juiste gedrag van de politiemedewer-kers in het kader van informatiebeveiliging.

ORGANISATIE

Voldoende personeel (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Maak voldoende personeel vrij voor de coördinatie van informatiebeveiligingsactiviteiten om een adequate implementatie van het Stelsel mogelijk te maken. Op basis van de onderzoeksgegevens lijken korpsen met goed opgeleide, enthousiaste en actieve IBF-ers die voldoende tijd kunnen besteden aan informatiebeveiligingstaken succesvoller te zijn bij het implementeren van het Stelsel voor Informatiebeveiliging dan korpsen zonder of met beperkte inzet van IBF-ers.

EVALUATIE

Audits (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Maak systematisch gebruik van het instrument van interne (en externe) audits om zekerheid te verkrijgen over de implementatie van (onderdelen van) het Stelsel voor Informatiebeveiliging. Interregionale (interne) audits zijn hierbij een effectieve werkwijze.

Beleidsevaluatie en INK (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Evalueer het (informatie)beveiligingsbeleid en maak dit onderdeel van de beleids-evaluatie- en INK-cyclus.

Geen activiteit maar een proces

Algemeen aandachtspunt hierbij is dat de implementatie van bovengenoemde aanbevelingen niet als een op zichzelf staande activiteit moet worden gezien; informatie-beveiliging is boven alles een proces, dat dient te zijn ingebed in de managementcyclus van de politiekorpsen.

SYSTEEM

Planmatige aanpak (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Realiseer een planmatige implementatie van het BBNP door het opstellen van informatie-beveiligingsplannen en het monitoren van de uitvoering daarvan mede door het (laten) uitvoeren van interne en externe audits.

Samenwerking (geadresseerd aan korpsbeheerders, korpschefs en bestuur en directie vtsPN)

Zorg in het hele land voor verdergaande interregionale samenwerking op het gebied van informatiebeveiliging en zorg dat de in samenwerking tot stand gekomen producten snel in de korpsen kunnen worden geïmplementeerd.

Rapportage korpsbeheerders (geadresseerd aan de korpsbeheerders en bestuur en directie vtsPN)

Zorg dat de korpsen en de vtsPN vierjaarlijks rapporteren aan de korpsbeheerders over de werking en effectiviteit van de informatiebeveiliging in hun korpsen en bij de vtsPN. Het Korpsbeheerdersberaad zou deze rapportage kunnen agenderen voor overleg met de ministers van BZK en van Justitie. De Inspectie geeft de korpsbeheerders in overweging om deze rapportage een gezamenlijke te laten zijn om zodoende het belang van gezamenlijkheid bij informatiebeveiliging te onderstrepen. Gezien de huidige stand van zaken met betrekking tot de informatiebeveiliging bij de Nederlandse politie beveelt de Inspectie verder aan om in eerste instantie de frequentie van deze rapportages te verhogen, zodat de eerste rapportage voor het eind van 2008 beschikbaar is.

Implementatie Normstelling inrichting interceptiefaciliteiten

6

In 2004 is de Normstelling Inrichting Interceptiefaciliteiten aan de RIP toegevoegd. De minister heeft in december 2003 toegezegd te zullen toezien op de manier waarop de aanvullende regeling op het punt van de inrichting tapfaciliteiten zal worden uitgevoerd. Hierbij gaf hij tevens aan dat de geconstateerde kwetsbaarheden zo snel mogelijk weggenomen dienen te worden. Dit is voor de Inspectie OOV aanleiding geweest om in het kader van dit onderzoek specifieker aandacht te schenken aan het onderwerp interceptie. Een deel van de interceptie van telecommunicatieverkeer door de politie vindt decentraal plaats bij de korpsen en een ander deel wordt centraal verzorgd door de Unit Landelijke Interceptie (ULI) van het Korps Landelijke Politiediensten. Om een zo compleet mogelijk beeld te schetsen van de beveiliging met betrekking tot interceptie wil de Inspectie beide kanten belichten. Daartoe heeft de Inspectie de decentrale vraagstelling in het eigen onderzoek meegenomen en maakt zij voor een antwoord op de vraag over de beveiliging bij de ULI gebruik van een recente audit door de departementale Auditdienst.

In dit hoofdstuk zal ten aanzien van de 25 regiokorpsen en het KLPD de volgende onderzoeksvraag worden beantwoord: welke maatregelen hebben de korpsen genomen met betrekking tot de beveiliging van de locale faciliteiten voor de toegang tot de interceptiefaciliteit?

In het tweede gedeelte van dit hoofdstuk wordt vervolgens ingegaan op de centraal, bij de ULI, georganiseerde onderdelen van de interceptie. De Auditdienst van het ministerie van BZK heeft in het najaar van 2006 hiernaar onderzoek gedaan. De Inspectie OOV heeft de Auditdienst gevraagd in dit hoofdstuk een kort overzicht te geven van haar bevindingen, conclusies en aanbevelingen. Voor de onderbouwing van dit gedeelte verwijst de Inspectie verder naar het auditrapport[12].

De norm voor zowel het onderzoek bij de regiokorpsen als bij de centraal georganiseerde onderdelen van de interceptie wordt gevormd door de Normstelling Inrichting Interceptiefaciliteiten uit 2004.

12 Rapportage Uitkomsten van het eerste deel van het onderzoek naar de centrale tapfaciliteiten bij de Unit Landelijke Interceptie van het KLPD, Kenmerk 2007-103986

STAND VAN ZAKEN ALGEMEEN

CENTRAAL EN DECENTRAAL

Parallel aan de invoering van de Normstelling is gestart met het landelijke project voor de herstructurering van de tapfaciliteiten, waarbij (dure) technische voorzieningen voor het daadwerkelijk tappen centraal worden ondergebracht bij het KLPD (thans de Unit Landelijke Interceptie (ULI)). De regiokorpsen maken inmiddels bijna allemaal gebruik van deze gezamenlijke voorziening. De laatste drie korpsen zullen nog voor de zomer 2007 overstappen op de gezamenlijke voorziening. Daarmee is een belangrijk deel van de technisch-functionele interceptiefaciliteit buiten het bereik van de regiokorpsen komen te liggen.
De Inspectie heeft onderzoek gedaan naar de implementatie door de korpsen van het procedurele deel van de Normstelling. Door de komst van de Unit Landelijke Interceptie is het technisch-functionele aspect binnen de regiokorpsen sterk gereduceerd.

NORMSTELLING INTERCEPTIEFACILITEITEN

INLEIDING

Interceptie van telecommunicatieverkeer is een belangrijk instrument in de opsporing en vervolging van strafbare feiten. Met het oog op een transparant en controleerbaar proces van de interceptie is onder leiding van het Openbaar Ministerie de Normstelling Inrichting Interceptiefaciliteiten opgesteld. Deze normstelling is in 2004 opgenomen in de Regeling Informatiebeveiliging Politie[13]. Bij het opstellen van de normstelling is door het OM samengewerkt met vertegenwoordigers van de ministeries van BZK, van Justitie, van Defensie en de Rechterlijke Macht.

PROCEDURES EN TECHNIEK

De Normstelling bestaat uit een procedureel en een technisch-functioneel gedeelte.
In het procedurele gedeelte worden normen gesteld met betrekking tot de personele organisatie, de gebouwen, de terreinen, de installaties en de informatiebeveiliging. Het technisch-functionele deel beschrijft technische normen die de systeemkwaliteit, de systeemopbouw en de operationele aspecten moeten waarborgen. Beide delen beogen de authenticiteit en integriteit van de interceptiefaciliteiten te garanderen.
Op de korpsbeheerders rust de verplichting de inrichting van de interceptiefaciliteit binnen hun korps te laten voldoen aan de Normstelling. De inhoud van de Normstelling is een aanvulling op de gemeenschappelijke betrouwbaarheidseisen en –maatregelen uit de Leidraad Basisbeveiligingsniveau Nederlandse Politie. De concrete uitwerking van de interceptiebeveiligingsmaatregelen is een verantwoordelijkheid van de korpsen zelf.

13 Artikel 3, lid 2 sub i van het Besluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 30 augustus 2004, nr. EA2004/60705

INTERCEPTIE BIJ DE KORPSEN

ALGEMEEN

Op basis van documentstudie en gesprekken met stakeholders binnen de korpsen is informatie verzameld over een aantal aspecten met betrekking tot het beleid, de organisatie, maatregelen en de naleving van de Normstelling. Bij een beperkt aantal korpsen is ook de locale interceptiefaciliteit (werkstations en uitluisterruimten) bezocht.

INTERCEPTIEBELEID

De korpsen behoren het beheer van de interceptiefaciliteit op te nemen in het algemene beleidsdocument over de informatiebeveiliging. Dit gebeurt echter zelden: slechts twee korpsen hebben in hun beleidsdocument een concrete verwijzing opgenomen naar het interceptiebeveiligingsbeleid. Ruim twee jaar na de formele invoering van de Normstelling is dat een geringe oogst. Diverse korpsen verwijzen in dit verband wel naar aparte interne documenten zoals een protocol, een handboek interceptie of een beveiligingsreglement, waarin de uitwerking van de interceptiefaciliteit is opgenomen. Ongeveer de helft van de korpsen heeft het beheer echter niet in expliciet beleid vertaald of volstaat in dit kader met een verwijzing naar afspraken met de Unit Landelijke Interceptie van het KLPD.
De Inspectie hanteert de norm dat ieder korps moet beschikken over een beleidskader waarin de aanpak van de interceptiebeveiliging is neergelegd. Dit is noodzakelijk voor een gestructureerde en planmatige benadering van dit onderdeel van de informatiebeveiliging. Dit is des te urgenter nu een belangrijk onderdeel van de interceptiefaciliteit is ondergebracht bij het KLPD. In dat verband is een verwijzing naar afspraken met de Unit Landelijke Interceptie onvoldoende. Deze afspraken dienen immers hun grond te vinden in vooraf geformuleerde beleidsdoelstellingen met betrekking tot informatiebeveiliging op het gebied van de interceptie. Eigenlijk geldt ook hetzelfde voor de relatie met ISC en CIP, inmiddels opgenomen in de vtsPN. De Inspectie onderkent het – in de tijd gezien – recente karakter van deze ontwikkelingen, maar is van oordeel dat het de korpsen niet ontslaat van de verplichting om aan die nieuwe kaders, zeker voor de toekomst, beleidsmatig aandacht te besteden.

BETROKKENHEID OM

Gelet op het belang van een planmatige aanpak heeft de Inspectie een aantal aspecten van beleid in het normenkader van haar onderzoek opgenomen (zie bijlage II). Het betreft in de eerste plaats de betrokkenheid – vanuit zijn strafrechtelijke en strafvorderlijke verantwoordelijkheid – van het Openbaar Ministerie bij het stellen van eisen aan de inrichting van de interceptiefaciliteit. Deze betrokkenheid staat los van de positie die het OM heeft in het feitelijke interceptieproces.

In het merendeel van de korpsen speelt het OM ten aanzien van die inrichting op enigerlei wijze een rol. Bijvoorbeeld bij de vaststelling van documenten, bij het implementatietraject of via (periodiek) overleg. Bij eenderde van de korpsen is die betrokkenheid er niet of wordt door het korps verwezen naar de rol van het OM bij de ontwikkeling van de Normstelling op landelijk niveau. Dit laatste is naar de mening van de Inspectie te mager, omdat het belang van het Openbaar Ministerie bij de Normstelling toch vooral te vinden is in de concrete uitvoering door de korpsen.

GEGEVENSBEHEER

De korpsen is gevraagd hoe zij de verantwoordelijkheid voor het beheer van de gegevens die in het kader van de interceptie worden verzameld in het beleidsdocument hebben belegd. De meeste korpsen verwezen in dit verband naar de kaders die binnen de korpsen gelden ten aanzien van de uitvoering van de Wet op de Politieregisters. Een aantal korpsen heeft opgemerkt dat dit onderdeel van de interceptiebeveiliging nog opgenomen zal worden in het beleidsdocument.

DE INTERCEPTIEBEVEILIGINGSORGANISATIE

De korpsen hebben maatregelen moeten treffen om de implementatie en uitvoering van de normen voor de inrichting van de interceptiefaciliteiten te realiseren. Primair gebeurt dit door de toewijzing van de verantwoordelijkheden aan het lijnmanagement. Die verantwoordelijkheid is in de Normstelling nader omschreven en heeft onder andere betrekking op het uitvoeren van uit de Normstelling voortvloeiende maatregelen, de evaluatie daarvan, de zorg voor een incidentenbeleid en de zorg voor (interne en externe) auditing van het interceptieproces.
Uit het onderzoek blijkt dat bijna alle korpsen een functionaris in het korpsmanagement hebben aangewezen die verantwoordelijk is voor het interceptieproces. In het merendeel van de korpsen is dit het hoofd van de recherche, die (in de rol van portefeuillehouder of proceseigenaar) is belast met de strategische en beleidsmatige aspecten van de interceptie. Daarnaast hebben enkele korpsen de regionale interceptiecoördinator belast met de meer op de uitvoering gerichte operationele taken. Soms is deze functionaris, of het hoofd van de Interceptie-eenheid tevens als directe verantwoordelijke voor de interceptiefaciliteit aangewezen. In enkele korpsen ontbreekt een eindverantwoordelijke: het is dan òf nog niet – formeel – geregeld, òf de verantwoordelijkheid is weggezet in het lijnmanagement van de onderdelen, bijvoorbeeld de districten.
De Inspectie acht de toewijzing van verantwoordelijkheid voor de interceptie op strategisch niveau een belangrijke katalysator voor het interceptiebeveiligingsbeleid.

SCHEIDING VAN FUNCTIES

Naast de verantwoordelijkheid op regionaal niveau speelt de verdeling van taken, bevoegdheden en verantwoordelijkheden ook een rol bij de uitvoering van interceptiewerkzaamheden. De Normstelling geeft in dat verband de kaders aan voor de invulling van de personele organisatie van de interceptiefaciliteit. Het gaat dan om de eenduidige vastlegging van functie-eisen en functieomschrijvingen, de scheiding in beschikkende, uitvoerende, administrerende en controlerende functies en de rechtspositie van medewerkers.
De Inspectie heeft zich in dit onderzoek gericht op de vraag naar de scheiding van functies binnen het interceptieproces. Een kwart van de korpsen heeft een dergelijke scheiding nog niet op adequate wijze geregeld. Veelal speelt de omvang van de (beperkte) personele bezetting die belast is met de interceptiewerkzaamheden hierbij een rol. In het merendeel van de korpsen is de functiescheiding wel geoperationaliseerd, waarbij de feitelijke uitvoering op verschillende wijzen is ingevuld. Het merendeel van de korpsen benoemt een aaneenschakeling van onderling afhankelijke en elkaar opvolgende controles. Het kan hier gaan om procedurele maatregelen voor het daadwerkelijk 'tappen' binnen de eigen organisatie (bijvoorbeeld: verzoek door onderzoeksleider – beschikken door OM – uitvoeren door rechercheur) en voor het beheer van het proces (bijvoorbeeld: administreren door informatiecoördinator RIC en controle door de unitchef). Of om logische toegangscontroles door middel van pincodes, pasjes of wachtwoorden. Soms is ook de ULI ingeschakeld voor het aanmaken van autorisaties. Een aantal korpsen verwijst bij de functiescheiding naar de ULI en in het kader daarvan (ook) op de scheiding in het technische deel tussen de ULI en de regio.

AFSPRAKEN MET ULI

Gelet op de recente veranderingen is de korpsen gevraagd naar afspraken met het KLPD/ULI. Het KLPD heeft daarvoor een aantal standaarddocumenten ontwikkeld:
- de dienstverleningsovereenkomst (DVO) heeft als doel het vastleggen van kwantitatieve en kwalitatieve afspraken over de dienstverlening door de Unit Landelijke Interceptie;
- het Dossier Afspraken en Procedures (DAP) dient om de processen waarvoor de opdrachtnemer en de opdrachtgever verantwoordelijk zijn vast te leggen. Tevens worden alle afspraken en procedures die relevant zijn voor het nastreven van de afgesproken dienstverlening in de DVO, in het DAP vastgelegd;
- tenslotte worden op basis van de DVO en het bijbehorende DAP met de verschillende opdrachtgevers separaat nadere overeenkomsten (NOK) gesloten waarin wordt vastgesteld hoeveel en welke diensten worden geleverd en tegen welk tarief.

De Inspectie meent overigens dat in het kader van de functiescheiding niet volstaan kan worden met een verwijzing naar deze documenten, omdat zij niet het complete scala aan interceptietaken binnen de eigen organisatie beslaan.
Het onderzoek biedt ten aanzien van de afspraken tussen de korpsen en het KLPD/ULI

een wisselend beeld. In veel gevallen is al sprake van DVO's, DAP's en soms ook NOK's. Doordat de overgang van de technische interceptiefaciliteiten van de regio naar het KLPD nog gaande is, hebben diverse korpsen aangegeven dat de afspraken feitelijk nog niet gerealiseerd en/of formeel vastgelegd zijn. Voor meer dan de helft van de korpsen is dat echter wel het geval.

INTERCEPTIEBEVEILIGINGSMAATREGELEN

De Normstelling geeft een nadere detaillering van de beveiligingseisen uit de Leidraad BBNP, toegespitst op de interceptiefaciliteit. Hierbij wordt gesteld, dat de concrete uitwerking van maatregelen door de direct verantwoordelijke voor de interceptiefaciliteit opgesteld moet worden. Deze maatregelen hebben onder meer betrekking op de procedures voor de toegang tot de fysieke interceptieruimten binnen het korps en op het beheer van de toegang tot de interceptiesystemen. De Normstelling geeft de kaders aan voor de fysieke toegangscontrole van gebouwen en terreinen die als zogenaamde kritische ruimten van de interceptiefaciliteit zijn aangemerkt. Het is de verantwoordelijkheid van de korpsbeheerder om deze maatregelen ook concreet te laten werken. De Inspectie heeft op basis van het documentenonderzoek en interviews geïnventariseerd in hoeverre de Normstelling als richtlijn voor de inrichting van de regionale interceptiefaciliteiten is gehanteerd. Daarbij is vooral gelet op de fysieke maatregelen met betrekking tot interceptieruimten, de toegang tot het systeem (de logische maatregelen) en de behandeling van incidenten.

UITLUISTERRUIMTEN

Alle korpsen beschikken over eigen interceptiefaciliteiten. Door de komst van de centrale technische tapvoorziening bij het KLPD/ULI en de – in de tijd gezien – geleidelijke overgang van de regiokorpsen naar die voorziening, beschikt een aantal korpsen nog over een eigen 'volledige' interceptiefaciliteit. Nadat alle regiokorpsen op het KLPD/ULI zullen zijn aangesloten, beschikken zij alleen nog over werkstations/uitluisterruimten. Het huidige beeld van deze voorzieningen binnen de korpsen is divers. Het varieert van één centrale voorziening van waaruit de interceptiewerkzaamheden uitgevoerd kunnen worden tot de situatie waarin de werkplekken over meerdere locaties binnen het korps zijn verspreid. Daarbij loopt het aantal uitluisterruimten of werkplekken ook sterk uiteen (van enkele tot tientallen). Sommige korpsen maken ook gebruik van mobiele tapvoorzieningen, die op aanvraag gebruikt kunnen worden. Een enkel korps voorziet in de mogelijkheid om op de eigen werkplek van de rechercheur de interceptiefaciliteit te gebruiken. De consequentie van dit gevarieerde beeld voor de kwaliteit van de interceptie staat of valt met de beveiligingsmaatregelen die door de korpsen voor hun specifieke situatie zijn getroffen.

KRITISCHE RUIMTEN

De interceptiefaciliteit kent diverse zogenaamde kritische ruimten zoals de werkplekken (werkstations/uitluisterruimten) voor de medewerkers en de ruimten voor computers en de overige apparatuur en de archieven. Met het oog op de beveiliging dienen de korpsen procedures te hebben waarin de toegang tot die ruimten en de autorisatie is geregeld. Uit het onderzoek blijkt dat alle korpsen op dit onderdeel maatregelen hebben getroffen. Over het algemeen zijn dit elektronische beveiligingsmaatregelen, waarbij een vorm van toegangsregulatie is ingevoerd. Terugkerende begrippen daarbij zijn registratie, autorisatie, compartimentering en zonering (tijdsgebonden toegang op basis van functie).
Een aantal korpsen heeft de maatregelen getroffen naar aanleiding van een A&K-analyse, een quick-scan op de beveiliging of een interne audit. Soms is het toegangsregime onderdeel van het algemene toegangsbeveiligingssysteem van het korps; in andere gevallen is het systeem voor de interceptie daarvan afgescheiden.
Voor zover de maatregelen bestaan uit 'sleutel en slotvoorzieningen' in combinatie met een aangewezen beheerdersverantwoordelijkheid pleit de Inspectie ervoor te voorzien in elektronische maatregelen, omdat de beveiliging van de interceptie daarbij het objectiefst controleerbaar is. Een aantal korpsen koppelt de verbetering van de fysieke beveiligingsmaatregelen aan (komende) verbouwingen van de voorzieningen. Door een heldere autorisatieprocedure vooraf en persoonsgebonden toegangscodes is sprake van een overzichtelijk en controleerbaar proces, met de mogelijkheid informatie over de in- en uitregistratie van de betreffende ruimten te bewaren (historische gegevens).

TOEGANG TOT HET SYSTEEM

Voor de toegang tot het systeem van de interceptiefaciliteit is eveneens door alle korpsen een regeling getroffen. Doordat de Normstelling zich beperkt tot kaders voor dit beveiligingsaspect, biedt het onderzoek ook hier een beeld van de verschillende manieren waarop de korpsen daaraan concreet invulling hebben gegeven. De autorisatieprocedures zijn meestal opgebouwd uit elkaar opvolgende activiteiten van personen: gebruiker – beheerder – supervisor – toestemming – toegang. De Regionale Interceptiecoördinator speelt hierbij veelal een centrale rol.
In een enkel geval is de toegang echter geautomatiseerd door bijvoorbeeld een inlogprocedure met gebruikersnaam en wachtwoorden zoals in een citrixomgeving. Eén korps heeft de logische toegangsbeveiliging gekoppeld aan mutaties in het personeelssysteem Beaufort.
Het KLPD/ULI heeft bij inmiddels de meeste korpsen een functie in dit proces, enerzijds als technische beheerder van de interceptiefaciliteit door het overzicht van de gebruikersactiviteiten, anderzijds als de dienst die de toestemming tot de toegang van het systeem feitelijk realiseert.

Hoewel de indruk bestaat dat de korpsen voor de logische toegangbeveiliging maatregelen hebben getroffen, ontbreekt naar de mening van de Inspectie ook hier nog vaak de weerslag daarvan in een toetsbaar document.

INCIDENTEN

De Inspectie heeft gekeken naar de uitwerking door de korpsen van de incidentenprocedure. Het incidentenbeheersproces heeft tot doel verstoringen, die de dienstverlening ongewenst beïnvloeden, tijdig te verhelpen. De uitwerking van deze categorie maatregelen heeft in veel korpsen nog een (voornamelijk) ad hoc karakter. De individuele actie van de functionaris is bepalend, meldingen worden bijvoorbeeld aangemerkt als een persoonlijke verantwoordelijkheid, of zijn afhankelijk van het initiatief van de medewerker. Zij komen aan de orde in het werkoverleg of zijn onderwerp in een (periodiek) overleg van de regionale interceptiecoördinator met teamchefs of beveiligingsfunctionarissen. Een enkel korps heeft de maatregelen vastgelegd in werkafspraken en procedures voor de interceptie. Soms wordt verwezen naar het integrale regionale informatiebeveiligingsbeleid of zijn er werkafspraken geregeld met het KLPD/ULI en het ISC over de 'technische meldingen'.
De Inspectie vindt dat het beeld, dat thans uit de inventarisatie naar voren komt, aanleiding is voor een verbetering van de incidentenprocedure. Onverminderd de notie dat medewerkers de eerst aangewezen functionarissen zijn om bij dit aspect van de interceptiemaatregelen een wezenlijke rol te spelen, dienen de procedure, registratie en rapportage met betrekking tot incidenten op duidelijke wijze vastgelegd en algemeen bekend te zijn als richtlijn voor de praktijk.

EVALUATIE INTERCEPTIEFACILITEITEN

Strikte naleving van de Normstelling is van cruciaal belang. Om dat te bevorderen is in de Normstelling voorzien in periodieke interne en externe audits. De implementatie en de uitvoering dienen jaarlijks te worden beoordeeld door daartoe geautoriseerde medewerkers binnen de korpsen. De Normstelling benoemt daarbij een aantal aspecten waarop de interne audit gericht dient te zijn. Het betreft ondermeer de maatregelen die in de vorige paragraaf zijn behandeld.
De externe audit wordt uitgevoerd door een daartoe gekwalificeerde derde partij en vindt tenminste om de drie jaar plaats; de eerste keer binnen twee jaar na de vaststelling van de Normstelling (medio 2004). De audit moet uitsluitsel geven over de juiste naleving van de Normstelling.
Ondanks de voorgeschreven norm blijkt dat meer dan de helft van de korpsen interne noch externe audits hebben uitgevoerd of doen uitvoeren. Dit betekent dat in deze korpsen ruim twee jaar na de invoering van de Normstelling nog geen toetsbaar onderzoek heeft plaatsgevonden naar de in- en uitvoering van de maatregelen, die daarin zijn beschreven.

Ten aanzien van de overige korpsen geldt het volgende. Door de vormvrijheid worden interne audits op diverse wijzen ingevuld, zoals interne scans, site survey en gesprekken, waarvan niet steeds verslaglegging heeft plaatsgevonden. Externe audits zijn nog nauwelijks uitgevoerd en hebben daarbij soms nog betrekking op de situatie voor of ten tijde van de invoering van de Normstelling. Slechts een enkel korps heeft kunnen laten zien dat het diverse interne en externe audits heeft uitgevoerd met betrekking tot de informatiebeveiliging waarbij specifieke deelaspecten, opzet, bestaan, en werking van het BBNP en de Normstelling zijn beoordeeld. Eén korps heeft tot voor kort met regelmaat audits uitgevoerd, maar is daar in verband met de overgang naar het KLPD/ULI tijdelijk mee gestopt. Dit laatste argument wordt overigens ook door veel andere korpsen aangevoerd als reden voor het uitblijven van audits tot op heden.

AANBEVELINGEN

Beleidskader (geadresseerd aan de korpsbeheerders en korpschefs)

Formuleer een beleidskader voor een gestructureerde en planmatige aanpak van de interceptiebeveiliging en beleg de verantwoordelijkheid voor de uitvoering daarvan op strategisch niveau binnen het korps.

Overeenkomsten (geadresseerd aan de korpsbeheerders)

Leg de relatie van het politiekorps met het KLPD/ULI over het interceptieverkeer vast in een geformaliseerde overeenkomst.

Audits (geadresseerd aan korpsbeheerders en korpschefs)

Zorg dat op korte termijn de voorgeschreven interne en externe audits worden uitgevoerd, zodat kan worden vastgesteld welke hiaten er (nog) zijn in de implementatie van de Normstelling (toegespitst op het uitluisteren).

DE CENTRALE ONDERDELEN VAN DE INTERCEPTIE, EEN KORT OVERZICHT VAN DE BEVINDINGEN VAN DE AUDITDIENST VAN HET MINISTERIE VAN BZK

De Inspectie OOV heeft de Auditdienst gevraagd om in dit hoofdstuk kort haar belangrijkste bevindingen, conclusies en aanbevelingen weer te geven. Op deze wijze ontstaat een zo compleet mogelijk beeld van de informatiebeveiliging bij interceptie, zowel decentraal als centraal.

ALGEMEEN

De Unit Landelijke Interceptie van het Korps Landelijke Politie Diensten (ULI) faciliteert de Nederlandse Politie sinds mei 2005 met de interceptie van alle wettelijk aftapbare communicatie. Het afgelopen jaar heeft de ULI zich noodzakelijkerwijs gericht op de continuïteit en de opbouw van de primaire dienstverlening. De oorzaak hiervan is de overgang van de centrale onderdelen van de interceptiefaciliteiten van de regiokorpsen naar de ULI en de vernieuwingsslag voor wat betreft de technische faciliteiten.

Voor de uitvoering van het onderzoek heeft de Auditdienst gekozen voor een gefaseerde aanpak gegeven de complexiteit van het onderwerp. De eerste fase van het onderzoek is inmiddels afgerond en heeft een verkennend karakter gehad. Het onderzoek heeft zich ondermeer gericht op de organisatie en de bestuurlijke omgeving van het ULI en op de actualiteit en naleving (op hoofdlijnen) van de normstelling interceptie.

BESTUURLIJKE CONTEXT & NORMSTELLING

De ULI onderhoudt een aantal sturings- en verantwoordingsrelaties met partijen in haar omgeving. Een eerste belangrijke partij is de Commissie Interceptie bestaande uit vertegenwoordigers van de klanten van de ULI. De Commissie Interceptie is verantwoordelijk voor de functionele aansturing van de ULI. Een tweede belangrijke partij is de minister van BZK als korpsbeheerder van het KLPD.

Uit de beoordeling van de bestuurlijke context komt naar voren dat de ULI zich aan de ene kant niet verantwoordt over de naleving van de Normstelling. Aan de andere kant vragen de Commissie Interceptie en de minister van BZK ook niet om een dergelijke verantwoording. Het bijbehorende risico is dat de naleving van de normstelling niet zichtbaar wordt gemaakt en eventuele knelpunten in de normstelling niet worden vastgesteld en dus ook niet kunnen worden verbeterd. De Auditdienst beveelt de ULI aan om jaarlijks te rapporteren over de naleving van de normstelling. De met de governance belaste organen zouden overigens ook jaarlijks om een dergelijke verantwoording van de ULI moeten vragen.

INTERNE AUDIT EN KWALITEITSBEHEERSING

In de normstelling wordt een jaarlijkse interne audit op de naleving van de normstelling voorgeschreven. De ULI heeft aangegeven dat op het moment niet is voorzien in een dergelijke audit. De leiding van de ULI mist hiermee de basis om scherp te sturen op de naleving van de normstelling en om hierover extern verantwoording af te leggen. Voor het uitvoeren van een goede interne controle en audit ontbreken binnen de ULI de functies gericht op onder meer kwaliteitsbeheersing en security management. De aanbeveling van de Auditdienst is om op korte termijn de inrichting van een kwaliteits-

managementfunctie binnen de ULI ter hand te nemen en een security officer functie op te zetten, waarbij dient te worden onderzocht of in de staande organisatie voldoende capaciteit aanwezig is.

NALEVING NORMSTELLING DOOR ULI

Het onderzoek naar de naleving van de normstelling door de ULI levert op hoofdlijnen de volgende conclusies op:

- de ULI kan zelf niet aangeven hoe zij scoort ten opzichte van de normstelling (in lijn met de bevindingen over interne audit);
- op onderdelen voldoet de ULI niet aan de normstelling interceptie. Hierbij merkt de Auditdienst overigens op geen aanwijzingen te hebben dat hier directe risico's uit voortvloeien.

AANDACHTSPUNTEN NORMSTELLING

De normstelling betreft een complex stelsel van maatregelen (een combinatie van eisen/maatregelen die essentieel worden geacht en eisen die bijdragen aan de doelmatigheid) dat moet aansluiten op de actuele interceptieomgeving. Vanuit deze benadering zijn de volgende aandachtspunten vastgesteld:

- De normstelling is geschreven vanuit een situatie waarin de interceptie van het signaal en het uitluisteren van de informatie binnen één korps plaatsvindt. Dit stemt niet meer overeen met de huidige situatie.
- De normstelling is opgezet met de (impliciete) veronderstelling dat interceptie betrekking heeft op een beperkt aantal telecomaanbieders en 'volwassen' diensten. In het licht van de ontwikkelingen rondom telecommunicatie via internet is deze aanname niet langer valide.
- De normstelling wordt niet geëvalueerd en bijgesteld.

Het risico hierbij is dat de naleving van de essentiële eisen uit de normstelling aan de kwaliteit van de interceptie van (nieuwe) telecomdiensten onvoldoende is geborgd. Dit kan ertoe leiden dat de ULI en de afnemende korpsen mogelijk worden gedwongen tot een eigen interpretatie en prioritering van maatregelen uit de normstelling. De Auditdienst beveelt aan om de normstelling op korte termijn te evalueren en vervolgens jaarlijks bij te stellen op basis van de uitkomsten van de jaarlijkse interne audits bij de korpsen en de ULI.

Resumerend acht de Auditdienst het gewenst dat de ULI, nadat ook de laatste korpsen zijn aangesloten en de vernieuwingsslag inzake de technische faciliteiten is afgerond, werk maakt van het kwaliteitsmanagement en de inrichting van de security officer functie. Vervolgens is van belang om de overige in de rapportage van de Auditdienst genoemde punten voortvarend ter hand te nemen.

Bijlage: Lijst met afkortingen

I

A&K-analyse	Afhankelijkheids- en Kwetsbaarheidsanalyse
ABM	Algemene Beveiligingsmaatregelen
AIVD	Algemene Inlichtingen- en Veiligheids Dienst
ARK	Algemene Rekenkamer
BBNP	Basis Beveiligingsniveau Nederlandse Politie
BEI-eisen	Beschikbaarheid, Exclusiviteit en Integriteits-eisen
BPI	Beleidsadviescollege voor de Politiële Informatievoorziening
BZK	Binnenlandse Zaken en Koninkrijksrelaties
CIO	Chief Information Officer
CIP	Concern Informatiemanagement Politie
DAP	Dossier Afspraken en Procedures
DGV	Directoraat Generaal Veiligheid
DVO	Dienstverleningsovereenkomst
DJI	Dienst Justitiële Inrichtingen
ECIB	Expertisecentrum Informatiebeveiliging Nederlandse Politie
ESAKa	Expertsysteem Afhankelijkheid- en Kwetsbaarheidanalyse
EXIN	Examen Instituut voor ICT-ers
Fte	Fulltime-equivalent
GGD	Gemeentelijke Gezondheidsdienst
IB	Informatiebeveiliging
IBF (IBF-er)	Informatie Beveiliging Functionaris
ICT	Informatie- en Communicatietechnologie
ITO	Agentschap Organisatie Informatie- en Communicatie Technologie
INK	Instituut Nederlandse kwaliteit
Inspectie OOV	Inspectie Openbare Orde en Veiligheid
ISC	ICT-Service Coöperatie Politie, Justitie en Veiligheid
ISF	Information Security Foundation
ISMA	Information Security Management
KBB	Korps Beheerdersberaad
KLPD	Korps Landelijke Politiediensten
NOK	Nadere overeenkomsten
NPI	Nederlands Politie Instituut
OM	Openbaar Ministerie
P&O	Personeel en Organisatie
PDC	Producten en Diensten Catalogus
PPI	Platform Politiële informatievoorziening
PwC	PricewaterhouseCoopers
RBS	Recherche Basis Systeem

RvHC	Raad van Hoofdcommissarissen
RIC	Regionale Informatiecoördinator
RIP	Regeling Informatiebeveiliging Politie
RvT	Raad van Toezicht
SLA	Service Level Agreement
Stcrt	Staatscourant
TIB	Taakaccenthouder Informatiebeveiliging
TVB	Taken, Verantwoordelijkheden en Bevoegdheden
ULI	Unit Landelijke Interceptie van het KLPD
VIR	Voorschrift Informatiebeveiliging Rijksdienst
vtsPN	Voorziening tot samenwerking Politie Nederland
Wpolr	Wet politieregisters

Bijlage: Normenkader Informatiebeveiliging Politie (korpsbezoek)

II

Normen	Broninfo	Bevind./ Conclusie	Risico's
A: Informatiebeveiligingsbeleid (vastleggen, bekrachtigen, uitdragen en inhoud)			
1. RIP artikel 3: De korpsbeheerder dient een beleidsdocument vast te leggen, te bekrachtigen en op actieve wijze uit te dragen aan alle werknemers. Dit document dient de betrokkenheid van het management te verwoorden, alsmede de benadering van de organisatie ten aanzien van het omgaan met informatiebeveiliging.			
Interceptiebeveiligingsbeleid 1. art. 3 jo 6a RIP: de korpsbeheerder heeft het beheer van de interceptie-faciliteiten (RIP) en voor de gegevens (Wet Pol. registers) belegd in het beleidsdocument over informatiebeveiligingsbeleid.			
C2000 beveiligingsbeleid 2. De korpsbeheerder heeft het geaccordeerde beveiligingsbeleid C2000 ingebed/in lijn gebracht met het beleidsdocument over informatie-beveiligingsbeleid.			
2. RIP artikel 3: Het document beveiligingsbeleid omvat tenminste: - de strategische uitgangspunten en randvoorwaarden, met name de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningbeleid; - de organisatie van de beveiligingsfunctie (incl. verantwoordelijkheden, taken en bevoegdheden); - informatievoorzieningfaciliteiten en toewijzing vertaling naar concrete maatregelen inclusief wijze van financiering; - de gemeenschappelijke betrouwbaarheidseisen en maatregelen; - wijze van melding en afhandeling inbreuken op de informatiebeveiliging; - evaluatieschema informatiebeveiligingsbeleid, toets op toereikendheid en beoordeling implementatie en de uitvoering; - bevordering beveiligingsbewustzijn.			
Interceptiebeveiligingsbeleid 1. In het interceptiebeveiligingsbeleid is specifiek aandacht voor: - verantwoordelijkheid voor de naleving van de Normstelling (zie norm 2 b); - behandeling incidenten (zie norm 2 e); - evaluatie (zie norm 2 f).			
2. Strafrechtelijke verantwoordelijkheid, brief d.d. 05-12-2003 aan de TK 29 200 VII, nr 39, pag. 2; het Openbaar Ministerie is betrokken bij de eisen die aan de inrichting van de tapfaciliteiten worden gesteld.			

Normen (vervolg)	Broninfo	Bevind./ Conclusie	Risico's
B: Organisatie informatiebeveiligingsfunctie - algemeen (specifiek: opleiding, functiescheiding, samenwerken en afspraken, inbreuken melden en afhandelen)			
3. RIP artikel 3: Taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging dienen vastgesteld te zijn. Beveiligingsrollen en verantwoordelijkheden dienen in functiebeschrijvingen opgenomen te worden. ! (Uit handreiking hulporganisatie) Er is een hulpoganisatie[1] ingericht die voorziet in: de Portefeuillehouder Informatiebeveiliging, de Infomatie-beveiligingsfunctionaris (IBF) en het Informatiebeveiligingsberaad (IB-beraad); en daarnaast in de Auditor informatiebeveiliging en de Taakaccenthouder informatiebeveiliging (TI). ! (Uit handreiking hulporganisatie) De IBF is deskundig op het gebied van informatiebeveiliging en is in staat de korpsbeheerder en diens leiding-gevenden te adviseren op dat gebied. Voor deskundige invulling van specifieke informatiebeveiligingsrollen (zie 4.a) is voorzien in een opleidings-plan. Dit opleidingsplan bevat de deskundigheidseisen IBF (kenniseisen). ! BBNP: Bij de inrichting van de informatiebeveiligingsfunctie dient functie-scheiding te zijn toegepast (Scheiding tussen beschikkende, uitvoerende, administrerende en controlerende taken). NB: Ten aanzien van functiescheiding richt het onderzoek zich specifiek tot vragen over twee specifieke objecten: de interceptiefaciliteit en de infodesk. ! BBNP: Functiescheiding is één van de meest elementaire voorwaarden om beveiligingsmaatregelen binnen het korps effectief te laten zijn. Concentratie van bevoegdheden in één persoon kan tot gevolg hebben dat noodzakelijke controles niet worden uitgevoerd, waardoor aantasting van de integriteit, de beschikbaarheid en de exclusiviteit van de gegevens onopgemerkt blijft.			
Interceptiebeveiligingsorganisatie 1. par. 2.2 Normstelling: taken, bevoegdheden en verantwoordelijkheden van het lijnmanagement van de gebruikersorganisatie respectievelijk de automatiseringsorganisatie in het korps zijn vastgelegd; 2. par. 5.1 Normstelling: taken, bevoegdheden en verantwoordelijkheden van de medewerkers zijn vastgelegd in functieomschrijvingen; 3. par. 5.2 Normstelling: er is sprake van functiescheiding tussen beschikkende, uitvoerende, administratieve en controlerende taken (vier functiecategorieën: operationeel gebruiker, operationeel beheerder interceptie, operationeel beheer supervisor, technisch beheerder). **Infodesk** 4. De wijze waarop informatiebeveiliging Infodesk binnen het korps is georganiseerd is vastgelegd. 5. Functiescheiding dient te zijn toegepast, dan wel er zijn hiervoor compenserende maatregelen gedefinieerd.			
4. RIP artikel 5: Afspraken in het kader van gegevensuitwisseling en ICT-dienstverlening: - politiekorpsen en ITO[2] werken samen voor zo uniform mogelijke beveiligings-afspraken, betrouwbaarheidseisen en maatregelen, en informatiebeveiligings-plannen; - RIP artikel 2: Het politiekorps dient met ITO en andere politiekorpsen schriftelijke afspraken te hebben opgesteld over de informatiebeveiligings-normen op basis van de in de RIP-bijlage genoemde criteria en bijbehorende normklassen;			

1 Genoemde hulporganisatie was oorspronkelijk bedoeld voor het maken van een inhaalslag informatiebeveiliging

2 ITO dan wel de opvolger van de organisatorische entiteit ITO (CIP en ISC)

Normen (vervolg)	Broninfo	Bevind./ Conclusie	Risico's
B: Organisatie informatiebeveiligingsfunctie - algemeen (specifiek: opleiding, functiescheiding, samenwerken en afspraken, inbreuken melden en afhandelen)			
- RIP artikel 2: Het politiekorps dient met ITO en andere instanties schriftelijke afspraken te hebben opgesteld over de betrouwbaarheid van informatiesystemen plus informatie en de wijze waarop hierover zekerheid wordt verkregen (realisatie). ! (Best practice overheid) Voor de ter zake te sluiten (interne of externe) contracten (nadere overeenkomsten, service level agreements, dossiers met afspraken en procedures) dient voorzien te zijn in afspraken die er voor zorgen dat storingen en incidenten beperkt blijven binnen de gestelde betrouwbaarheidseisen (beschikbaarheid, exclusiviteit en integriteit) en daarmee niet conflicteren. ! (Best practice overheid) Wanneer er uitbestedingen plaatsvinden aan externe instanties, dient er een adequaat contractbeheer te worden gevoerd, waarbij er van de zijde van het politiekorps op hoofdlijnen sturing moet worden gegeven aan de inhoud van die contracten. Een stuurmiddel in deze is het op de terzake afgesproken momenten ontvangen van rapportages over de dienstverlening en de status van het overeengekomen beveiligingsniveau en onafhankelijke controles (TPM, EDP-audit, etc.). ! BBNP: Dienstenniveaubeheer heeft tot doel de basis te leggen om de juiste diensten, in de juiste omvang op de juiste plaats en van de juiste kwaliteit te kunnen leveren, door afspraken daarover te maken tussen de gebruikersorganisatie en de automatiseringsorganisatie. ! BBNP: Het uitbesteden van het beheer van de netwerkinfrastructuur vindt in toenemende mate plaats. Indien dit onder de juiste conditie plaatsvindt hoeft uitbesteden vanuit beveiligingsoogpunt geen belemmering te zijn. Wel zullen er waarborgen moeten zijn omtrent het te hanteren beveiligingsniveau.			
Interceptiebeveiligingsorganisatie 1. art. 5 RIP: de samenwerking tussen het korps en het KLPD/ULI en korpsen onderling met betrekking tot het gebruik van de interceptiefaciliteiten is vastgelegd in afspraken over beveiligingsmaatregelen met betrekking tot de gegevensuitwisseling;			
C: Informatiebeveiliging; vertaling naar concrete maatregelen, classificatie			
5. RIP artikel 3: Er dient ten behoeve van een totaaloverzicht per dienstonderdeel een overzicht van alle informatiesystemen/gemeenschappelijke IT-diensten te zijn opgesteld en te worden onderhouden. Daarbij dient aan de genoemde informatiesystemen/gemeenschappelijke IT-diensten een verantwoordelijke manager te zijn toegewezen. De hierbij te hanteren beveiligingsclassificaties dienen de landelijk afgestemde normklassen en criteria te bevatten.			
6. RIP artikel 4: Er dient een, van het RIP afgeleid, basisbeveiligingsniveau te zijn gedefinieerd, vastgesteld en geïmplementeerd (Basisbeveiligingsniveau Nederlandse Politie) ten behoeve van het afdekken van risico's in geval van niet kritische informatiesystemen/gemeenschappelijke IT-diensten. Dit basisbeveiligingsniveau dient geïmplementeerd te zijn. Eind 2005 is de (gefaseerde) invoering van geïdentificeerde informatiebeveiligingsmaatregelen gereed.			

Normen (vervolg)	Broninfo	Bevind./ Conclusie	Risico's
C: Informatiebeveiliging; vertaling naar concrete maatregelen, classificatie			
a. BBNP: set van benodigde maatregelen kan niet in één keer ingevoerd worden. Prioritering is op zijn plaats. Daarom is in een bijlage bij deze leidraad een instrument opgenomen om de korpsen in staat te stellen op systematische wijze, dat wil zeggen op basis van een aantal criteria een goede afweging te maken wat eerst en wat later geïmplementeerd dient te worden. Het zogenaamde 'Wegingsinstrument' is ook in geautomatiseerde vorm beschikbaar. Voor de wijze waarop gebruik kan worden gemaakt van het Wegingsinstrument' wordt verwezen naar de daarop betrekking hebbende handleiding.			
7. RIP artikel 4: De korpsbeheerder dient zorg te dragen voor het op systematische wijze identificeren van te treffen maatregelen voor informatiebeveiliging. Per informatiesysteem en gemeenschappelijke IT-dienst dient (bovenop het basisbeveiligingsniveau) invulling gegeven te zijn aan: - uitvoeren afhankelijkheidsanalyse; - identificeren en analyseren van bedreigingen; - uitvoeren kwetsbaarheidanalyses. ! BBNP: leidraad geeft een set van maatregelen die in de basis door elk korps en daarmee door de hele Nederlandse politie genomen worden. Het is een minimale set van maatregelen om te voldoen aan de normklassen 'laag' en 'gemiddeld' van de RIP. ! BBNP: Door middel van A&K-analyses zal moeten worden vastgesteld welke maatregelen genomen moeten worden om de normklassen 'hoog' en 'zeer hoog' van de RIP (de meer gevoelige informatie) veilig te stellen.			
8. RIP artikel 6: De korpsbeheerder dient zorg te dragen voor het op systematische wijze vaststellen en operationaliseren van te treffen maatregelen voor informatiebeveiliging. Per informatiesysteem en gemeenschappelijke IT-dienst dient (bovenop het basisbeveiligingsniveau) invulling gegeven te zijn aan: - opstellen informatiebeveiligingsplan (schriftelijke vastlegging beveiligingsmaatregelen); - opstellen van een actieplan ter implementatie van alle beveiligingsmaatregelen; - opstellen van een calamiteitenparagraaf (in het beveiligingsplan) waarvan de effectiviteit periodiek wordt getoetst.			
Interceptiebeveiligingsmaatregelen 1. Artikel 6a RIP: de inrichting van de Interceptiefaciliteiten is de basis voor de uitwerking van de beveiligingsmaatregelen van de tapfaciliteit van het korps (Toelichting wijziging RIP 2004); 2. par. 4 Normstelling: voor de zgn. kritische ruimten in gebruik voor interceptie zijn procedures opgesteld met betrekking tot toegang en autorisatie; 3. par. 14 Normstelling: voor de logische toegang tot en het beheer van het systeem zijn procedures opgesteld.			
9. RIP artikel 3: Het politiekorps dient te beschikken over richtlijnen en procedures voor het melden, registreren en afhandelen van beveiligingsincidenten. ! BBNP: Indien zich een beveiligingsincident voordoet of een vermoeden bestaat dat een incident manifest wordt, is het zaak, teneinde escalatie te voorkomen, dit incident zo spoedig mogelijk aan te pakken. Bronnen waar incidenten gemeld worden, kunnen de administraties zijn van de Bureaus Interne Onderzoeken, de klachtenafhandeling, de helpdesk en de registraties			

Normen (vervolg)	Broninfo	Bevind./ Conclusie	Risico's
C: Informatiebeveiliging; vertaling naar concrete maatregelen, classificatie			
in het kader van de ARBO-wetgeving. Daarnaast kan in het kader van de beveiliging een registratie 'risk management' zijn opgezet.			
Interceptiebeveiligingsmaatregelen 1. Artikel 6a RIP: de inrichting van de Interceptiefaciliteiten is de basis voor de uitwerking van de beveiligingsmaatregelen van de tapfaciliteit van het korps (Toelichting wijziging RIP 2004). 2. par. 6 Normstelling: er is een procedure opgesteld en vastgesteld voor het administreren van incidenten en rapporteren van (potentiële) risico's.			
10. RIP artikel 3: Het bevorderen van security awareness is vertaald naar concrete acties en is opgenomen in het informatiebeveiligingsjaarplan. ! BBNP: Medewerkers van het korps zijn op de hoogte van de afspraken die gelden ten aanzien van de informatiebeveiliging. Medewerkers moeten weten wat, waarom van hen verwacht wordt. Naarmate de medewerkers de achtergrond van beleid en maatregelen beter kennen, is de acceptatie ervan groter. Medewerkers kunnen en zullen alleen correct, dat wil zeggen gewenst gedrag vertonen, indien zij goed geïnformeerd zijn over wat de leiding van het korps van hen verwacht.			
D: Naleving			
11. RIP artikel 3: Periodiek dient het informatiebeveiligingsbeleid aan een beschouwing te worden onderworpen, waarbij met name gelet dient te worden op veranderingen in de organisatie en in de omgeving van de organisatie en incidenten. *(Note: er is een verschuiving gaande van decentrale automatiseringsorganisaties binnen de korpsen naar centrale ICT-diensten-leverancier ISC).* ! Specifiek: Het BBNP dient in de reguliere evaluatiecyclus van de informatie-beveiliging meegenomen te worden. ! Specifiek: De classificatie van informatie dient in de reguliere evaluatiecyclus van de informatiebeveiliging meegenomen te worden. ! Specifiek: De evaluatiecyclus van informatiebeveiliging is verweven in de beleidsevaluatiecyclus en geborgd in het INK-proces.			
12. RIP artikel 6: De korpsbeheerder dient zorg te dragen voor periodieke controle op werking van de informatiebeveiligingsmaatregelen door volgens een vast-gesteld schema te voorzien in een onafhankelijk oordeel over de kwaliteit van de getroffen informatiebeveiligingsmaatregelen van operationele systemen en over het handhaven en naleven daarvan. ! BBNP: Er dient volgens een vastgesteld schema een onafhankelijk oordeel opgesteld te worden over de kwaliteit van de getroffen informatiebeveiligings-maatregelen en over het handhaven en het naleven daarvan.			
Interceptie naleving 1. par. 3 Normstelling: er wordt jaarlijks een interne audit uitgevoerd met betrekking tot de naleving van de Normstelling en de interne uitwerking daarvan; 2. par. 3 Normstelling: er wordt tenminste om de drie jaar een externe audit uitgevoerd met betrekking tot de naleving van de Normstelling en de interne uitwerking daarvan.			

Normen (vervolg)	Broninfo	Bevind./ Conclusie	Risico's
D: Naleving			
13. RIP artikel 6: De korpsbeheerder dient bij systeemverwerving te voorzien in het toetsen op implementatie en werking van maatregelen (conform informatie-beveiligingsplan van het betreffende systeem).			
14. RIP artikel 6: De korpsbeheerder is verantwoordelijk voor de beoordeling van de naleving van alle beveiligingsprocedures binnen de verschillende verantwoordelijkheidsgebieden. Alle verantwoordelijkheidsgebieden binnen het politiekorps dienen regelmatig aan een controle te worden onderworpen, om te waarborgen dat voldaan wordt aan het beveiligingsbeleid en de beveiligingsnormen. ! BBNP: De korpsleiding (laat) periodiek toetsen of de voorgeschreven beveiligingsmaatregelen ook naar behoren functioneren. ! BBNP: In het kader van de beheersbaarheid en de controle op het beleid met betrekking tot de betrouwbaarheid van de informatievoorziening en de maatregelen die in dat kader genomen zijn, is het gewenst dat één keer in een bepaalde periode een algeheel oordeel verkregen wordt met betrekking tot de opzet, bestaan en werking van het informatiebeveiligingsbeleid en de informatiebeveiligingsmaatregelen.			

Bijlage: Vragenlijst Informatiebeveiliging Politie

III

Deze vragenlijst is opgesteld voor het onderzoek van de Inspectie OOV naar informatiebeveiliging bij de Nederlandse politie. Een van de doelstellingen van het onderzoek is om vast te stellen of de korpsen het Stelsel voor Informatiebeveiliging volgens afspraak hebben ingevoerd.
Onderdeel van het onderzoek is deze vragenlijst. Deze dient ingevuld, inclusief aanvullende bijlagen opgestuurd te worden naar de auditors. Vervolgens zal deze tijdens een korpsbezoek besproken worden. Op basis hiervan zal het concept korpsbeeld opgesteld worden.
Bij de vragen is in de kolom documentatie door middel van een @ aangegeven of door het korps relevante documentatie moet worden aangeleverd. Natuurlijk kan ook bij andere vragen relevante documentatie toegevoegd worden. Wilt u de betreffende documentatie invullen in de documentatielijst? In de documentatielijst dient u de titel op te nemen en tevens de versie en datum inwerkingtreding (ondertekening) van het document. In de vragenlijst kunt u vervolgens verwijzen naar het nummer van het document. Eventueel kunt u ook aangeven op welke pagina's de informatie zich bevindt.

Documentatielijst			
Nr.	Titel	Versie	Datum
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

Vragenlijst		
Deel A: Informatiebeveiligingsbeleid	Antwoord politiekorps	Documentatie
1. Heeft de korpsbeheerder een beleidsdocument voor informatiebeveiliging vastgelegd en bekrachtigd?		@
2. Op welke wijze is het beleidsdocument uitgedragen naar de medewerkers?		
3. Hoe is de betrokkenheid van het management verwoord in het beleidsdocument?		@
4. Hoe is in het beleidsdocument de benadering van de organisatie ten aanzien van het omgaan met informatiebeveiliging vastgelegd?		@
5. Hoe is het beheer van de interceptiefaciliteiten belegd in het beleidsdocument?		@
6. Hoe is het beheer van de gegevens (Wet Politieregisters) belegd in het beleidsdocument?		@
7. Hoe is het beveiligingsbeleid C2000 in lijn gebracht met/ingebed in het beleidsdocument?		@
8. Op welke wijze zijn de volgende onderwerpen in het beleidsdocument verwerkt: a. de strategische uitgangspunten en randvoorwaarden en de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningbeleid?		@
b. de organisatie van de beveiligingsfunctie (waaronder verantwoordelijkheden, taken en bevoegdheden)?		@
c. de informatievoorzieningsfaciliteiten in informatiesystemen en de toewijzing van verantwoordelijkheden daarvoor?		@
d. de wijze van vertaling van het beleid naar concrete maatregelen inclusief de wijze van financiering?		@
e. de gemeenschappelijke betrouwbaarheidseisen en maatregelen (de baseline)?		@
f. wijze van melding en afhandeling inbreuken op de informatiebeveiliging?		@
g. evaluatie van het informatiebeveiligingsbeleid en de beoordeling door een onafhankelijke deskundige van de implementatie en de uitvoering van het beleid?		@
h. de wijze waarop het beveiligingsbewustzijn wordt bevorderd?		@
10. Hoe is het Openbaar Ministerie betrokken bij de eisen die gesteld zijn aan de inrichting van de interceptiefaciliteiten?		

Vragenlijst		
Deel B: Informatiebeveiligingsorganisatie	Antwoord politiekorps	Documentatie
11. Hoe is ervoor gezorgd dat de taken, verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging vastgesteld zijn voor de volgende functies? a. de functionaris met eindverantwoordelijkheid voor de informatiebeveiliging binnen het korps		@
b. de verantwoordelijke functionaris voor het coördineren van de informatiebeveiligingsactiviteiten binnen het korps		@
c. de verantwoordelijke functionaris voor de informatiebeveiliging van C2000		@
d. de verantwoordelijke functionaris voor de informatiebeveiliging van de interceptiefaciliteiten		@
e. de operationele executieve functionarissen		@
f. de operationele administratieve functionarissen		@
g. de tactische leidinggevende functionarissen		@
h. de strategisch leidinggevende functionarissen		@
12. Zijn de taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging opgenomen in de functiebeschrijvingen? Het verzoek is om functiebeschrijvingen te overleggen van de functionarissen welke genoemd zijn bij vraag 11 (a tot en met h).		@
13. Uit welke functionarissen bestaat de hulporganisatie voor informatiebeveiliging?		
14. Welke kenniseisen zijn in het opleidingsplan gesteld aan de deskundigheid van de medewerkers in de hulporganisatie voor de informatiebeveiliging?		@
15. Hoe wordt de deskundigheid van de informatiebeveiligingsfunctionaris (IBF-er) op peil gehouden?		
16. Hoe wordt de functiescheiding tussen de beschikkende, uitvoerende, administrerende en controlerende taken bij de inrichting van de informatiebeveiligingsfunctie van de interceptieorganisatie gewaarborgd?		
17. Hoe wordt de functiescheiding tussen de beschikkende, uitvoerende, administrerende en controlerende taken bij de inrichting van de informatiebeveiligingsfunctie van de infodesk gewaarborgd?		
18. Hoe is de samenwerking met het CIP en de ISC vormgegeven zodat beveiligingsafspraken, betrouwbaarheidseisen en -maatregelen en informatiebeveiligingsplannen zo uniform mogelijke zijn?		

Vragenlijst		
Deel B: Informatiebeveiligingsorganisatie (vervolg)	Antwoord politiekorps	Documentatie
19. Welke schriftelijke afspraken heeft het politiekorps gemaakt met het CIP, de ISC, andere overheidsinstanties en leveranciers betreffende de betrouwbaarheid van informatiesystemen en informatie met betrekking tot de volgende aspecten: a. de wijze waarom zal worden voldaan aan de betrouwbaarheidseisen, criteria en normklassen in de bijlage van de RIP?		@
b. de wijze waarop beveiligingsprocessen zijn ingericht zodat storingen en incidenten beperkt blijven binnen de gestelde betrouwbaarheidseisen met betrekking tot beschikbaarheid, exclusiviteit en integriteit?		@
c. de wijze waarop over de uitvoering van de beveiligingsprocessen en -incidenten wordt gerapporteerd?		@
d. de wijze waarop (onafhankelijke) zekerheid wordt verkregen over de betrouwbaarheid van de informatiesystemen en de informatie (door een TPM, EDP-audit, etc.)?		@
20. Hoe is het contractbeheer ingericht om te waarborgen dat wordt voldoen aan de in vraag 19 genoemde aspecten?		@
21. Is de samenwerking met het KLPD, het CIP, de ISC en andere korpsen met betrekking tot de interceptiefaciliteit vastgelegd in afspraken over beveiligingsmaatregelen met betrekking tot de gegevensuitwisseling?		@

Vragenlijst		
Deel C: Informatiebeveiligingsmaatregelen	Antwoord politiekorps	Documentatie
22. Is er een totaaloverzicht met alle informatie-systemen/gemeenschappelijke IT-diensten?		@
23. Hoe wordt dit totaaloverzicht onderhouden?		@
24. Is voor elk(e) informatiesysteem/IT-dienst een verantwoordelijke manager aangewezen?		@
25. Hoe is ervoor zorggedragen dat de gehanteerde beveiligingsclassificaties de landelijk afgestemde normklassen en criteria bevatten?		@
26. Wat is de status van het implementeren van de maatregelen uit het BBNP bij het korps en waaruit blijkt dit?		@
27. Wanneer zijn alle maatregelen uit het BBNP geïmplementeerd door het korps?		
28. Heeft het korps een implementatieplan met betrekking tot het BBNP opgesteld aan de hand van het Wegingsinstrument?		@
29. Is voor alle informatiesystemen met normklassen 'hoog' en 'zeer hoog' een A&K-analyse uitgevoerd?		@
30. Hoe zijn de resultaten van de A&K-analyse verwerkt?		@
31. Waaruit bestaan de interceptiefaciliteiten van het korps?		@
32. Hoe is rekening gehouden met de Normstelling Inrichting Interceptiefaciliteiten bij de uitwerking van de beveiligingsmaatregelen voor de interceptiefaciliteit?		@
33. Hoe is invulling gegeven aan paragraaf 4 van de Normstelling Inrichting Interceptiefaciliteiten met betrekking tot de fysieke toegangscontrole tot gebouwen en terreinen?		@
34. Hoe is invulling gegeven aan paragraaf 14 van de Normstelling Inrichting Interceptiefaciliteiten met betrekking tot het beheer en de logische toegangsbeveiliging?		@
35. Heeft het korps richtlijnen en procedures voor het melden, registreren en afhandelen van beveiligingsincidenten?		@
36. Hoe wordt ervoor zorggedragen dat medewerkers beveiligingsincidenten kunnen herkennen en bekend zijn met de te volgen handelswijze?		
37. Welke informatie wordt opgenomen in de incidentenregistratie?		@
38. Hoe wordt ervoor zorggedragen dat zwakke plekken in de beveiliging van de interceptie-faciliteit gemeld worden?		@
39. Hoe wordt de security awareness van de medewerkers bevorderd?		@
40. Zijn voor het bevorderen van de security awareness van de medewerkers concrete acties opgenomen in het informatiebeveiligingsjaarplan?		@

Vragenlijst		
Deel D: Naleving	Antwoord politiekorps	Documentatie
41. Hoe wordt ervoor gezorgd dat het informatiebeveiligingsbeleid en de classificatie van informatie up-to-date is?		
42. Hoe is de evaluatiecyclus van de informatiebeveiliging verweven in de beleidsevaluatiecyclus en geborgd in het INK-proces?		@
43. Hoe zijn in het afgelopen jaar door een onafhankelijke deskundige de volgende objecten beoordeeld/getest: a. de maatregelen gericht op functiescheiding voor wat betreft opzet, bestaan en werking?		@
b. de technische infrastructuur op inbraakbestendigheid?		@
c. de opzet, bestaan en werking van de logische toegangsbeveiliging?		@
d. de ingestelde parameters van de besturingssystemen op de mate waarin deze instellingen overeen komen met de van tevoren vastgestelde gewenste instellingen?		@
44. Is in de afgelopen vier jaar een externe audit uitgevoerd op de opzet, bestaan en werking van het BBNP?		@
45. Is in het afgelopen jaar een interne audit uitgevoerd met betrekking tot de naleving van de Normstelling Inrichting Interceptiefaciliteiten en de interne uitwerking daarvan?		@
46. Is in de afgelopen drie jaar een externe audit uitgevoerd met betrekking tot de naleving van de Normstelling Inrichting Interceptiefaciliteiten en de interne uitwerking daarvan?		@
47. Hoe wordt bij systeemverwerving op voorhand rekening gehouden met de verplichting om de implementatie en werking van maatregelen te toetsen?		
48. Hoe wordt getoetst op de implementatie en de werking van maatregelen na systeemverwerving?		
Aanvullende vragen		
49. Wat is de mening van het korps over de aansluiting van het Stelsel voor Informatiebeveiliging (RIP, BBNP, et cetera) op de huidige organisatie van informatiebeveiliging binnen de Nederlandse politie?		
50. Wat is de mening van het korps over de actualiteit van het BBNP?		
51. Welke samenwerkingsvormen zijn er op het gebied van informatiebeveiliging tussen de korpsen?		

IV Bijlage: Korpsbeelden

Groningen
Fryslân
Drenthe
IJsselland
Twente
Noord- en Oost-Gelderland
Gelderland-Midden
Gelderland-Zuid
Utrecht
Noord-Holland Noord
Zaanstreek-Waterland
Kennemerland
Amsterdam-Amstelland
Gooi en Vechtstreek
Haaglanden
Hollands Midden
Rotterdam-Rijnmond
Zuid-Holland-Zuid
Zeeland
Midden- en West-Brabant
Brabant-Noord
Brabant-Zuid-Oost
Limburg-Noord
Limburg-Zuid
Flevoland
Korps Landelijke Politiediensten

De korpsbeelden zijn opgesteld door PricewaterhouseCoopers (PwC) en voor hoor en wederhoor voorgelegd aan de korpsen. De korpsen hebben de gelegenheid gehad om aan te geven of er feitelijke onjuistheden in het korpsbeeld voorkomen. In dat geval is het korpsbeeld aangepast.
De peildatum voor de korpsbeelden is het derde kwartaal van 2006.

KORPSBEELD GRONINGEN

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Groningen grotendeels geïmplementeerd. Met name de volledige implementatie van de maatregelen uit het BBNP verdient nog de aandacht.

INFORMATIEBEVEILIGINGSBELEID

Het korps Groningen heeft in 1997 reeds een informatiebeveiligingsbeleid vastgelegd, welke vervolgens regelmatig ge-update is. In dit beleid wordt aandacht besteed aan de meeste aandachtspunten zoals genoemd in de RIP.
Voor de interceptiefaciliteiten wordt gebruik gemaakt van de voorzieningen van het ULI. Het korps Groningen was het laatste regiokorps in Noord-Nederland dat overgegaan is op het ULI in verband met kinderziektes en het voldoen aan de ULI gestelde beveiligingseisen. Voorafgaand aan de overgang heeft het korps een quick-scan uitgevoerd.
Voor C2000 is een Beveiligings Informatie Pakket GMG opgesteld, dat gelieerd is aan het informatiebeveiligingsbeleid van het korps. Dit informatiebeveiligingsplan is door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties goedgekeurd en heeft gediend als voorbeeld voor een aantal andere korpsen.

INFORMATIEBEVEILIGINGSORGANISATIE

De verantwoordelijke voor informatiebeveiliging is de korpschef, daartoe gemandateerd door de korpsbeheerder. De portefeuillehouder informatiebeveiliging is het hoofd Dienst Bedrijfsvoering. De coördinatie van de activiteiten op het gebied van informatiebeveiliging vindt plaats door het hoofd Integriteit & Bedrijfsveiligheid. Daarnaast heeft

het korps een hulporganisatie informatiebeveiliging welke bestaat uit twee informatiebeveiligingsfunctionarissen, de taakaccenthouders security en de Informatie Management Adviseurs.
Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn integraal vastgelegd in de functieomschrijvingen van de diverse functionarissen.
Met het ISC vindt dagelijkse samenwerking plaats, waarbij volgens het korps begrip is voor ieders verantwoordelijkheid met betrekking tot veiligheid en beveiliging. Verder vindt tevens overleg plaats met de IBF-ers van de drie noordelijke regio's als ook met de IBF-ers van het ISC-verzorgingsgebied Noordoost. Bij dit laatste overleg is ook het ISC en het CIP vertegenwoordigd.
De medewerkers van de hulporganisatie zijn gecertificeerd conform het Examenreglement Politieopleidingen 2001. Nieuwe opleidingen worden enkel op ad hoc basis gevolgd.
Voor zowel de interceptiefaciliteiten als de Infodesk is de functiescheiding op een adequate wijze ingericht.
Met ISC Noordoost zijn nog geen afspraken gemaakt over de betrouwbaarheid van informatiesystemen en de beveiliging van informatie. De oude SLA en DAP moeten nog gewijzigd worden in verband met de overgang naar het ISC. Hiervoor is door een projectgroep een Plan van Aanpak opgesteld, welke begin 2007 waarschijnlijk zal resulteren in een nieuwe SLA en DAP. Tevens vindt hierover ook terugkoppeling plaats door middel van maandelijkse rapportages over beveiligingsprocessen en -incidenten. Deze maandrapportages worden gehinderd door onduidelijkheid met betrekking tot incidenten. Tevens heeft het korps voor de interceptiefaciliteiten afspraken gemaakt met het KLPD.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps heeft een overzicht met informatiesystemen/gemeenschappelijke ICT-diensten, dat bijgehouden wordt in de CMDB van het ISC. Een werkgroep die ingesteld is door de CIO en de service liaison zijn verantwoordelijk voor het actueel houden van dit overzicht. De eigenaren zijn ook vastgesteld en in oktober 2006 stond een nieuw voorstel hiervoor op de agenda van het Regionaal Management Overleg.
Het korps heeft niet alle maatregelen uit het BBNP geïmplementeerd. Voor de implementatie wordt aangesloten bij de dagelijkse praktijk en daarnaast zijn de maatregelen in de nulmeting geprioriteerd.
Het korps Groningen heeft voor een groot deel van de informatiesystemen geen A&K-analyses uitgevoerd. Van wel uitgevoerde A&K-analyses zijn de resultaten daadwerkelijk geïmplementeerd. Bij de uitwerking van de interceptiefaciliteiten is door het korps de Normstelling Inrichting Interceptiefaciliteiten gehanteerd.
Het korps heeft procedures voor beveiligingsincidenten, maar deze moeten aangepast worden in verband met de overgang naar ISC Noordoost. Tevens is de voorlichting naar de medewerkers niet voldoende adequaat, waardoor niet alle incidenten als

beveiligingsincident onderkend zullen worden.
De security awareness van de medewerkers wordt op diverse manieren bevorderd, zoals opgenomen in het beveiligingsplan, projectvoorstellen en projectplannen.

NALEVING

Informatiebeveiliging is door het korps opgenomen in de evaluatiecyclus. Hierdoor wordt elk half jaar door de korpsleiding gestuurd op de resultaten.
Tot op heden zijn op deelgebieden audits uitgevoerd bij het korps Groningen. Alleen met betrekking tot de Normstelling Inrichting Interceptiefaciliteiten is een interne scan (quick-scan) uitgevoerd met betrekking tot de stand van zaken bij de overgang naar het toenmalige LIO.

KORPSBEELD FRYSLÂN

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Fryslân ten dele geïmplementeerd. Met name de implementatie van de maatregelen uit het BBNP binnen het korps verdient nog de aandacht.

INFORMATIEBEVEILIGINGSBELEID

Het korps Fryslân heeft een informatiebeveiligingsbeleid, dat per juli 2006 gedurende twee jaar in werking treedt. In dit beleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
In het informatiebeveiligingsbeleid wordt verwezen naar de voor de interceptiefaciliteiten op te stellen voorschriften. Deze voorschriften zijn inmiddels vastgelegd in het protocol interceptieruimten politie Fryslân, dat in nauw overleg met het Openbaar Ministerie tot stand is gekomen.
In het informatiebeveiligingsbeleid is de verantwoordelijkheid voor C2000 belegd bij de chef Meldkamer. Dit beleid is nader uitgewerkt in het beveiligingsplan C2000 en het beveiligingsplan randapparatuur C2000.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging is de korpsbeheerder c.q. de korpschef. Van de korpsleiding is een lid aangewezen als portefeuillehouder informatiebeveiliging (CIO). De coördinatie van de activiteiten op het gebied van informatiebeveiliging vindt plaats door de informatiebeveiligingsfunctionaris. De informatiebeveiligingsfunctionaris (IBF) is één van de twee adviseurs op het gebied van beveiliging binnen het cluster Informatiemanagement (IM). De andere adviseur richt

zich meer op de fysieke beveiliging. De IBF, de beveiligingsadviseur en de CIO vormen gezamenlijk de hulporganisatie informatiebeveiliging. De taakaccenthoudersstructuur wordt momenteel ingericht, waarbij de taakaccenten informatiebeveiliging waarschijnlijk toegewezen zullen worden aan de operationeel leidinggevenden.
Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn alleen vastgelegd voor de IBF. Het korps Fryslân maakt gebruik van generieke functiebeschrijvingen, waarbij specifieke componenten uitgewerkt worden in competentieprofielen.
Er is frequent contact tussen de beveiligingsfunctionarissen van de regio enerzijds en het ISC en het CIP anderzijds. Dit overleg vindt op informele basis plaats met de IBF-ers van de drie noordelijke regio's en op formele basis plaats met de IBF-ers van de acht noordelijke regio's die gebruikmaken van de diensten van VZG NO.
Kenniseisen zijn vastgelegd in de competentieprofielen door middel van opleidingsniveau en functiegerichte competenties. De deskundigheid van de IBF wordt op peil gehouden door middel van kennisuitwisseling via het landelijke IBF-netwerk en vakliteratuur.
Voor de interceptiefaciliteiten is de functiescheiding adequaat vastgelegd en ingericht. Voor de Infodesk is de functiescheiding niet expliciet vastgelegd.
Met ISC-Noordoost zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van de Basisdienstverlening ISC-Noordoost, het DAP, de SLA en de PDC. Deze documenten worden momenteel geactualiseerd naar aanleiding van de nieuwe situatie. Tevens heeft het korps voor de interceptiefaciliteiten afspraken gemaakt in een DVO, een NOK en SLA met het KLPD.

INFORMATIEBEVEILIGINGSMAATREGELEN

In de PDC is een overzicht met informatiesystemen/gemeenschappelijke ICT-diensten opgenomen, dat bijgehouden wordt door de regionale service liaison via de wijzigingsprocedure. Tevens wordt gebruik gemaakt van de lijst met toegestane systemen. In het informatiebeveiligingsbeleid is de verantwoordelijkheid voor een gegevensverzameling, informatiesysteem of IT dienst belegd bij de desbetreffende proceseigenaar.
Het korps voert de implementatie van het BBNP per cluster/taakveld uit, waarbij prioritering plaatsvindt op basis van een risicoafweging in samenhang met de actuele dreigingen. Het draagvlak van de maatregelen wordt vergroot door in te spelen op de actualiteit. Het korps Fryslân heeft geen inzicht in hoeverre de maatregelen uit het BBNP geïmplementeerd zijn, omdat er geen recente meting van de huidige status van de implementatie is uitgevoerd en omdat het voor het korps moeilijk is om de status van de implementatie vast te stellen voor de maatregelen die nu door het ISC en het CIP worden uitgevoerd.
Het korps Fryslân heeft geen A&K-analyses uitgevoerd. Bij de inrichting van het interceptieproces is door het korps de Normstelling Inrichting Interceptiefaciliteiten als

uitgangspunt gehanteerd. De diverse maatregelen zijn opgenomen in het protocol interceptieruimten en tevens geïmplementeerd.
Het korps heeft een procedure voor beveiligingsincidenten opgenomen in het informatiebeveiligingsbeleid. Alle beveiligingsincidenten worden geregistreerd door de informatiebeveiligingsfunctionaris.
De security awareness van de medewerkers wordt op diverse manieren bevorderd, zoals publicaties, voorlichtingssessies, opleidingen en individuele gesprekken. Dit is geen onderdeel van een informatiebeveiligingsjaarplan.

NALEVING

Informatiebeveiliging is door het korps nog niet opgenomen in de evaluatiecyclus. Tot op heden is alleen in 2004 een interne audit uitgevoerd op de naleving van de Normstelling Inrichting Interceptiefaciliteiten.

KORPSBEELD DRENTHE

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Drenthe onvoldoende geïmplementeerd. Het korps is momenteel bezig om dit stelsel te implementeren.

INFORMATIEBEVEILIGINGSBELEID

Het korps Drenthe heeft het informatiebeveiligingsbeleid vastgelegd in een nog niet vastgestelde notitie. In dit beleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
Voor de interceptiefaciliteiten wordt gebruik gemaakt van de voorzieningen van het ULI. Informatiebeveiliging is voor de interceptiefaciliteiten nog niet uitgewerkt. Het voornemen is om dit in de toekomst als deelplan van het informatiebeveiligingsplan uit te werken.
Voor C2000 is gezamenlijk met de partners een beveiligingsbeleidsplan opgesteld. In 2006 heeft hiervan een update plaatsgevonden en het geactualiseerde beveiligingsplan is momenteel gereed voor besluitvorming.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging is de korpschef. De korpschef mandateert zijn taken en verantwoordelijkheden aan de portefeuillehouder informatiebeveiliging (hoofd O&I). De portefeuillehouder wordt bijgestaan door de informatiebeveiligingsfunctionaris die verantwoordelijk is voor de coördinatie van de activiteiten op het gebied van informatiebeveiliging, de ontwikkeling van het informatiebeveiligingsbeleid en de vertaling van het beleid naar plannen en de controle op het gebied van informatiebeveiliging. De informatiebeveiligingsfunctionaris is een

taakonderdeel van de functioneel beheerder Kantoorautomatisering. Het korps zal nog evalueren of de informatiebeveiligingsfunctionaris als aparte functie gepositioneerd dient te worden binnen het korps.
Taken, bevoegdheden en verantwoordelijkheden zijn niet integraal vastgelegd. De enige uitzondering hierop is de concept functiebeschrijving voor de informatiebeveiligingsfunctionaris.
Met het ISC vindt regelmatig overleg plaats op drie verschillende niveaus, namelijk de IBF-ers met betrekking informatiebeveiliging, de CIO's op strategisch niveau en de service liaisons op operationeel niveau.
De huidige informatiebeveiligingsfunctionaris zal de basisopleiding informatiebeveiliging gaan volgen. Daarnaast is nog geen concreet opleidingsplan voor de hulporganisatie geformuleerd. De informatiebeveiligingsfunctionaris draagt door middel van opleidingen, overlegstructuren en literatuur zorg voor het op peil houden van zijn deskundigheid.
Voor de interceptiefaciliteiten is onduidelijk of de functiescheiding afdoende is vastgelegd. De functiescheiding bij de Infodesk is goed geregeld door middel van scheiding tussen aanvrager, beoordelaar, uitvoerder en toezichthouder.
Met ISC Noordoost zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie. Tevens vindt hierover ook terugkoppeling plaats door middel van rapportages, welke zich nog in een ontwikkelstadium bevinden. Tevens heeft het korps voor de interceptiefaciliteiten afspraken gemaakt met het ULI.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps heeft een overzicht met informatiesystemen/gemeenschappelijke ICT-diensten, dat door het ISC opgesteld is en onderhouden wordt. Voor eigenaren heeft het korps een notitie houderschap informatiesystemen en gemeenschappelijke (IT) diensten. Deze notitie is verouderd en momenteel is het korps bezig om proceseigenaren aan te wijzen, welke ook eigenaar worden van de binnen het proces in gebruik zijnde informatiesystemen.
Het korps heeft geen inzicht in de mate waarin de maatregelen uit het BBNP zijn geïmplementeerd. Het korps heeft momenteel de focus gericht op het formaliseren van het informatiebeveiligingsplan en het opstellen van een communicatieplan. Aan het einde van 2006 zou gestart worden met het wegen van de maatregelen uit het BBNP om de volgorde van implementatie te bepalen.
Het korps Drenthe heeft nog geen A&K-analyses uitgevoerd. Momenteel is het plan om gezamenlijk met ISC-NO een A&K-analyse uit te voeren op BPS en RBS.
Op basis van het informatiebeveiligingsbeleid zal voorzien gaan worden in een richtlijn/procedure met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten.
De security awareness van de medewerkers wordt momenteel nauwelijks bevorderd.

De informatiebeveiligingsfunctionaris is momenteel bezig om hiervoor een communicatieplan op te stellen. Tevens zal hieraan ook aandacht besteed worden in het jaarplan, welke opgesteld zal worden na de vaststelling van het informatiebeveiligingsbeleid.

NALEVING

Informatiebeveiliging is door het korps nog niet verweven in het INK-proces en daardoor nog niet geborgd. Dit heeft ermee te maken dat het informatiebeveiligingsbeleid pas weer recent opgestart is.
Tot op heden zijn nog geen interne audits uitgevoerd met betrekking tot de informatiebeveiliging (van de interceptiefaciliteiten) binnen het korps Drenthe. Wel is in 2002 door een externe auditor beoordeeld of in opzet en deels in bestaan en werking voldaan werd aan het RIP. De conclusie was dat niet voldaan werd aan het RIP. Tevens is in 2004 een externe audit uitgevoerd op de interceptiefaciliteiten, waaruit bleek dat niet voldaan werd aan de Normstelling Inrichting Interceptiefaciliteiten. Voor beide audits is onbekend welke acties ondernomen zijn naar aanleiding van de conclusie.

KORPS IJSSELLAND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps IJsselland grotendeels geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps IJsselland heeft een informatiebeveiligingsbeleid, welke momenteel geëvalueerd en herzien wordt. De bedoeling is om te komen tot één beleid voor alle politieregio's in het verzorgingsgebied Noordoost. In dit beleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
Het beheer van de interceptiefaciliteiten is belegd in het informatiebeveiligingsbeleid. Dit beheer is verder uitgewerkt in een informatiebeveiligingsplan en een implementatieplan. Tijdens het implementatieproject is het Openbaar Ministerie betrokken geweest. Voor C2000 zijn informatiebeveiligingsplannen opgesteld, waarin het informatiebeveiligingsbeleid kort aangestipt wordt.

INFORMATIEBEVEILIGINGSORGANISATIE

De korpschef heeft de directeur Bedrijfsvoering aangewezen als portefeuillehouder Integrale Beveiliging. De portefeuillehouder is eindverantwoordelijk voor de organisatorische, fysieke en personele beveiliging van het korps in brede zin, wat binnen het korps wordt aangeduid met 'interne veiligheid'. De portefeuillehouder heeft aspecten van informatiebeveiliging gedelegeerd aan de CIO. De senior beveiligingsfunctionaris is als IBF verantwoordelijk voor de coördinatie van de informatiebeveiliging.
De hulporganisatie voor informatiebeveiliging wordt door het korps als gedateerd beschouwd en wordt als niet noodzakelijk gezien. De informatiebeveiligingsorganisatie wordt momenteel in de lijn gebracht door de lijnverantwoordelijkheid te geven voor de

interne veiligheid binnen het korps. De IBF faciliteert de lijn bij het opstellen van beveiligingsplannen en het sturen op de uitvoering van deze plannen.
Taken, bevoegdheden en verantwoordelijkheden zijn deels vastgelegd. Voor de medewerkers die direct betrokken zijn bij informatiebeveiliging zijn de taken, verantwoordelijkheden en bevoegdheden vastgelegd in de functiebeschrijvingen.
De korpsen Twente, IJsseland en Noord-Oost Gelderland werken samen op het gebied van informatiebeveiliging in het samenwerkingsverband SATIJN. Daarnaast heeft de CIO op regelmatige basis overleg met de CIO's van de acht Noordelijke korpsen, met het ISC en het CIP. De IBF overlegt op verschillende niveaus met het ISC, bijvoorbeeld in het platform IBF-NO, waarin naast de IBF-ers van de Noordelijke korpsen ook de IBF-er van ISC-NO en een CIO, die als linking-pin optreedt naar het Noordelijke CIO-overleg, participeren. Daarnaast wordt zowel met als zonder service liaison regelmatig overleg gevoerd op diverse niveaus met medewerkers van ISC-NO.
De IBF draagt door middel van deelname aan landelijke projecten, seminars, literatuur en contacten met deskundigen zorg voor het op peil houden van zijn deskundigheid.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk zijn adequaat ingericht. Dit wordt regelmatig gecontroleerd door de IBF.
Met ISC Noordoost zijn afspraken gemaakt en vastgelegd in een DAP en SLA met betrekking tot de dienstverlening door het ISC. Deze documenten worden momenteel geleidelijk herzien in het kader van het project concentratie en consolidatie. Tevens vindt wekelijks rapportage plaats over storingen, problemen, wijzigingen en wijzigingsverzoeken aan de service liaison. In het kader van de interceptiefaciliteiten zijn afspraken gemaakt met het KLPD en het CIP.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps heeft een overzicht met applicaties, welke bijgehouden wordt door de afdeling Informatie Management. Applicaties zijn aan de hand van de processen toebedeeld aan de proceseigenaren.
Het korps heeft zo'n 71% van de maatregelen uit het BBNP geïmplementeerd. Bij de implementatie van de maatregelen is niet uitgegaan van een Wegingsinstrument, maar van een quick-scan 2004 welke afgeleid is van het Wegingsinstrument. Dit heeft geresulteerd in een prioriteitenmatrix aan de hand waarvan implementatie plaatsvindt.
Het korps IJsselland heeft geen A&K-analyses uitgevoerd, maar risicoanalyses welke gebaseerd zijn op de methode van de A&K-analyse. Dit heeft plaatsgevonden voor een groot aantal onderwerpen met een grote diversiteit. Deze resultaten zijn vervolgens verwerkt in beleidsnotities/voorstellen. De Normstelling Inrichting Interceptiefaciliteiten is door het korps verwerkt in een implementatieplan.
Het korps heeft een protocol 'Melden en afhandelen beveiligingsincidenten', welke ook van toepassing is voor de interceptiefaciliteiten.
Het communicatietraject (structurele voorlichting middels bestaande kanalen zoals de Korpskrant en Intranet) is volop punt van aandacht, ook op strategisch niveau waar het

deel uitmaakt van de RMT-agenda. Security awareness is in volle gang. Vanuit het Bureau Inlichtingen en Veiligheid (waar onder meer Interne Veiligheid en Bureau Interne Onderzoeken (BIO) zijn georganiseerd) worden structureel presentaties in de teams (inclusief de BRNON) gegeven door de senior beveiligingsfunctionaris en het hoofd BIO; veelal in combinatie met een presentatie over Interne Veiligheid en een presentatie vanuit het Bureau Interne Onderzoeken. Daarnaast zal in 2007 een bewustwordingscampagne met betrekking tot informatiebeveiliging gevoerd gaan worden.

NALEVING

Informatiebeveiliging is door het korps geborgd in de marap-cyclus. In 2003 is een quick-scan uitgevoerd door een externe auditor met betrekking tot de opzet, bestaan en werking van het BBNP. Tevens is in 2006 een interne audit uitgevoerd op de naleving van de Normstelling Inrichting Interceptiefaciliteiten.

KORPSBEELD TWENTE

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Twente nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Twente heeft een informatiebeveiligingsbeleid, welke op 16 augustus 2006 in het Regionaal Management Team (RMT) goedgekeurd is. In dit beleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
Voor de interceptiefaciliteiten wordt gebruik gemaakt van de voorzieningen van het ULI. Het inrichten van de interceptiefaciliteiten conform de Normstelling Inrichting Interceptiefaciliteiten heeft nog niet plaatsgevonden. Het formuleren van de eisen bevindt zich momenteel in de ontwikkelfase.
Voor C2000 is een informatiebeveiligingsplan opgesteld, waarin het informatiebeveiligingsbeleid kort aangestipt wordt. Dit plan is gezamenlijk opgesteld met de partners binnen C2000.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging is de plaatsvervangend korpschef. De informatiebeveiligingsfunctionaris is verantwoordelijk voor de coördinatie van de informatiebeveiliging. Deze valt qua lijnverantwoordelijkheid onder de CIO (hoofd Strategie en Beleid), waardoor beveiligingsaspecten in ruime zin opgepakt kunnen worden. Conform het beleid zullen taakaccenthouders aangewezen worden om te ondersteunen bij het uitwerken van het informatiebeveiligingsbeleid. Deze hulporganisatie is echter nog niet ingericht.

Taken, bevoegdheden en verantwoordelijkheden zijn nog niet integraal vastgelegd. De enige uitzondering hierop is de functiebeschrijving voor de adviseur Informatiebeveiliging.
De portefeuillehouder (plaatsvervangend korpschef) en de informatiebeveiligingsfunctionaris hebben direct overleg.

Doordat de informatiebeveiligingsfunctionaris onder lijnverantwoordelijkheid van de CIO valt, worden beveiligingsaspecten in ruime zin opgepakt. Het gevraagd en ongevraagd adviseren functioneert hierbij volgens het korps voldoende.
Met het CIP vindt geregeld overleg plaats over informatiebeveiliging (bijvoorbeeld bij het ontwikkelen van beleid) bijvoorbeeld tijdens het landelijk overleg tussen de IBF-ers en het CIP. Met betrekking tot het ISC vindt overleg plaats tussen de IBF-er van het ISC NO en de IBF-er van het korps. Daarnaast zijn diverse afspraken met het ISC schriftelijk bekrachtigd.
Het korps Twente probeert beveiliging integraal te benaderen. Dit blijkt bijvoorbeeld uit het opgestelde beleid, welke algemeen op beveiliging is gericht en niet enkel op informatiebeveiliging.
Het opleidingsplan voor de hulporganisatie is nog niet geformuleerd. De informatiebeveiligingsfunctionaris draagt door middel van opleidingen, congressen, seminars, literatuur en contacten met deskundigen zorg voor het op peil houden van zijn deskundigheid.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk zijn niet vastgelegd. Voor de interceptiefaciliteiten zullen deze nog vastgelegd worden in een protocol.
Met ISC Noordoost zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en expliciet over de beveiliging van informatie in DAP, SLA en specifieke afspraken. Tevens vindt hierover ook terugkoppeling plaats door middel van rapportages. In het verleden zijn afspraken gemaakt over gegevensuitwisseling met het KLPD. Landelijk wordt momenteel actie ondernomen om aanvullende afspraken te maken. Voor de interceptiefaciliteiten zijn nog geen aanvullende afspraken gemaakt. Hierop wordt momenteel landelijk actie ondernomen.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps heeft een overzicht met informatiesystemen/gemeenschappelijke ICT-diensten (indeling systeemeigenaren naar RBP-model), waarin zowel de proceseigenaren opgenomen zijn als de beheerders van onderdelen. Een adviseur van PIO (Proces en Informatiemanagement Ondersteuning) heeft een taakaccent om dit overzicht te onderhouden.
Het korps heeft de maatregelen uit het BBNP nog niet allemaal geïmplementeerd. Bij de implementatie van de resterende maatregelen zal uitgegaan worden van risicomanagement in plaats van het Wegingsinstrument, omdat deze volgens het korps niet

aansluit bij de beleveniswereld van de medewerkers. Naar aanleiding van een audit op de informatiebeveiliging in 2004 door een externe auditor, werkt men momenteel aan het implementeren van de aanbevelingen die naar aanleiding van deze audit zijn gedaan.
Het korps Twente heeft nog geen A&K-analyses uitgevoerd met uitzondering van RBS, waarvoor momenteel een A&K-analyse uitgevoerd wordt. De Normstelling Inrichting Interceptiefaciliteiten wordt door het korps momenteel uitgewerkt in een protocol.
Op basis van het informatiebeveiligingsbeleid zal voorzien gaan worden in een richtlijn/procedure met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten.
Het korps onderkent dat de security awareness van de medewerkers nog verder bevorderd moet worden. Hiervoor is momenteel nog geen structurele aandacht, maar informatie wordt bijvoorbeeld aangereikt via het intranet. Informatie wordt bijvoorbeeld verstrekt na het bekend worden van incidenten (ook uit andere regio's).

NALEVING

Informatiebeveiliging is door het korps nog niet verweven in het INK-proces en daardoor nog niet geborgd. Tot op heden zijn nog geen interne audits uitgevoerd met betrekking tot de informatiebeveiliging binnen het korps Twente. Wel is in 2004 door een auditor een externe audit uitgevoerd op de informatiebeveiliging binnen het korps Twente. De aanbevelingen uit deze audit worden door het korps uitgevoerd.

KORPSBEELD NOORD- EN OOST-GELDERLAND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Noord- en Oost-Gelderland nagenoeg geheel geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Noord- en Oost-Gelderland heeft een informatiebeveiligingsbeleid, wat is besproken binnen de driehoek en op 9 september 2004 door de korpsbeheerder is ondertekend. Bij de totstandkoming van dit beleid zijn de uitkomsten meegenomen van de externe audit op het BBNP die eind 2003 is uitgevoerd. In dit beleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
In het informatiebeveiligingsbeleid wordt verwezen naar de interceptiefaciliteiten. Dit heeft te maken met de vroegtijdige participatie van deze regio in het toenmalige LIO. Op het moment van het vaststellen van het informatiebeveiligingsbeleid waren de beveiligingseisen aan de interceptiefaciliteiten nog niet duidelijk. Inmiddels is voor de interceptiefaciliteiten het proces protocol interceptie opgesteld, welke besproken is met het Openbaar Ministerie.
De verantwoordelijkheden met betrekking tot C2000 worden toegelicht in het informatiebeveiligingsbeleid. Het beveiligingsbeleid C2000 is in lijn gebracht met het informatiebeveiligingsbeleid door participatie van de regionale informatiebeveiligings-functionaris bij de ontwikkeling van dit beleid.
Het korps zal de komende tijd informatiebeveiliging steeds meer vanuit het 'control'-perspectief gaan aansturen, waarmee de beweging is ingezet om het accent van de primair planmatige naar de controlerende benadering van informatiebeveiliging te verleggen.

INFORMATIEBEVEILIGINGSORGANISATIE

Het korps beschikt over een actieve en werkende hulporganisatie. De korpschef is verantwoordelijk voor informatiebeveiliging. De portefeuillehouder informatiebeveiliging is de divisiechef Bedrijfsvoering. De informatiebeveiligingsfunctionaris is verantwoordelijk voor de coördinatie van de informatiebeveiliging. De hulporganisatie voor de informatiebeveiliging bestaat daarmee uit de korpsbeheerder (eindverantwoordelijke), de korpschef (verantwoordelijke), de portefeuillehouder, de informatiebeveiligingsfunctionaris en de taakaccenthouders informatiebeveiliging (meestal hoofden Bedrijfsbureaus).
Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn door het korps Noord- en Oost-Gelderland niet opgenomen in de functiebeschrijvingen. Dit is een bewuste keuze, waarbij de algemene beveiligingsvoorschriften gekoppeld zijn aan de algemene functies en specifieke beveiligingsvoorschriften aan de vertrouwensfuncties.
De CIO (hoofd afdeling Informatie Management) is verantwoordelijk voor het vaststellen van de betrouwbaarheidseisen die op contractbasis gesteld moeten worden aan externe organisatie die een rol spelen in het informatievoorzieningsproces van het korps, zoals het ISC en de ULI. De verantwoordelijkheid voor de operationele afstemming met het ISC is belegd bij de service liaison.
Voor de hulporganisatie zijn geen formele kenniseisen gesteld. Met betrekking tot de taakaccenthouders Informatiebeveiliging zijn wel opleidingseisen gesteld, waaraan het korps momenteel invulling aan geeft.
De functiescheiding met betrekking tot de interceptiefaciliteiten is adequaat geborgd. Met betrekking tot de Infodesk is de functiescheiding niet maximaal geborgd vanwege het ontbreken van systeemmogelijkheden en de procesinrichting bij de Infodesk.
Het korps Noord- en Oost-Gelderland heeft basis- en specifieke afspraken met het ISC vastgelegd, gebaseerd op de PDC. Verder zijn afspraken uitgewerkt in procedures en vastgelegd in het DAP. De SLA wordt momenteel herzien, waarna deze net zoals de huidige afspraken door de service liaison in beheer genomen zal worden. Voor de interceptiefaciliteiten zijn op landelijk niveau afspraken gemaakt.

INFORMATIEBEVEILIGINGSMAATREGELEN

In de PDC met het ISC is een overzicht met informatiesystemen/gemeenschappelijke ICT-diensten opgenomen, welke door het ISC onderhouden wordt. Tevens heeft het korps in de gebruikersorganisatie systeemeigenaren aangewezen.
Het korps heeft de maatregelen uit het BBNP nog niet allemaal geïmplementeerd. In 2003 heeft een externe audit met betrekking tot het BBNP plaatsgevonden, welke geresulteerd heeft in een informatiebeveiligingsplan 2004 met een plan van aanpak voor de issues met een hoge prioriteit. De issues met een prioriteit midden en laag zijn in een later plan van aanpak opgenomen. Verder heeft iedere operationele eenheid na

het uitvoeren van een zelf ontwikkelde wegingsmethodiek (ontwikkeld op basis van het wegingsinstrument van het Expertise Centrum Informatiebeveiliging Politie) een beveiligingsplan opgesteld in relatie tot de BBNP-maatregelen. Regelmatig worden zelfevaluaties uitgevoerd door de taakaccenthouders op basis van deze beveiligingsplannen. De planning is dat eind 2006 het BBNP geïmplementeerd is.
Met betrekking tot de vier belangrijkste processen van de CIE is een A&K-analyse uitgevoerd, waarvan de resultaten verwerkt zijn in een informatiebeveiligingsplan.
Het korps Noord- en Oost-Gelderland heeft voor de interceptiefaciliteiten een protocol opgesteld, welke gebaseerd is op de Normstelling Inrichting Interceptiefaciliteiten en op een interne toets van de interceptiefaciliteiten.
Het korps heeft een procedure met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten. Tijdens presentaties worden medewerkers erop gewezen hoe omgegaan moet worden met beveiligingsincidenten.
Bij het implementatieproces van het BBNP heeft het bevorderen van security awareness een vaste plaats gekregen. Zo wordt maandelijks een introductiecursus georganiseerd waar het onderdeel informatiebeveiliging vast onderdeel van uitmaakt.

NALEVING

Het korps Noord- en Oost-Gelderland is momenteel gestart met de evaluatie van het beleid om te komen tot een nieuw beleidsdocument. Daarnaast is informatiebeveiliging opgenomen in het korpsbeeld, waarmee het onderdeel uitmaakt van de INK-cyclus.
Het korps Noord- en Oost-Gelderland heeft één externe audit op het BBNP laten uitvoeren in 2003. De resultaten van deze audit zijn gebruikt om een prioritering aan te brengen voor de nog te implementeren maatregelen van het BBNP in het beveiligingsplan 2004.

KORPSBEELD GELDERLAND-MIDDEN

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Gelderland-Midden nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Gelderland-Midden heeft een concept beleidsplan informatiebeveiliging uit juni 2003 welke niet bekrachtigd is. Momenteel wordt dit beleid geactualiseerd en zal het vervolgens formeel goedgekeurd worden. Het beleidsplan is opgesteld conform de richtlijnen van de RIP.
In het beleidsplan informatiebeveiliging is algemeen vastgelegd wie verantwoordelijk is voor gegevensverzamelingen en informatiesystemen. Dit is niet expliciet vastgelegd voor de interceptiefaciliteiten of C2000.

INFORMATIEBEVEILIGINGSORGANISATIE

De plaatsvervangend korpschef is portefeuillehouder Informatiebeveiliging. De coördinatie van de informatiebeveiligingswerkzaamheden vindt plaats door de informatiebeveiligingsfunctionaris. Gezamenlijk vormen zij ook de hulporganisatie voor informatiebeveiliging. De bedoeling is om de informatiecoördinator de taak-accenthouder in het onderdeel te laten worden.
Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatie-beveiliging zijn niet vastgelegd in de functiebeschrijvingen. Alleen voor de informatie-beveiligingsfunctionaris zijn de taken expliciet benoemd in de functie-beschrijving.
Het contractbeheer is de verantwoordelijkheid van de service manager bij het Facilitair Bedrijf.

Het korps Gelderland-Midden heeft nog geen eisen gesteld met betrekking tot de deskundigheid van de hulporganisatie voor informatiebeveiliging. De deskundigheid van de informatiebeveiligingsfunctionaris zal opgebouwd worden door het volgen van de basisopleiding Informatiebeveiliging van de Politieacademie.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk zijn voldoende ingericht gegeven de grootte van het korps.
Met ISC-Midden zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een PDC, SLA en DAP. Tevens zijn korpsspecifieke afspraken gemaakt over de dienstverlening 'as-is'. In het kader van de interceptiefaciliteiten zijn afspraken gemaakt met het KLPD in een DVO, NOK en DAP.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Gelderland-Midden maakt gebruik van drie overzichten met informatiesystemen, namelijk een landelijk overzicht (de Politie Applicatie Portfolio), een overzicht van het verzorgingsgebied Noordoost (PDC) en een regionaal overzicht (Overzicht Applicaties en Functioneel Beheer). Het laatste overzicht is korpsspecifiek, welke onderhouden wordt door een beleidsmedewerker van de afdeling Informatiemanagement. Hierin is de verantwoordelijkheid voor de informatiesystemen ook belegd bij de proceseigenaren.
Het korps Gelderland-Midden heeft geen inzicht in hoeverre het BBNP geïmplementeerd is en momenteel is ook geen planning beschikbaar met betrekking tot de verdere implementatie van het BBNP.
Tot op heden zijn geen A&K-analyses uitgevoerd. Het korps geeft aan een scan uitgevoerd te hebben op de interceptiefaciliteiten naar aanleiding van de Normstelling Inrichting Interceptiefaciliteiten.
Het korps heeft een conceptprocedure voor de melding en afhandeling van informatiebeveiligingsincidenten.
De security awareness van de medewerkers wordt momenteel voornamelijk bevorderd door middel van het tekenen van een geheimhoudingsverklaring en korpsrichtlijnen. Het bevorderen van de security awareness is als speerpunt benoemd voor de komende jaren.

NALEVING

Het korps heeft de bedoeling om informatiebeveiliging op te nemen in de marap-cyclus voor 2007, waardoor de leidinggevenden verplicht worden over informatiebeveiliging te rapporteren. Tot op heden heeft bij het korps geen expliciete audit met betrekking tot informatiebeveiliging plaatsgevonden.

KORPSBEELD GELDERLAND-ZUID

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Gelderland-Zuid nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Gelderland-Zuid heeft een informatiebeveiligingsbeleid, waarin aandacht wordt besteed aan de aandachtspunten zoals genoemd in de RIP.
Het Openbaar Ministerie in Gelderland-Zuid is niet betrokken bij de vertaling van de Normstelling Inrichting Interceptiefaciliteiten naar de lokale situatie. Het beheer van de interceptiefaciliteiten is niet expliciet belegd in een beleidsdocument.
In het informatiebeveiligingsbeleid zijn de taken en verantwoordelijkheden voor C2000 op een hoog abstractieniveau opgenomen. Het informatiebeveiligingsbeleid C2000 is verder niet concreet en expliciet opgenomen in het beleidsdocument.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging is de korpsbeheerder. De korpschef is de dagelijkse verantwoordelijke en de plaatsvervangend korpschef is portefeuillehouder Informatiebeveiliging en heeft zodoende de regelende en sturende verantwoordelijkheid. De hulporganisatie bestaat uit vier taakaccenthouders informatiebeveiliging, één materiedeskundige fysieke beveiliging, één beleidsmedewerker algemeen, één adviseur informatiebeveiliging en één privacyfunctionaris.
Taken, bevoegdheden en verantwoordelijkheden zijn nog niet vastgelegd behalve voor de specifiek met informatiebeveiliging belaste functionarissen, zoals de adviseur informatiebeveiliging en de interceptiecoördinator. Enkele verantwoordelijkheden zijn nu reeds benoemd in het informatiebeveiligingsbeleid.

De adviseur informatiebeveiliging wordt door de afdeling Informatiemanagement betrokken bij hun activiteiten. Voorbeelden hiervan zijn het beoordelen van contracten en het toetsen van deze aan het BBNP.
De CIO heeft de verantwoordelijkheid voor de afspraken met het CIP en het ISC. Hij wordt hierbij ondersteund door de service liaison ISC binnen de korpsstaf. Daarnaast vinden landelijke overleggen plaats met het CIP en het ISC. Tevens overleggen de IBF-ers in het IBF-NO overleg.
Het korps Gelderland-Zuid stuurt aan op een integrale benadering van beveiliging. Dit wordt onder andere duidelijk door de integratie van het interceptiebeleid en het informatiebeveiligingsbeleid C2000 in het informatiebeveiligingsbeleid.
Binnen het korps wordt geen structurele aandacht besteed aan het op peil houden van de deskundigheid van de IBF-er en andere medewerkers welke verantwoordelijk zijn voor informatiebeveiliging door middel van een opleidingsplan. Voor de IBF-er bestaat de mogelijkheid om seminars te volgen, deel te nemen aan landelijke informatie-beveiligingsbijeenkomsten en zelfstudie.
Voor de interceptiefaciliteiten wordt de functiescheiding gewaarborgd door middel van het verlenen van autorisaties (zowel logisch als fysiek) door de onderzoeksleider en de interceptiecoördinator.
Het korps Gelderland-Zuid heeft al een Dossier Afspraken en Procedures (DAP) met het ISC gemaakt. Na de concentratie en consolidatie van alle IT-middelen in ISC-NO, welke momenteel plaats vindt door middel van een project, zal een SLA opgesteld gaan worden. Voor de interceptiefaciliteiten is er een DVO tussen het KLPD en het korps en een overeenkomst tussen het ISC en het korps.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Gelderland-Zuid heeft een totaaloverzicht met alle informatiesystemen inclusief de applicatiebeheerders. Dit overzicht wordt op ad hoc basis onderhouden door applicatiebeheer, functioneel beheer en gebruikersoverleg. De maatregelen uit het BBNP zijn nog niet allemaal geïmplementeerd. Implementatie vindt plaats aan de hand van een implementatieplan, welke begin 2000 met het Wegingsinstrument opgesteld is.
Voor het RBS is een A&K-analyse uitgevoerd bij de concentratie en consolidatie naar ISC-NO. Andere A&K-analyses zijn niet uitgevoerd. De Normstelling Inrichting Interceptiefaciliteiten is door het korps nog niet uitgewerkt in formeel beleid en formele procedures, maar de uitvoering is bijna conform Normstelling.
Het korps Gelderland-Zuid heeft een korpsrichtlijn aanmelden en afhandelen van beveiligingsincidenten uit 1998, welke voor alle medewerkers beschikbaar is via intranet. Deze richtlijn is ook van toepassing op de interceptiefaciliteiten.
De security awareness van de medewerkers wordt voornamelijk bevorderd door (het opvolgen van) incidenten en het plaatsen van informatie over informatiebeveiliging op het intranet. Dit is nog niet geformaliseerd in een informatiebeveiligingsjaarplan.

NALEVING

Informatiebeveiliging is door het korps nog niet voldoende opgenomen in het INK-proces en daardoor nog niet geborgd. Tot op heden zijn nog geen interne of externe audits uitgevoerd met betrekking tot de informatiebeveiliging bij het korps Gelderland-Zuid.

KORPSBEELD UTRECHT

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Utrecht nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Utrecht heeft een geïntegreerd beveiligingsbeleid, waarin zowel ingegaan wordt op persoonsbeveiliging, informatiebeveiliging als fysieke beveiliging. De vaststelling van dit document kan door het korps niet bevestigd worden. De bedoeling is om het beleid in 2007 te evalueren en te herzien. Het beleid voldoet deels aan de richtlijnen van de RIP.
In het geïntegreerd beveiligingsbeleid zijn de interceptiefaciliteiten niet expliciet belegd. Dit zal bij de evaluatie en herziening in 2007 plaatsvinden. Het Openbaar Ministerie is niet betrokken bij de inrichting van de interceptiefaciliteiten.
In het geïntegreerd beveiligingsbeleid is C2000 niet expliciet belegd. Dit zal bij de evaluatie en herziening in 2007 plaatsvinden.

INFORMATIEBEVEILIGINGSORGANISATIE

De portefeuille Informatievoorziening (inclusief de verantwoordelijk voor de veiligheid en integriteit) is binnen de korpsleiding belegd.. De coördinatie van de informatiebeveiligingswerkzaamheden vindt plaats door de informatiebeveiligingsfunctionaris (medewerker bureau Veiligheid en Integriteit). De hulporganisatie voor informatiebeveiliging bestaat uit het hoofd BVI (portefeuillehouder integrale veiligheidszorg), de IBF en het hoofd Interceptiefaciliteit. De hulporganisatie met taakaccenthouders is niet van de grond gekomen, maar het korps gaat hiervoor nog een poging doen.
Het korps Utrecht besteedt in de functiebeschrijving aandacht aan taken, bevoegd-

heden en verantwoordelijkheden met betrekking tot integrale veiligheid. Expliciet voor informatiebeveiliging zijn deze niet opgenomen.
Het overleg met CIP en ISC vindt plaats op diverse niveaus door middel van de volgende overleggen:
Strategisch: leden van de korpsleiding, hoofd ISC-Midden en hoofd Promenens in de stuurgroep.
Tactisch: de CIO's van verzorgingsgebied Midden, hoofd ISC-Midden en één lid van de stuurgroep in de adviesgroep.
Operationeel: service liaisons van verzorgingsgebied Midden met de servicecoördinator van het ISC.
Het korps Utrecht heeft geen opleidingsplan. De eisen aan de deskundigheid aan de hulporganisatie van informatiebeveiliging is opgenomen in de functiebeschrijvingen.
De deskundigheid van de informatiebeveiligingsfunctionaris wordt op peil gehouden door de opleiding tot IBF, diverse cursussen en diverse overlegvormen.
De functiescheiding met betrekking tot de interceptiefaciliteiten is adequaat ingericht.
De functiescheiding van de Infodesk zijn volgens het korps adequaat vastgelegd conform het CIE-reglement.
Met ISC-Midden zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een PDC, SLA en DAP. In het kader van de interceptiefaciliteiten zijn nog geen afspraken gemaakt met het KLPD/ULI, omdat de aansluiting met het ULI nog niet gerealiseerd is.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Utrecht heeft in de PDC een overzicht met alle informatiesystemen en gemeenschappelijke IT-diensten, welke onderhouden wordt door ISC-Midden. Voor alle informatiesystemen zijn systeemeigenaren aangewezen doordat de proceseigenaren verantwoordelijk zijn voor de onder hun proces vallende informatiesystemen.
Utrecht heeft het BBNP deels geïmplementeerd. Momenteel wordt beoordeeld of het mogelijk is om de districten informatiebeveiligingsplannen te laten opstellen om het BBNP verder te implementeren.
Tot op heden zijn geen A&K-analyses uitgevoerd. Het korps geeft aan te voldoen aan de strekking van de maatregelen zoals opgenomen in de Normstelling Inrichting Interceptiefaciliteiten.
Het korps heeft geen procedure voor de melding en afhandeling van informatiebeveiligingsincidenten.
De security awareness van de medewerkers wordt bevorderd door middel van het intranet, Code Blauw (houding en gedragsregels) en de introductie Welkom bij de Politie. Informatiebeveiliging is hierbij een onderdeel van de integrale veiligheidszorg en integriteitzorg binnen het korps.

NALEVING

Informatiebeveiliging is geen onderdeel van de beleidsevaluatiecyclus. Het korps heeft in 2004 een interne audit uitgevoerd op de automatiseringsmaatregelen van het BBNP. In 2006 heeft ook een audit vanuit ISC-Midden plaatsgevonden op de automatiseringsmaatregelen van het BBNP bij het korps. Het korps heeft nog geen externe audits laten uitvoeren met betrekking tot informatiebeveiliging.

KORPSBEELD NOORD-HOLLAND NOORD

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Noord-Holland Noord grotendeels geïmplementeerd. De implementatie van de naleving op het gebied van informatiebeveiliging krijgt binnen het korps constante aandacht en wordt geëvalueerd in 2010.

INFORMATIEBEVEILIGINGSBELEID

Het korps Noord-Holland Noord heeft een informatiebeveiligingsbeleid, welke op 20 mei 2005 vastgesteld is door de korpsbeheerder. In dit beleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
Het beheer van de interceptiefaciliteiten is niet expliciet belegd in het informatiebeveiligingsbeleid. Het korps geeft aan dat dit valt binnen de in het beleid beschreven algemene verantwoordelijkheden ten aanzien van de informatiebeveiliging van het hoofd van de afdeling Procesondersteuning. Binnen de regio wordt niet overlegd over de inrichting van de interceptiefaciliteiten met het Openbaar Ministerie. Wel wordt regelmatig overlegd met het OM over de dagelijkse procesgang rondom interceptie. C2000 valt expliciet niet onder het informatiebeveiligingsbeleid. Dit heeft te maken met de landelijke voorschriften met betrekking tot C2000 welke richtinggevend zijn. Aangezien de informatiebeveiligingsfunctionaris betrokken is bij het C2000 informatiebeveiligingsbeleid, is het beschreven en vastgestelde C2000-beleid wel in lijn gebracht met het informatiebeveiligingsbeleid van het korps.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging is de korpsbeheerder, welke taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging heeft

gedelegeerd aan andere leidinggevenden binnen het korps. De dagelijkse verantwoordelijkheid voor de beveiliging van de informatievoorziening en de bescherming van de privacy is belegd bij de korpschef. De informatiebeveiligingsfunctionaris is verantwoordelijk voor de coördinatie van de informatiebeveiliging. De hulporganisatie voor informatiebeveiliging bestaat uit de informatiebeveiligingsfunctionaris, de servicemanager, de adviseur Procesondersteuning, de coördinator interceptiefaciliteiten en twee facilitair medewerkers gebouwen. Door de brede samenstelling van de hulporganisatie wordt informatiebeveiliging integraal opgepakt.
Taken, bevoegdheden en verantwoordelijkheden zijn voor de informatiebeveiligingsfunctionaris vastgelegd in de functiebeschrijving. De overige medewerkers worden bekend gemaakt met hun taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging door middel van gesprekken en protocollen, gedragscodes en werkwijzen met betrekking tot informatiebeveiliging.
De CIO is formeel verantwoordelijk voor het maken van afspraken met het ISC. De verantwoordelijkheid voor de contacten met ISC-NW is toebedeeld aan de service liaison. De service liaisons binnen de regio Noordwest overleggen periodiek met elkaar en het ISC-NW. Tevens overleggen ook de hoofden IM van de korpsen binnen de regio Noordwest met het ISC-NW.
Het korps Noord-Holland Noord heeft geen eisen gesteld met betrekking tot de deskundigheid van de hulporganisatie voor informatiebeveiliging. De deskundigheid van de informatiebeveiligingsfunctionaris wordt voornamelijk op peil gehouden door middel van overleg met informatiebeveiligingsfunctionarissen van naburige korpsen, het CIP en het ISC.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk is adequaat ingericht.
Met ISC-NW zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een PDC, SLA en DAP. Hierin is geen aandacht besteed aan het verkrijgen van (onafhankelijke) zekerheid over de betrouwbaarheid van de informatiesystemen en informatie. Wel wordt door een onafhankelijke partij op dit moment de beveiliging bij ISC-NW beoordeeld als onderdeel van een CIE-gerelateerd onderzoek. In het kader van de interceptiefaciliteiten zijn afspraken gemaakt met het KLPD.

INFORMATIEBEVEILIGINGSMAATREGELEN

In de PDC en het DAP is een overzicht opgenomen met in gebruik zijnde applicaties. Dit overzicht wordt door het ISC onderhouden. De verantwoordelijkheid voor de informatiesystemen is in het informatiebeveiligingsbeleid belegd bij de proceseigenaren.
Het korps Noord-Holland Noord heeft het BBNP grotendeels geïmplementeerd. Een audit door de informatiebeveiligingsfunctionaris van een ander korps heeft nog wel tekortkomingen geconstateerd. De implementatie heeft niet plaatsgevonden aan de hand van het Wegingsinstrument.

Tot op heden zijn geen A&K-analyses uitgevoerd. Momenteel wordt een A&K-analyse uitgevoerd door een externe leverancier met betrekking tot het CIE-systeem. Het korps geeft aan te voldoen aan de Normstelling Inrichting Interceptiefaciliteiten, maar men is nog bezig om een interceptiereglement op te stellen, welke nog de concept status heeft. In het beveiligingsbeleid is een procedure met betrekking tot beveiligingsincidenten opgenomen.
De security awareness van de medewerkers zal verbeterd worden door middel van een bewustwordingscampagne. Deze campagne wordt deels gebaseerd op de campagne in de regio Amsterdam-Amstelland en wordt ontwikkeld in samenwerking met de andere regio's in Noordwest.

NALEVING

Op ad hoc basis wordt de informatiebeveiliging geactualiseerd en geëvalueerd, maar dit is nog geen onderdeel van de INK-evaluatiecyclus. Binnen het korps Noord-Holland Noord zijn diverse initiatieven genomen met betrekking tot audits en nulmetingen. Deze worden voornamelijk uitgevoerd door eigen medewerkers of andere politieonderdelen. Complete audits inclusief vastleggingen zijn nog niet beschikbaar.

KORPSBEELD ZAANSTREEK-WATERLAND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Zaanstreek-Waterland grotendeels geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Zaanstreek-Waterland heeft een concept beleidsdocument informatie-beveiliging, welke nog in 2006 vastgesteld moest worden, waarna dit voor vijf jaar geldig is. Het beleid voldoet aan de richtlijnen van de RIP.
In het beleidsdocument wordt voor de interceptiefaciliteiten verwezen naar het Handboek Interceptie. Bij de ontwikkeling van dit Handboek is het Openbaar Ministerie betrokken geweest en deze heeft dit mede ondertekend.
In dit beleidsdocument wordt voor C2000 verwezen naar het beleidsdocument C2000.

INFORMATIEBEVEILIGINGSORGANISATIE

Het hoofd Kabinet Korpsleiding is eindverantwoordelijk voor de informatiebeveiliging binnen het korps. De coördinatie van de informatiebeveiligingswerkzaamheden vindt plaats door de informatiebeveiligingsfunctionaris (IBF). De hulporganisatie voor informatiebeveiliging is nog niet formeel benoemd, maar zal conform het beleids-document informatiebeveiliging gaan bestaan uit de IBF en de medewerkers Informatie Management (IM).
Het korps Zaanstreek-Waterland heeft in de functiebeschrijvingen geen aandacht voor taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging. Uitzondering hierop zijn de functiebeschrijvingen van de informatiebeveiligings-functionaris en de administratief medewerker KKL, privacy en informatiebeveiliging (ondersteuning van de informatiebeveiligingsfunctionaris met administratieve taken).

Het overleg met CIP en ISC vindt plaats door middel van de volgende overleggen:
- driewekelijks interregionaal werkoverleg met IBF-ers;
- tweewekelijks interregionaal werkoverleg met IM-ers, waarbij een keer per vier weken ISC-Noordwest aanwezig is.

Het korps Zaanstreek-Waterland heeft geen opleidingsplan. De deskundigheid van de informatiebeveiligingsfunctionaris wordt op peil gehouden door zelfstudie en overleg op diverse niveaus met informatiebeveiligingsfunctionarissen.
De functiescheiding met betrekking tot de interceptiefaciliteiten en Infodesk wordt zoveel mogelijk toegepast. In verband met de grootte van de regio is dit niet altijd mogelijk.
Met ISC-Noordwest zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een PDC, SLA en DAP. In het kader van de interceptiefaciliteiten zijn afspraken gemaakt met het KLPD in een DVO en NOK.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Zaanstreek-Waterland heeft de beschikking over meerdere overzichten met alle informatiesystemen/gemeenschappelijke IT-diensten. Deze overzichten worden bijgehouden door ISC. De systeemeigenaren zijn impliciet aangewezen via de proces-eigenaren.
Het korps Zaanstreek-Waterland heeft een groot deel van het BBNP geïmplementeerd, maar nog niet alles vastgelegd. Hoe en wanneer de verbeterpunten opgevolgd zullen worden, zal opgenomen worden in het informatiebeveiligingsbeleid.
Tot op heden zijn geen A&K-analyses uitgevoerd. Het korps voldoet met het Handboek Interceptie aan de Normstelling Inrichting Interceptiefaciliteiten.
Het korps heeft in het informatiebeveiligingsbeleid een procedure opgenomen voor de melding en afhandeling van informatiebeveiligingsincidenten.
Het primaire aandachtspunt met betrekking tot informatiebeveiliging binnen het korps is cultuur en gedrag. De focus ligt hierdoor op awareness activiteiten in plaats van het borgen van processen in procedures. Zodoende wordt op diverse manieren gecommuniceerd over informatiebeveiliging om de security awareness van de mede-werkers te bevorderen. In het informatiebeveiligingsbeleid zal dit ook vastgelegd worden.

NALEVING

Informatiebeveiliging is geen onderdeel van de beleidsevaluatiecyclus. In 2005 is een interregionale audit uitgevoerd met betrekking tot de opzet en het bestaan van het BBNP. Hiernaast zijn geen audits uitgevoerd.

KORPSBEELD KENNEMERLAND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Kennemerland grotendeels geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Kennemerland heeft een informatiebeveiligingsbeleid 2004, welke geldig is tot en met 2008. Het informatiebeveiligingsbeleid is grotendeels opgesteld conform de richtlijnen van de RIP.
In het informatiebeveiligingsbeleid is geen expliciete verantwoordelijkheid belegd voor de interceptiefaciliteiten. Door de korpschef is deze verantwoordelijkheid toegewezen aan de Divisiechef Regionale Recherche als verantwoordelijke voor het proces opsporing. Voor de inrichting van het ULI concept per 1 januari 2007 vindt afstemming plaats met het Openbaar Ministerie.
In het informatiebeveiligingsbeleid is geen expliciete verantwoordelijkheid belegd voor C2000. Door de korpschef is de verantwoordelijkheid toegewezen aan de Divisiechef Operationele Ondersteuning als eindverantwoordelijke voor het proces C2000. Binnen de regio wordt momenteel een informatiebeveiligingsplan opgesteld naar aanleiding van de nieuwe veiligheidsregio.

INFORMATIEBEVEILIGINGSORGANISATIE

De directeur bedrijfsvoering is portefeuillehouder informatiebeveiliging. De coördinatie van de informatiebeveiligingswerkzaamheden vindt plaats door de adviseur informatiebeveiliging. De hulporganisatie voor informatiebeveiliging bestaat uit de portefeuillehouder informatiebeveiliging, de CIO, de adviseur informatiebeveiliging, de taakaccenthouders informatiebeveiliging in de divisies/districten en het dienstencluster.

Het korps Kennemerland maakt gebruik van functietyperingen en functieprofielen. Hierin is geen aandacht besteed aan taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging. De enige uitzondering hierop is de functietypering voor de adviseur informatiebeveiliging.
De CIO is verantwoordelijk voor het contractbeheer, waarbij hij wordt ondersteund door de service liaison. De service liaison participeert in een verzorgingsgebiedoverleg met de andere service liaisons en het ISC. Tevens overleggen de IBF-ers van de 4 korpsen periodiek met de IBF-er van ISC Noordwest. Tevens heeft de IBF-er geadviseerd in het concentratie- en consolidatieproject.
Het korps Kennemerland heeft geen eisen gesteld met betrekking tot de deskundigheid van de hulporganisatie voor informatiebeveiliging. De deskundigheid van de IBF wordt op peil gehouden door periodieke opleiding, bijscholing, collegiaal overleg en het volgen van vakliteratuur en bronnen op internet.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk zijn adequaat.
Met ISC-Noordwest zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een PDC, SLA en DAP. In het kader van de interceptiefaciliteiten zijn nog geen afspraken gemaakt met het KLPD. Het korps gaat per 1 januari 2007 over en momenteel is er een concept interceptiereglement.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Kennemerland heeft in de PDC een overzicht met alle informatiesystemen /gemeenschappelijke IT-diensten, welke onderhouden wordt door ISC-Noordwest. Voor alle informatiesystemen zijn systeemeigenaren aangewezen.
Kennemerland heeft het BBNP nog niet geheel geïmplementeerd. Implementatie vindt plaats door middel van teambeveiligingsplannen, welke door teamchefs opgesteld worden. Voor de teambeveiligingsplannen wordt gebruik gemaakt van het Wegingsinstrument.
Tot op heden zijn geen A&K-analyses uitgevoerd. Het korps geeft aan bij de inrichting van de interceptiefaciliteiten per 1 januari 2007 rekening te houden met de Normstelling Inrichting Interceptiefaciliteiten.
Het korps heeft een procedure voor de melding en afhandeling van informatiebeveiligingsincidenten. Periodiek wordt aan de medewerkers voorlichting gegeven waarbij gebruik gemaakt wordt van beveiligingsincidenten uit andere organisaties.
De security awareness van de medewerkers wordt bevorderd door middel van periodieke voorlichting, het bespreken van de resultaten van audits, het introduceren van teambeveiligingsplannen.

NALEVING

Informatiebeveiliging is onderdeel van de jaarlijkse beleidsevaluatie op korpsniveau. Daarnaast wordt momenteel gewerkt aan een sjabloon voor managementrapportages betreffende integriteit (informatiebeveiliging is daarvan een onderdeel). Het korps voert diverse interne audits uit op verschillende aspecten. Op de implementatie van het BBNP heeft in het najaar van 2002 een externe audit plaatsgevonden.

KORPSBEELD AMSTERDAM-AMSTELLAND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Amsterdam-Amstelland nagenoeg geheel geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Amsterdam-Amstelland heeft een Informatiebeveiligingsbeleid Politiekorps Amsterdam-Amstelland, welke op 10 maart 2003 vastgesteld is door de korpschef. Het beleid voldoet aan de richtlijnen van de RIP.
Het beheer van de interceptiefaciliteiten is niet belegd in het beleidsdocument.
C2000 is niet opgenomen in het beleidsdocument. Het beveiligingsplan C2000, waarin het beleid opgenomen is, is opgesteld door de projectgroep C2000 in opdracht van de proceseigenaar. Dit is in nauwe samenwerking met de informatiebeveiligingsadviseur van het korps gebeurd.

INFORMATIEBEVEILIGINGSORGANISATIE

De dagelijkse verantwoordelijkheid voor de beveiliging van de processen van de politie Amsterdam-Amstelland is belegd bij de zogenaamde informatie-eigenaren van die processen. De korpschef neemt als eindverantwoordelijke voor de beveiliging besluiten indien korpsbrede activiteiten noodzakelijk zijn. De coördinatie van de informatie-beveiligingswerkzaamheden vindt plaats door de senior adviseur beveiliging. De hulporganisatie voor informatiebeveiliging bestaat uit DBI Informatiebeveiliging (4 medewerkers), de informatie-eigenaren en de portefeuillehouders Bewustwording (in het kader van de campagne Weet wat je Weet).
Het korps Amsterdam-Amstelland heeft bewust gekozen in de functiebeschrijvingen, met uitzondering van de medewerkers van Informatiebeveiliging, geen beveiligings-

aspecten mee te nemen. De integrale verantwoordelijkheid van medewerkers maakt dat naar beleving van het korps overbodig.
Regelmatig vindt beveiligingsoverleg plaats tussen de korpsen binnen ISC-Noordwest, waarbij ook ISC Centraal, ISC-Noordwest en CIP vertegenwoordigd zijn. Dit overleg is zowel op het niveau van de CIO (niet expliciet over informatiebeveiliging, maar soms over deelaspecten) als van de IBF (eens in de zes weken). Onafhankelijk van de formele trajecten heeft Amsterdam-Amstelland daarnaast zelf regelmatig overleg met ISC en CIP.
Aan de deskundigheid van de medewerkers van de hulporganisatie zijn functie-eisen gesteld. Elke medewerker heeft een persoonlijk opleidingsplan, waardoor de verschillen tussen kennis en de functie-eisen moeten worden opgelost. Tevens mogen functie gerelateerde cursussen/opleidingen gevolgd worden. De deskundigheid van de informatiebeveiligingsfunctionaris wordt op peil gehouden door overleg op regionaal, bovenregionaal en landelijk niveau en cursussen.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk is adequaat ingericht.
Met ISC-Noordwest zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een DAP, SLA en PDC. In het kader van de interceptiefaciliteiten zijn geen afspraken gemaakt, omdat nog geen gebruik gemaakt wordt van de landelijke faciliteiten.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Amsterdam-Amstelland maakt gebruik van de zogenaamde kruisjeslijst voor een overzicht van alle informatiesystemen/gemeenschappelijke IT-diensten. Deze wordt onderhouden door ISC-Noordwest en supply management. Per proces en gegevensverzameling zijn informatie-eigenaren aangewezen, welke vervolgens verantwoordelijk zijn voor alle daaronder vallende systemen (zowel geautomatiseerd als niet-geautomatiseerd).
Het korps Amsterdam-Amstelland geeft aan momenteel te voldoen aan de eigen baseline, welke gelijk is of beter dan het BBNP. In de geest wordt hierdoor voldaan aan het BBNP, maar niet op detailniveau. De eigen baseline bestaat volgens het korps uit een set eenvoudiger, goedkopere of effectievere maatregelen.
Amsterdam-Amstelland heeft een Blauwdruk Informatiebeveiligingsplan RPAA, welke door de eigenaar van een informatiesysteem gebruikt kan worden om een informatiebeveiligingsplan op te stellen. Op deze manier wordt een A&K-analyse uitgevoerd. Voor de aanvullende maatregelen wordt dit omgezet in implementatieplannen door de uitvoerende partij. DBI Informatiebeveiliging controleert de aanwezigheid van het plan en monitort tevens de status van de implementatie/verbeteringen. Voor diverse processen zijn procesanalyses uitgevoerd, waarbij tegelijkertijd een analyse uitgevoerd is voor meerdere informatiesystemen. Het korps heeft een beveiligingsanalyse uitgevoerd in 2004 naar aanleiding van de Normstelling Inrichting Interceptiefaciliteiten. Hierin werd

geconstateerd dat niet voldaan werd aan de Normstelling Inrichting Interceptiefaciliteiten, maar dat de informatiebeveiliging met relatief eenvoudige maatregelen op korte termijn verbeterd kon worden. De Normstelling Inrichting Interceptiefaciliteiten wordt echter nog steeds niet gehaald. In verband met de toenmalige verwachte overgang naar het ULI is ervoor gekozen om geen grote investeringen te doen. Deze overstap zal per 1 maart of april 2007 plaatsvinden.
Het korps Amsterdam-Amstelland heeft een procedure voor het melden en afhandelen van beveiligingsincidenten, welke door de campagne 'Weet wat je Weet' weer extra onder de aandacht is gekomen. De bewustwording in bredere zin stimuleert dus de meldingsdiscipline van medewerkers. De gemelde incidenten worden geregistreerd en hierover wordt gerapporteerd door middel van een balance score card.
De security awareness wordt bevorderd door middel van de campagne 'Weet wat je Weet'. Deze campagne heeft een beoogde levensduur van drie jaar waarin telkens subthema's, zogenaamde 'flights', worden belicht. Op dit moment zijn drie flights uitgevoerd, te weten:
Weet wat je ZEGT.
Weet wat je DOET.
Weet wat je VRAAGT.
Deze thema's worden door middel van verschillend promotiemateriaal onder de aandacht van de medewerkers gebracht. Het effect van de campagne wordt na elke flight getoetst en na de derde flight heeft een externe audit plaatsgevonden.

NALEVING

Beveiliging is door Amsterdam-Amstelland nog niet opgenomen in de jaarcyclus van planning en control. De bedoeling is om dit alsnog te realiseren. Momenteel wordt informatiebeveiliging nog apart behandeld door middel van een balance score card. Overall is in 2005 101% ten opzichte van de norm gescoord.
In de afgelopen vier jaar is door het korps Amsterdam-Amstelland geen complete audit op het BBNP uitgevoerd, maar wel op onderdelen. Audits met betrekking tot de Normstelling Inrichting Interceptiefaciliteiten zijn recentelijk niet uitgevoerd, omdat hiermee gewacht wordt op de verwachte overgang naar het ULI.

KORPSBEELD GOOI EN VECHTSTREEK

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Gooi en Vechtstreek nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Gooi en Vechtstreek heeft geen informatiebeveiligingsbeleid. Momenteel is de regio in samenwerking met de regio Flevoland bezig om een gezamenlijk beleid op te stellen.
Bij het vernieuwen van de inrichting van de interceptiefaciliteiten is de Officier van Justitie betrokken geweest om het nieuwe werkproces voor interceptie door te nemen.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging is de korpsbeheerder, welke deze taken, verantwoordelijkheden en bevoegdheden gedelegeerd heeft aan de korpschef. De verantwoordelijkheid voor de uitvoering van de normen is toebedeeld aan het lijnmanagement en de diensthoofden. Een functie van informatiebeveiligingsfunctionaris (IBF) is gesplitst in twee functies: de beleidsmedewerker IT voor de ICT-aspecten en het hoofd CDFO voor de niet ICT-aspecten. De hulporganisatie voor informatiebeveiliging bestaat uit het hoofd BKO (tevens CIO), het hoofd Facilitaire Ondersteuning, de beleidsmedewerker IT en de beleidsmedewerker IM. Door de samenstelling van de hulporganisatie wordt de informatiebeveiliging opgepakt vanuit meerdere aspecten.
Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn niet vastgelegd in de functiebeschrijvingen. Het is de bedoeling dit wel te gaan doen.
De CIO is formeel verantwoordelijk voor het maken van afspraken met het ISC, maar

heeft dit gedelegeerd aan het hoofd Facilitaire Ondersteuning. Operationeel vindt de afstemming met het ISC plaats door de service liaison. De CIO's van de regio Midden (voor Gooi en Vechtstreek het hoofd Facilitaire Ondersteuning) overleggen periodiek met het hoofd verzorgingsgebied van ISC-Midden in de stuurgroep. Tevens is er overleg in de vorm van een adviesgroep van alle CIO's en CDFO's van de korpsen van de regio Midden. Daarnaast overlegt de service liaison met de service coördinator van het ISC.
Het korps Gooi en Vechtstreek heeft geen eisen gesteld met betrekking tot de deskundigheid van de hulporganisatie voor informatiebeveiliging. De deskundigheid van de informatiebeveiligingsfunctionaris wordt op peil gehouden door middel van overleggen van IBF-ers.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk zijn adequaat doordat hiervoor de landelijke richtlijnen gevolgd worden.
Met ISC-Midden zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een SLA en DAP.
In het kader van de interceptiefaciliteiten zijn afspraken gemaakt met het LIO in een DVO.

INFORMATIEBEVEILIGINGSMAATREGELEN

In de PDC is een overzicht opgenomen met in gebruik zijnde applicaties. Dit overzicht wordt door het ISC onderhouden. De verantwoordelijkheid voor de informatiesystemen is belegd bij het management.
Het korps Gooi en Vechtstreek heeft het BBNP deels geïmplementeerd. Momenteel is het korps bezig met de implementatie, welke plaatsvindt aan de hand van het Wegingsinstrument. De bedoeling is om per 1 januari 2007 een deel van de maatregelen geïmplementeerd te hebben en een ander deel per 1 januari 2008. Eén januari 2007 gaat waarschijnlijk niet gehaald worden.
Tot op heden zijn geen A&K-analyses uitgevoerd. Het korps geeft aan de Normstelling Inrichting Interceptiefaciliteiten gebruikt te hebben bij de implementatie van de interceptiefaciliteiten. Op basis van de Normstelling is een notitie opgesteld welke aanpassingen noodzakelijk waren om te voldoen aan de Normstelling.
Met betrekking tot beveiligingsincidenten zijn geen procedures vastgelegd. De incidenten dienen gemeld te worden aan het hoofd CDFO.
De security awareness van de medewerkers wordt momenteel niet bevorderd.

NALEVING

Aangezien het korps geen informatiebeveiligingsbeleid heeft kan dit niet geactualiseerd en geëvalueerd worden. Tot op heden heeft bij het korps geen audit plaatsgevonden met uitzondering van een externe audit op hoofdstuk 3 (automatiseringsorganisatie) van het BBNP op verzoek van ISC-Midden voor de overdracht van de automatisering.

KORPSBEELD HAAGLANDEN

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Haaglanden grotendeels geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Haaglanden heeft een concept informatiebeveiligingsbeleid, welke nog niet vastgesteld is in verband met reorganisaties binnen het korps en ontwikkelingen binnen de ICT. Het conceptbeleid is een integraal beveiligingsbeleid, waarbij zowel ingegaan wordt op persoonsbeveiliging, de informatiebeveiliging als de fysieke beveiliging. Binnen het concept informatiebeveiligingsbeleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
Voor zover bekend heeft het Openbaar Ministerie een verantwoordelijkheid met betrekking tot het bewaren van de interceptiegegevens, maar hoe deze verantwoordelijkheid uitgewerkt is bij het stellen van de eisen voor de inrichting van de interceptiefaciliteiten is onbekend bij het korps. Het beheer van de interceptiefaciliteiten is niet belegd in een informatiebeveiligingsbeleid en/of -plan. Eind november zijn de interceptiefaciliteiten overgedragen aan het ULI.
Het korps Haaglanden heeft voor het beveiligingsbeleid C2000 meegewerkt aan de werkgroep Veiligheid binnen het C2000-project. Het resulterende beveiligingsbeleid is uitgevoerd.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging, de portefeuillehouder informatiebeveiliging wordt ondersteund door de informatiebeveiligingsfunctionaris (beleidsmedewerker security). De hulporganisatie bestaat formeel uit de IBF-er en de taak-

accenthouders. In de praktijk is deze hulporganisatie verwaterd en wordt gebruik gemaakt van zogenaamde IB-vertegenwoordigers in de lijn.
Taken, bevoegdheden en verantwoordelijkheden zijn nog niet integraal vastgelegd. Als enige uitzondering hierop geldt de CIO, waarvoor informatiebeveiligingsaspecten opgenomen zijn in de functiebeschrijving. Enkele verantwoordelijkheden zijn nu reeds benoemd in de bestaande beleidsdocumenten en informatiebeveiligingsplannen.
De CIO heeft de verantwoordelijkheid voor het onderhouden van de contacten met het CIP en het ISC. Alle CIO's, het CIP en het ISC hebben onder andere maandelijks een overleg. Met betrekking tot de dienstverlening heeft alleen de korpsbeheerder hier eens per jaar inspraak in.
De IBF volgt de beschikbare opleidingen en cursussen en neemt tevens deel aan de landelijke IBF-dagen en intercollegiale overleggen. Binnen het korps wordt geen structurele aandacht besteed aan het op peil houden van de deskundigheid van de IBF-er en andere medewerkers welke verantwoordelijk zijn voor informatiebeveiliging door middel van een opleidingsplan.
Voor de interceptiefaciliteiten is functiescheiding gewaarborgd door middel van de autorisaties. Dit is procedureel niet vastgelegd. Voor de Infodesk heeft het korps niet aantoonbaar gemaakt dat functiescheiding adequaat is geïmplementeerd.
De dienstverlening met het ISC bevindt zich nog in de projectfase. Zodoende zijn nog geen gedetailleerde afspraken op het gebied van informatiebeveiliging gemaakt. Voor de interceptiefaciliteiten zijn afspraken met het KLPD nog niet belegd in verband met de overgang van de technische interceptievoorzieningen naar het KLPD.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Haaglanden heeft een totaaloverzicht met alle informatiesystemen en gemeenschappelijke IT-diensten inclusief de verantwoordelijke managers. Dit overzicht wordt onderhouden door het Bureau Informatiemanagement.
De maatregelen uit het BBNP zijn nog niet allemaal geïmplementeerd. Implementatie zal niet plaatsvinden aan de hand van het Wegingsinstrument, omdat dit volgens het korps te omslachtig en ingewikkeld is. Zodoende zal gebruik gemaakt worden van het door het korps aangeschaft tool PDA2L (Process Dependency Analysis Tool).
Voor het proces CIE (Criminele Inlichtingen Eenheid) is een A&K-analyse uitgevoerd door het korps. Dit heeft geresulteerd in een implementatieplan CIE. De Normstelling Inrichting Interceptiefaciliteiten is door het korps nog niet uitgewerkt in beveiligingsmaatregelen.
Het korps Haaglanden heeft een conceptrichtlijn Registratie en afhandeling van beveiligingsincidenten. Met betrekking tot de interceptiefaciliteiten is de beveiliging een terugkerend item op het werkoverleg. Incidenten worden door de medewerkers in de lijn of bij BIS gemeld. De aangemelde incidenten worden onderzocht en met de uitkomst van de onderzoeken wordt het beleid aangepast of bijgesteld.
De security awareness van de medewerkers wordt voornamelijk ad hoc bevorderd door

het publiceren van incidenten. In het werkplan van het Bureau Integriteit en Security is informatiebeveiliging opgenomen in voorlichtingsbijeenkomsten en cursussen.

NALEVING

Informatiebeveiliging is door het korps nog niet verweven in het INK-proces en daardoor nog niet geborgd. Het Bureau Integriteit en Security heeft interne audits uitgevoerd, bijvoorbeeld op het internet op de standaard werkplek en internet op een stand-alone computer. Tot op heden zijn nog geen externe audits uitgevoerd met betrekking tot de informatiebeveiliging bij het korps Haaglanden.

KORPSBEELD HOLLANDS MIDDEN

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Hollands Midden ten dele geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Hollands Midden heeft een geïntegreerd beveiligingsbeleid (personele-, informatie- en fysieke beveiliging), welke opgesteld is door een stuurgroep van de regiopolitie Utrecht. Het beleid voldoet grotendeels aan de richtlijnen van de RIP.
De interceptiefaciliteiten zijn niet opgenomen in het geïntegreerd beveiligingsbeleid. Het beleid hiervoor is opgenomen in het Beveiligingsreglement Interceptie. De inrichting van de interceptiefaciliteiten is gefaseerd ingericht conform de Normstelling Inrichting Interceptiefaciliteiten. Bij alle fasen is de Officier van Justitie betrokken geweest.
C2000 is niet opgenomen in het geïntegreerd beveiligingsbeleid. Het beleid hiervoor is opgenomen in het beveiligingsplan C2000.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijkheid voor informatiebeveiliging is door de korpsleiding gedelegeerd aan het lijnmanagement van de districten, de korpsrecherche, de divisie Operationele Ondersteuning en de stafafdelingen. De coördinatie van de informatie-beveiligingswerkzaamheden vindt plaats door de portefeuillehouder Veiligheid & Integriteit (directeur politie) en de adviseur Veiligheid & Integriteit. De hulporganisatie voor informatiebeveiliging bestaat uit de portefeuillehouder Veiligheid & Integriteit, de adviseur Veiligheid & Integriteit, de Functionaris voor de Gegevensbescherming en vanuit de districten/dienstonderdelen de contactpersonen Veiligheid & Integriteit en deelportefeuillehouders Veiligheid & Integriteit. Momenteel is de IBF-functie vacant,

omdat de adviseur Veiligheid & Integriteit nu acteert als functionaris voor de Gegevensbescherming; een meer toezichthoudende rol.
Het korps Hollands Midden heeft in de functiebeschrijvingen geen aandacht voor taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging met uitzondering van de functieomschrijving voor de adviseur Veiligheid & Integriteit.
De IBF van Haaglanden, waargenomen door de adviseur Veiligheid & Integriteit van Hollands Midden, en de IBF van ISC-West hebben vier maal per jaar afstemmingsoverleg. De CIO's overleggen maandelijks met het CIP en daarnaast overlegt de CIO van Hollands Midden met het hoofd van VG West.
Het korps Hollands Midden heeft momenteel geen eisen voor de deskundigheid van de medewerkers van de hulporganisatie gesteld.
De functiescheiding met betrekking tot de interceptiefaciliteiten is formeel geregeld in het Beveiligingsreglement Interceptie. Binnen de Infodesk is dit volgens het korps afdoende geregeld doordat gevoelige informatie niet via de Infodesk verstrekt mag worden. Alle informatie is beschikbaar voor alle politiefunctionarissen.
Met ISC-West zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een DAP, SLA en PDC. In het kader van de interceptiefaciliteiten zijn afspraken gemaakt met het KLPD in een DAP, DVO en NOK.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Hollands Midden heeft een applicatieportfolio inclusief autorisaties en registratiehouders. Functioneel beheer houdt deze portfolio bij en bewaakt tevens de afstemming met de landelijke applicatieportfolio.
Het korps Hollands Midden heeft het BBNP grotendeels geïmplementeerd conform een intern onderzoek uit 2005 door bureau Veiligheid & Integriteit. Op basis van dit onderzoek moeten de proceseigenaren verbeterplannen opstellen, maar daar is nog niet veel van gekomen. Bij de implementatie is het Wegingsinstrument wel gebruikt, maar is geen implementatieplan opgesteld.
Tot op heden heeft het korps geen A&K-analyses uitgevoerd.
Het korps heeft het Beveiligingsreglement Interceptie opgesteld naar aanleiding van de Normstelling Inrichting Interceptiefaciliteiten. In de praktijk wordt nog niet geheel voldaan aan de Normstelling Inrichting Interceptiefaciliteiten als gevolg van nieuwbouw, verbouw en herinrichtingsprojecten. De verwachting van het korps is dat binnen een jaar volledig voldaan wordt aan de Normstelling Inrichting Interceptiefaciliteiten.
Het korps Hollands Midden heeft geen procedure voor het melden en afhandelen van beveiligingsincidenten. Registratie van gemelde incidenten vindt op drie locaties plaats, namelijk de helpdesk van het korps, het ISC en door Veiligheid & Integriteit.
De security awareness wordt voornamelijk op ad hoc manier bevorderd door middel van voorlichting bij nieuwe informatiesystemen/IT-diensten. Dit is niet verankerd in een informatiebeveiligingsjaarplan.

NALEVING

Informatiebeveiliging is geen onderdeel van de beleidsevaluatiecyclus. Binnen het korps zijn nog geen specifieke audits met betrekking tot informatiebeveiliging uitgevoerd.

KORPSBEELD ROTTERDAM-RIJNMOND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Rotterdam-Rijnmond grotendeels geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

De korpsbeheerder van het korps Rotterdam-Rijnmond heeft in 1996 het eindrapport Informatiebeveiliging Politie Rotterdam-Rijnmond vastgesteld, waarin de RIP vertaald is naar het korps. De actualisering van dit beleid is gepland voor 2007. In dit beleid wordt aandacht besteed aan de meeste aandachtspunten zoals genoemd in de RIP.
Het korps heeft geen verdere invulling gegeven aan de Normstelling Inrichting Interceptiefaciliteiten. Beslissingen met betrekking tot de interceptiefaciliteiten worden in de driehoek besproken en genomen.
C2000 is niet verweven in het informatiebeveiligingsbeleid. Op basis van het C2000 beveiligingsbeleid is een Beveiligingsplan C2000 voor de regio Rotterdam-Rijnmond opgesteld, welke volgens het korps op korte termijn verankerd zal worden in de diverse korpsregelingen.

INFORMATIEBEVEILIGINGSORGANISATIE

De regionaal portefeuillehouder Integriteit & Security is zowel de eindverantwoordelijke voor informatiebeveiliging als verantwoordelijke voor de coördinatie van de activiteiten op het gebied van informatiebeveiliging. De hulporganisatie bestaat uit de deelnemers van de Werkgroep Security: Personeel & Organisatie, Facilitair Bedrijf-Security, Facilitair Bedrijf-Beveiliging, DR3i (I&AT), Bureau Interne Zaken, Bureau Veiligheids Onderzoeken, Korps Security Functionaris (IBF), Decentrale Security Functionarissen, Hoofden Bedrijfs Hulpverlening en Communicatie.

Regionaal en interregionaal vindt er overleg plaats op het gebied van informatiebeveiliging door de IBF van het korps met ISC verzorgingsgebied Zuidwest en het CIP, eventueel samen met de IBF-ers van de andere Zuidwestelijke korpsen. De IBF neemt ook op landelijk niveau deel aan overleggen met het ISC, het CIP en IBF'ers van andere korpsen.
Alleen voor de Korps Security Functionaris zijn de taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging vastgelegd in een functieomschrijving.
De CIO is verantwoordelijk voor het maken van afspraken met het ISC. De tactische verantwoordelijkheid is gedelegeerd aan het hoofd Informatie Management (tevens plaatsvervangend CIO). De operationele afstemming met het ISC wordt uitgevoerd door de service liaison.
Voor de deelnemers aan de Werkgroep Security worden geen kenniseisen gesteld, omdat het korps het bij elkaar brengen van kennis en ervaring vanuit verschillende vakdisciplines als belangrijkste meerwaarde ziet. Voor de Decentrale Security Functionarissen zullen opleidingseisen gesteld gaan worden als onderdeel van de verdere professionalisering.
Voor zowel de interceptiefaciliteiten als de Infodesk is de functiescheiding adequaat ingericht.
Het korps Rotterdam-Rijnmond heeft met het ISC momenteel een PDC en SLA. Met betrekking tot de interceptiefaciliteiten heeft het korps geen afspraken met het KLPD/ULI, omdat het korps daarop nog niet aangesloten is.

INFORMATIEBEVEILIGINGSMAATREGELEN

De applicatieportfolio wordt in verband met de gewijzigde situatie momenteel aangepast. In dit overzicht met informatiesystemen zijn tevens de proceseigenaren opgenomen. De applicatieportfolio wordt conform de SLA onderhouden door het ISC, waarbij de besluitvorming plaats vindt door de stuurgroep van het verzorgingsgebied.
Het korps heeft ongeveer 75% van de maatregelen uit het BBNP geïmplementeerd. De overige maatregelen worden niet geïmplementeerd, omdat deze niet werkbaar zijn en/of hoge kosten met zich meebrengen. Daarnaast vindt het korps het BBNP op een aantal punten gedateerd, waardoor zij een aantal maatregelen niet zal implementeren.
Het korps Rotterdam-Rijnmond heeft beperkt A&K-analyses uitgevoerd door middel van het project 'Blauwe (p)lekken'. De verbeterpunten uit de A&K-analyses zijn opgepakt en inmiddels gerealiseerd. Naar aanleiding van een audit op de interceptiefaciliteiten in 2003/2004 zijn enkele risico's gemitigeerd, maar niet alleen in verband met de overgang naar het KLPD/ULI. Deze overgang is echter meerdere malen uitgesteld en heeft nog steeds niet plaatsgevonden.
Het korps heeft een meldingsprocedure voor beveiligingsincidenten uit 2004, welke momenteel geactualiseerd wordt. De incidentregistratie wordt gevoerd door een medewerker van het Facilitair Bedrijf en de informatiebeveiligingsfunctionaris.

De security awareness van de medewerkers wordt bevorderd door middel van een focus op gedrag. Concreet wordt dit uitgevoerd door middel van publicaties, het aanspreken van medewerkers op hun gedrag en het laten ondertekenen van gedragsprotocollen.

NALEVING

Informatiebeveiliging is door het korps momenteel niet opgenomen in de evaluatiecyclus. Het is wel de bedoeling om informatiebeveiliging op termijn op te nemen in de planning & control cyclus van het korps.
Bij het korps Rotterdam-Rijnmond zijn diverse interne en externe audits uitgevoerd met betrekking tot de informatiebeveiliging. Dit betreft zowel specifieke deelaspecten, de opzet, bestaan en werking van het BBNP als de Normstelling Inrichting Interceptiefaciliteiten.

KORPSBEELD ZUID-HOLLAND-ZUID

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps ten dele geïmplementeerd. Op beleidsniveau is het RIP grotendeels geïmplementeerd en een deel van de maatregelen uit het BBNP is ook geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Zuid-Holland-Zuid heeft in 1999 het informatiebeveiligingsbeleid vastgelegd, welke vervolgens in 2003 geactualiseerd is. In dit beleid wordt aandacht besteed aan de meeste aandachtspunten zoals genoemd in de RIP.
Het korps heeft een beleidsnotitie interceptiefaciliteiten, welke niet afgestemd is met het informatiebeveiligingsbeleid. Deze notitie is ook bekend bij het Openbaar Ministerie.
Voor C2000 is een apart beveiligingsplan opgesteld door het project. De Controller Beveiliging heeft voor dit project het aspect informatiebeveiliging ingevuld.

INFORMATIEBEVEILIGINGSORGANISATIE

De verantwoordelijke voor informatiebeveiliging is de chef DOCC, welke tevens CIO is en lid van het regionaal managementteam. De coördinatie van de activiteiten op het gebied van informatiebeveiliging vindt plaats door de Controller Beveiliging & Privacy.
De hulporganisatie met betrekking tot informatiebeveiliging is initieel wel opgezet door middel van het benoemen van taakaccenthouders informatiebeveiliging, maar bleek in de praktijk niet in stand te houden.
Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatie-beveiliging zijn alleen vastgelegd voor specifieke informatiebeveiligingsfunctionarissen. Doordat de eindverantwoordelijke voor informatiebeveiliging ook CIO is, worden beveiligingsaspecten in ruime zin opgepakt. De CIO en de Controller Beveiliging & Privacy hebben regelmatig overleg.

Met het ISC wordt op drie niveaus overleg gevoerd, namelijk op strategisch (korpschef), tactisch (CIO) en operationeel niveau (service liaison).
Het korps Zuid-Holland-Zuid probeert beveiliging integraal te benaderen. Dit blijkt bijvoorbeeld uit het opgestelde beleid, welke algemeen op beveiliging is gericht en niet enkel op informatiebeveiliging.
De Controller Beveiliging & Privacy houdt zijn deskundigheid op peil door het volgen van cursussen, het bijhouden van vakliteratuur en het bijwonen van landelijke bijeenkomsten van informatiebeveiligingsfunctionarissen.
Voor de interceptiefaciliteiten is de functiescheiding adequaat ingericht. Met betrekking tot de Infodesk is onduidelijk of voldoende functiescheiding aangebracht is.
Het korps Zuid-Holland-Zuid heeft met het ISC momenteel een PDC, SLA en aanvullende afspraken gemaakt. Momenteel is het korps in samenwerking met het korps Rotterdam-Rijnmond wel bezig om een nieuwe PDC en SLA op te stellen. Met betrekking tot de interceptiefaciliteiten heeft het korps afspraken met het ISC, omdat nog geen gebruik gemaakt wordt van het ULI.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps heeft een overzicht met informatiesystemen/gemeenschappelijke ICT-diensten, welke bijgehouden wordt door de Controller Beveiliging & Privacy. Aan alle applicaties zijn ook proceseigenaren gekoppeld, maar dit is niet expliciet vastgelegd.
Het korps heeft niet alle maatregelen uit het BBNP geïmplementeerd. Tevens is onbekend op welke termijn alle maatregelen geïmplementeerd zullen zijn.
Het korps Zuid-Holland-Zuid heeft geen A&K-analyses uitgevoerd. Met betrekking tot de interceptiefaciliteiten is een notitie opgesteld naar aanleiding van de Normstelling Inrichting Interceptiefaciliteiten. De aanbevelingen uit deze notitie zijn geïmplementeerd door het korps.
Het korps heeft geen procedure voor beveiligingsincidenten. Voor de technische beveiligingsincidenten is dit gedeeltelijk ondergebracht bij het ISC en ook vastgelegd in een SLA.
De security awareness van de medewerkers wordt bevorderd door middel van communicatie via intranet en het personeelsblad, maar dit wordt niet planmatig opgepakt.

NALEVING

Informatiebeveiliging is door het korps momenteel niet opgenomen in de evaluatie-cyclus en marap. Dit is momenteel wel een aandachtspunt van het korps, welke opgepakt is door de Controller Beveiliging & Privacy in overleg met de korpscontroller.
Bij het korps Zuid-Holland-Zuid zijn nog geen externe audits uitgevoerd. Jaarlijks vindt een interne quick-scan plaats met betrekking tot de verleende autorisaties voor BPS en RBS. Door Informatie Management is in het kader van de Normstelling Inrichting Interceptiefaciliteiten een interne audit uitgevoerd.

KORPSBEELD ZEELAND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Zeeland nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Zeeland heeft een informatiebeveiligingsbeleid, welke op 10 december 1998 door de korpsbeheerder en de Hoofdofficier van Justitie vastgesteld is. In 2000 is dit beleid voor het laatst geëvalueerd. In dit beleid wordt aandacht besteed aan de aandachtspunten zoals genoemd in de RIP.
Voor de interceptiefaciliteiten wordt gebruik gemaakt van de voorzieningen van het ULI. Het inrichten van de interceptiefaciliteiten conform de Normstelling Inrichting Interceptiefaciliteiten heeft nog niet plaatsgevonden.
Voor C2000 is een informatiebeveiligingsplan opgesteld, waarin het informatie-beveiligingsbeleid kort aangestipt wordt. Dit plan is gezamenlijk opgesteld met de partners binnen C2000. Het informatiebeveiligingsbeleid van het korps Zeeland is hierop nog niet aangepast.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging is de korpsbeheerder, welke het gemandateerd heeft aan de korpschef. Het Hoofd Stafbureau Korpsleiding is verantwoordelijk voor de coördinatie van de informatiebeveiliging. De hulporganisatie is momenteel niet volledig ingericht, omdat er geen informatiebeveiligingsfunctionaris en taakaccenthouders zijn benoemd. In het Formatievoorstel 2007 voor het Stafbureau Korpsleiding is 1fte beschikbaar als informatiebeveiligingsfunctionaris. Momenteel heeft het korps twee medewerkers (privacyfunctionaris en functionaris gegevens-bescherming) welke de IBF-opleiding gevolgd hebben.

Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn niet integraal vastgelegd in de functiebeschrijvingen. De enige uitzondering hierop is de functiebeschrijving van de functionaris gegevensbescherming. Het korps geeft aan dat zij werkt met een functiehuis waarbinnen de algemeen resultaatgerichte functiebeschrijvingen bijdragegebieden bevatten.
Het korps Zeeland benadert informatiebeveiliging vanuit het proces van geautomatiseerde informatievoorziening. Dit betekent dat de aandachtsgebieden mobilofonie, portofonie en telefonie bijvoorbeeld niet onder de informatiebeveiliging vallen.
In verband met de afwezigheid van een hulporganisatie heeft het korps ook geen opleidingsplan. Ook voor de privacyfunctionaris en functionaris gegevensbescherming is geen opleidingsplan aanwezig, maar worden opleidingen op basis van behoefte gevolgd. Deze medewerkers houden hun deskundigheid op peil door middel van collegiaal overleg en het volgen van regionale/landelijke themadagen en/of symposia.
De functiescheiding met betrekking tot de interceptiefaciliteiten en de Infodesk moet blijken uit de functiebeschrijvingen. Voor de interceptiefaciliteiten is dit niet expliciet beschreven voor het korps, terwijl voor de Infodesk in 2004 door middel van een externe audit aangetoond is dat voldaan werd aan de geldende ABRIO-regelingen.
Met ISC-Zuid zijn door de CIO afspraken gemaakt welke vastgelegd zijn in de SLA. Het beheer van de SLA wordt uitgevoerd door de service liaison. Landelijk wordt momenteel actie ondernomen om afspraken met het KLPD te maken voor de interceptiefaciliteiten.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps heeft een overzicht met informatiesystemen/gemeenschappelijke ICT-diensten, waarin de proceseigenaren opgenomen zijn. De afdeling Informatiemanagement onderhoudt dit overzicht.
Het korps heeft de maatregelen uit het BBNP nog niet allemaal geïmplementeerd. Tevens zijn nog niet alle maatregelen gedocumenteerd. Het korps heeft momenteel geen concreet plan met betrekking tot het implementeren van de overige maatregelen uit het BBNP.
Het korps Zeeland heeft nog geen A&K-analyses uitgevoerd. Uitzondering hierop is een analyse van de CIE-bestanden door het zuidelijke samenwerkingsverband. De Normstelling Inrichting Interceptiefaciliteiten wordt door het korps grotendeels nageleefd, maar dit is nog niet geformaliseerd.
Het korps heeft geen afzonderlijke richtlijnen met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten. In het informatiebeveiligingsbeleid is hiervoor een korte procedure opgenomen. Tevens zal hiervoor aangesloten worden bij de procedure welke op landelijk niveau door het CIP ontwikkeld wordt.
De security awareness van medewerkers wordt bevorderd door briefings, werkbesprekingen en functioneringsgesprekken. Hiervoor zal structurele aandacht komen door aansluiting te zoeken bij de werkgroep van het zuidelijke samenwerkingsverband, die dit op gaat pakken.

NALEVING

Informatiebeveiliging is door het korps in 2006 opgenomen in de Beleids- en Beheercyclus. Tot op heden zijn enkele interne audits uitgevoerd met betrekking tot de informatiebeveiliging binnen het korps Zeeland. De resultaten van de audits waren deels voldoende.

KORPSBEELD MIDDEN- EN WEST-BRABANT

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Midden- en West-Brabant ten dele geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Midden- en West-Brabant heeft een beleid uit 2000 van voor de oprichting van het ISC en het CIP. Dit is dus niet meer actueel. Door IBF-Zuid (samenwerkingsverband tussen de IBF-ers van de zuidelijke zes korpsen) is recent een meerjarenplan opgesteld met daarin de activiteiten die in de komende drie jaar uitgevoerd zullen worden. Midden- en West-Brabant volgt dit meerjarenplan, maar dat is formeel nog niet door de korpsleiding bekrachtigd. Het oude beleid besteedt aandacht aan de aandachtspunten zoals genoemd in de RIP.
Het concept beveiligingsreglement/interceptiereglement is in concept aangeboden aan de contactpersoon Interceptie van het Openbaar Ministerie Breda en akkoord bevonden. Het beheer van deze interceptiefaciliteiten is niet belegd in het meerjarenplan/beleid.
Het beveiligingsbeleid voor C2000 is niet belegd in het meerjarenplan/beleid. C2000 is opgepakt als een apart traject, welke zich nu in de afrondende fase bevindt. Momenteel wordt de overdracht van het project naar de lijnorganisatie per 1 januari 2007 besproken.

INFORMATIEBEVEILIGINGSORGANISATIE

Vanaf 1 juli 2006 is de proceseigenaar informatievoorziening verantwoordelijk voor de informatiebeveiliging. De proceseigenaar is tevens portefeuillehouder informatiebeveiliging. De coördinatie van de informatiebeveiligingsactiviteiten is de verantwoor-

delijkheid van het Hoofd Unit Veiligheid en Integriteit. Een beveiligingsfunctionaris is aangesteld bij de afdeling Recherche en tevens heeft de districtschef van Bergen op Zoom een verantwoordelijkheid voor informatiebeveiliging. De hulporganisatie voor informatiebeveiliging bestaat uit de proceseigenaar informatievoorziening (portefeuillehouder informatiebeveiliging), het Hoofd Unit Veiligheid en Integriteit, de beveiligingsfunctionaris van de afdeling Recherche en de CIO. De oorspronkelijke situatie met decentrale IBF-ers/TIB-ers functioneerde niet naar tevredenheid.
De taken, bevoegdheden en verantwoordelijkheden zijn volgens het korps vastgelegd voor de functies welke gerelateerd zijn aan informatiebeveiliging.
De communicatie met het CIP en het ISC vindt plaats door één CIO van IBF-Zuid. De CIO's voeren in het kader van IBF-Zuid regelmatig overleg en service level management is de portefeuille van één van de deelnemende CIO's. Tevens heeft elk korps service coördinatoren ISC, welke regelmatig overleggen in IBF-Zuid verband.
Het opstellen van opleidingsplannen is in de lijn belegd en niet specifiek geregeld voor informatiebeveiligingsfunctionarissen. In de praktijk vindt dit plaats door middel van activiteiten binnen IBF-Zuid en de landelijke IBF-dagen.
Voor de interceptiefaciliteiten is de functiescheiding niet gewaarborgd door de aanwezigheid van slechts één tapkamerbeheerder. Voor de Infodesk is de functiescheiding wel gewaarborgd.
In de afspraken tussen het korps Midden- en West-Brabant en het ISC en CIP wordt aandacht besteed aan informatiebeveiligingsaspecten, maar nog niet alle aspecten zijn hierin meegenomen. Momenteel wordt dit onder andere door IBF-Zuid en de CIO's van de zuidelijke regio's in samenwerking met het ISC en CIP opgepakt. Voor de interceptiefaciliteiten is nog niet voorzien in afspraken met het KLPD over de beveiligingsmaatregelen met betrekking tot de gegevensuitwisseling.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Midden- en West-Brabant heeft een overzicht van informatiesystemen, waarin de meeste systeemeigenaren ingevuld zijn. Het onderhoud van dit overzicht vindt plaats door de WijzigingsAdviesCommissie (WAC). Geschat is door middel van het invullen van het Wegingsinstrument dat 90% van de maatregelen uit het BBNP geïmplementeerd is. Voor de implementatie van de laatste 10% is geen implementatieplan opgesteld.
Voor GMK, C2000 en de recherchesystemen zijn A&K-analyses uitgevoerd door het korps. De resultaten hiervan zijn verwerkt in voorstellen met betrekking tot beveiliging en toegangsbeveiliging voor gebouwen en de afvoer van elektronische gegevensdragers. Voor de interceptiefaciliteiten is aanvullend op de RIP en de leidraad algemene beveiligingsmaatregelen een beveiligingsreglement opgesteld. Dit reglement is gebaseerd op de Normstelling Inrichting Interceptiefaciliteiten, welke ook gebruikt zal gaan worden binnen de andere korpsen van IBF-Zuid. Door de hoge werkdruk en onderbezetting op de afdeling Interceptie is dit reglement nog concept en is nog geen A&K-analyse uitgevoerd.

Binnen het korps ontbreekt een algemene richtlijn met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten. Het korps heeft het voornemen het incidentbeheer verder te gaan inrichten. Voor de interceptiefaciliteiten is dit vastgelegd in het concept beveiligingsreglement.
Binnen IBF-Zuid wordt gewerkt aan een communicatieplan voor informatiebeveiliging. Daarnaast is het korps Midden- en West-Brabant bezig met een bewustwordingscampagne als onderdeel van het verbeteringsproject 'Sterke Diender'. De bewustwordingscampagne is onderdeel van het beveiligingsplan informatiebeveiliging.

NALEVING

In het kader van het veld Informatie binnen het INK-model wordt er door de CIO's van de zuidelijke korpsen elk kwartaal gerapporteerd over informatiebeveiliging.
Tot op heden zijn nog geen interne of externe audits uitgevoerd met betrekking tot de informatiebeveiliging bij het korps Midden- en West-Brabant.

KORPSBEELD BRABANT-NOORD

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide SStelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Brabant-Noord ten dele geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Brabant-Noord had een informatiebeveiligingsbeleid van 1999, welke gedurende twee jaar geldig was. Sindsdien is dit beleid niet meer geactualiseerd of geëvalueerd. Inmiddels hebben de zes zuidelijke regio's een meerjarenplan/beleid 2006-2008 opgesteld. Het beleid uit 1999 besteedt aandacht aan de aandachtspunten zoals genoemd in de RIP, terwijl hiervoor minder aandacht is in het meerjarenplan/beleid 2006-2008 van de zes zuidelijke regio's.
Het korps heeft een specifieke normstelling met betrekking tot het beheer van de interceptiefaciliteiten opgesteld inclusief plan van aanpak. Tevens is een beveiligingsreglement opgesteld en een notitie interceptie van de zes zuidelijke regio's.
Het beveiligingsbeleid voor C2000 is niet belegd in het informatiebeveiligingsbeleid met uitzondering van een korte verwijzing (aandachtspunt).

INFORMATIEBEVEILIGINGSORGANISATIE

De korpsbeheerder is verantwoordelijk voor de informatiebeveiliging en deelt deze verantwoordelijkheden, taken en bevoegdheden toe aan de leidinggevenden binnen het korps. Dagelijks verantwoordelijke voor de beveiliging van de informatievoorziening en de bescherming van de privacy is de korpschef. De werkzaamheden worden in Brabant-Noord concreet uitgevoerd/gecoördineerd door twee fulltime medewerkers, waarvan één formeel informatiebeveiligingsfunctionaris is. De hulporganisatie voor informatiebeveiliging bestaat uit de informatiebeveiligingsfunctionaris en de taakaccenthouders van de vijf districten binnen de regio Brabant-Noord.

De taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn vastgelegd in de functieomschrijvingen.
De communicatie met het CIP en het ISC vindt plaats door één CIO van IBF-Zuid. De CIO's voeren in het kader van IBF-Zuid regelmatig overleg en service level management is de portefeuille van één van de deelnemende CIO's. Tevens heeft elk korps service coördinatoren ISC, welke regelmatig overleggen in IBF-Zuid verband.
Het korps heeft geen specifiek opleidingsplan opgesteld voor de hulporganisatie voor informatiebeveiliging. Een deel van de taakaccenthouders heeft de TIB-opleiding gevolgd en eind 2006 heeft de informatiebeveiligingsfunctionaris de IBF-opleiding gevolgd. Daarnaast wordt ad hoc invulling gegeven aan het op peil houden van de kennis van de informatiebeveiligingsfunctionaris.
Voor de interceptiefaciliteiten en de Infodesk is de functiescheiding gewaarborgd.
In de afspraken tussen het korps Brabant-Noord en het ISC en CIP wordt aandacht besteed aan informatiebeveiligingsaspecten, maar nog niet alle aspecten zijn hierin meegenomen. Momenteel wordt dit onder andere door IBF-Zuid en de CIO's van de zuidelijke regio's in samenwerking met het ISC en CIP opgepakt. Voor de interceptiefaciliteiten is nog niet voorzien in afspraken met het KLPD over de beveiligingsmaatregelen met betrekking tot de gegevensuitwisseling.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Brabant-Noord heeft een overzicht van informatiesystemen, welke onderhouden wordt door de WijzigingsAdviesCommissie. Het korps heeft per informatiesysteem geen eigenaar aangewezen, maar men is bezig om informatiesystemen te koppelen aan proceseigenaren. Het korps heeft geen inzicht in de mate waarin het BBNP geïmplementeerd is. Voor de implementatie is het Wegingsinstrument niet gebruikt. Dit instrument is wel gebruikt voor het beveiligingsplan CIE.
Een aantal jaar geleden zijn A&K-analyses gemaakt, maar het is onduidelijk hoe de resultaten hiervan verwerkt zijn. De Normstelling Inrichting Interceptiefaciliteiten is door het korps uitgewerkt in een Beveiligingsreglement Interceptie Politie Brabant-Noord.
De aanzet tot een procedure met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten is opgenomen in het informatiebeveiligingsbeleid. Onderdeel van het meerjarenplan 2006-2008 is het opzetten van zo'n procedure. De incidenten worden gemeld bij de informatiebeveiligingsfunctionaris, welke deze ook vastlegt.
Binnen IBF-Zuid wordt gewerkt aan een communicatieplan voor informatiebeveiliging. Daarnaast is het korps Brabant-Noord bezig om een communicatieplan voor bewustwording uit te werken.

NALEVING

Informatiebeveiliging is door het korps nog niet opgenomen in de evaluatiecyclus. Tot op heden zijn nog geen interne of externe audits uitgevoerd met betrekking tot de informatiebeveiliging bij het korps Brabant-Noord. Eind 2006 werd een externe audit uitgevoerd met betrekking tot de opzet, bestaan en werking van het BBNP.

KORPSBEELD BRABANT-ZUID-OOST

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Brabant-Zuid-Oost grotendeels geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Brabant-Zuid-Oost heeft een informatiebeveiligingsbeleid, welke op 1 januari 1999 in werking is getreden voor twee jaar. Het beleid is sindsdien (deels) geëvalueerd, maar nog niet geactualiseerd. Het beleid voldoet aan de richtlijnen van de RIP.
De interceptiefaciliteiten zijn niet expliciet opgenomen in het informatiebeveiligingsbeleid. De korpschef heeft de uitvoering van de Normstelling Inrichting Interceptiefaciliteiten belegd bij het hoofd Divisie Recherche. Het Openbaar Ministerie is betrokken geweest bij de inrichting van de nieuwe interceptiefaciliteiten.
C2000 is niet expliciet opgenomen in het informatiebeveiligingsbeleid. De verantwoordelijkheid hiervoor is belegd binnen de afdeling Regionaal Communicatie- en Informatie Centrum (RCIC).

INFORMATIEBEVEILIGINGSORGANISATIE

Door de korpsleiding is een lijnmanager (hoofd O&I) aangewezen als themaverantwoordelijke voor informatiebeveiliging. De coördinatie van de informatiebeveiligingswerkzaamheden vindt plaats door de informatiebeveiligingsfunctionaris en de taakaccenthouders. De hulporganisatie voor informatiebeveiliging bestaat uit de genoemde medewerkers.
Het korps Brabant-Zuid-Oost heeft in de functiebeschrijvingen deels aandacht voor taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging.
De IBF-ers van de zes zuidelijke regio's, het ISC en het CIP overleggen maandelijks.

Op tactisch niveau wordt door de CIO's overlegd en op strategisch niveau door de plaatsvervangend korpschefs. De strategische afspraak hierover is niet alleen samenwerking, maar het werken vanuit één virtuele O&I-organisatie ten behoeve van de zes zuidelijke korpsen.
Het korps Brabant-Zuid-Oost heeft geen eisen voor de deskundigheid van de medewerkers van de hulporganisatie opgenomen in het opleidingsplan. De deskundigheid van de informatiebeveiligingsfunctionaris wordt op peil gehouden door functiespecifieke opleidingen (MSIT en MSIM) en deelname aan relevante seminars/congressen en landelijke en regionale bijeenkomsten/vergaderingen/projecten/werkgroepen.
De functiescheiding met betrekking tot de interceptiefaciliteiten is formeel niet geregeld en ook in de praktijk is deze niet adequaat in verband met de personele bezetting. Binnen de Infodesk is dit volgens het korps wel geregeld, omdat via het procesmodel Regionale Infodesken gewerkt wordt.
Met ISC-Zuid zijn afspraken gemaakt met betrekking tot de betrouwbaarheid van informatiesystemen en de beveiliging van informatie door middel van een SLA. Hierin is niets opgenomen met betrekking tot de wijze waarop zekerheid wordt verkregen over de betrouwbaarheid van de informatiesystemen en de informatie. In het kader van de interceptiefaciliteiten zijn afspraken gemaakt met het KLPD in een DVO en NOK.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps Brabant-Zuid-Oost heeft de beschikking over de zogenaamde groene lijst, waarop de toegestane informatiesystemen voor de zes zuidelijke regio's worden bijgehouden. Deze wordt bijgehouden door de WijzigingsAdviesCommissie (WAC) onder regie van de CIO's van de regio's. De systeemeigenaren zijn niet formeel aangewezen, maar voor een deel vastgelegd in de regionale autorisatieprocedure.
Het korps Brabant-Zuid-Oost is nog bezig met de implementatie van het BBNP en ziet dit als een continu proces. De implementatie is veelal op basis van thema's opgepakt, waarbij geen gebruik gemaakt is van het Wegingsinstrument, maar van een eigen zelfevaluatie-instrument. Dit wordt in de praktijk echter niet gebruikt.
Tot op heden is in het verband van de zes zuidelijke regio's een A&K-analyse uitgevoerd voor het RBS gericht op de CIE-registers. Naar aanleiding van de resultaten is inmiddels een deel van de punten geëffectueerd. Daarnaast blijft nog een aantal punten over welke financieel, technisch of uit werkbaar oogpunt niet haalbaar zijn. Het korps heeft bij de inrichting en beheer zoveel mogelijk rekening gehouden met de Normstelling Inrichting Interceptiefaciliteiten. Formeel is dit echter niet omschreven en vooral de functiescheiding verdient hierbij nog aandacht.
Het korps heeft in het informatiebeveiligingsbeleid een procedure opgenomen voor de melding en afhandeling van informatiebeveiligingsincidenten. Deze procedure is verder uitgewerkt in het informatiebeveiligingsplan van de betrokken organisatieonderdelen.

De security awareness wordt bevorderd op de volgende manieren:

- Voorlichting/presentaties voor specifieke groepen van medewerkers.
- Folders en gadgets.
- Intranet (onder andere een maandelijks document over bijzonderheden met betrekking tot informatiebeveiliging en rubriek laatste nieuws voor bijvoorbeeld ernstige incidenten).
- Het opstellen van een communicatieplan is een actiepunt in Zuidelijk Nederland verband.

NALEVING

Informatiebeveiliging is geen onderdeel van de beleidsevaluatiecyclus. Momenteel worden hiervoor acties ondernomen. Binnen het korps zijn nog geen audits uitgevoerd met uitzondering van een externe audit op de opzet van het BBNP binnen twee organisatieonderdelen.

KORPSBEELD LIMBURG-NOORD

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Limburg-Noord nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Limburg-Noord heeft nog geen informatiebeveiligingsbeleid. Deze lacune is door het korps onderkend en het informatiebeveiligingsbeleid zal nog in 2006 aangeboden worden aan de korpsbeheerder. Bij het opstellen van het beleid zal aandacht worden besteed aan de aandachtspunten zoals genoemd in de RIP.
Bij het stellen van de eisen voor de inrichting van de interceptiefaciliteiten is het Openbaar Ministerie van Roermond niet betrokken.
Voor C2000 is een informatiebeveiligingsplan opgesteld voor 2005, waarin het informatiebeveiligingsbeleid kort aangestipt wordt. De gestelde betrouwbaarheidseisen zijn ontleend aan de RIP en het beveiligingsbeleid C2000 (van het Ministerie van Binnenlandse Zaken). De IBF-er is niet verantwoordelijk voor de inspectie en controle hiervan. De eindverantwoordelijkheid is belegd bij de plaatsvervangend korpschef.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging, de korpsbeheerder, delegeert zijn verantwoordelijkheden aan de korpschef. De beleidsvoorbereiding is de verantwoordelijkheid van de Security Officer, welke tevens de verantwoordelijke functionarissen voor informatiebeveiliging op de afdelingen ondersteunt bij het opstellen van specifieke informatiebeveiligingsplannen. De operationale informatiebeveiligingswerkzaamheden en de coördinatie daarvan zijn belegd bij de IBF-er.
Taken, bevoegdheden en verantwoordelijkheden zijn nog niet integraal vastgelegd.

Hierop zal aandacht gevestigd worden bij het opstellen van het informatiebeveiligingsbeleid. Enkele verantwoordelijkheden zijn nu reeds benoemd in de bestaande beleidsdocumenten en informatiebeveiligingsplannen met betrekking tot de interceptiefaciliteiten of C2000.
Afstemming met het CIP en het ISC vindt plaats middels een service liaison of via de CIO. De IBF-er heeft naar beiden geen formele ingang. De afstemming over informatiebeveiliging vindt dan ook plaats binnen het samenwerkingsverband IBF-Zuid.
Informatiebeveiliging is door het korps ondergebracht in de bredere veiligheidsbenadering. Aan deze benadering wordt momenteel alleen invulling gegeven door het project voor de vervanging van het toegangscontrolesysteem.
Binnen het korps wordt geen structurele aandacht besteed aan het op peil houden van de deskundigheid van de IBF-er en andere medewerkers welke verantwoordelijk zijn voor informatiebeveiliging.
In de inrichting van het Buro Interceptie is de functiescheiding voor de interceptiefaciliteiten uitgewerkt naar aanleiding van de A&K-analyse. Hierbij wordt geen aandacht besteed aan informatiebeveiliging, waardoor de functiescheiding met betrekking tot de informatiebeveiliging hierin ontbreekt. Voor de Infodesk heeft de lijnchef vooralsnog de aanwijzingen met betrekking tot informatiebeveiliging niet meegenomen bij de inrichting.
De IBF-er is niet betrokken bij het contractbeheer, waardoor met informatiebeveiligingsaspecten meestal geen rekening wordt gehouden. De DAP's en SLA's met het CIP en het ISC zijn de verantwoordelijkheid van de CIO. De definitieve SLA van februari 2006 is op een dermate abstract niveau dat beveiligingsaspecten hierin niet zijn beschreven.
Voor de interceptiefaciliteiten zijn afspraken belegd met het KLPD over de beveiligingsmaatregelen met betrekking tot de gegevensuitwisseling.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps is momenteel bezig met het project Uitvoering BBNP. Onderdeel van dit project is een inventarisatie van de informatiesystemen inclusief de systeem- en proceseigenaren. De inventarisatie is gereed en de systeem- en proceseigenaren worden momenteel benoemd. De maatregelen uit het BBNP zullen op basis van een prioritering geïmplementeerd worden. Het korps zal hierbij geen gebruik gaan maken van het Wegingsinstrument, omdat dit instrument niet onderhouden is.
Voor de interceptiefaciliteiten en RBS zijn A&K-analyses uitgevoerd door het korps. De resultaten hiervan zijn nog niet verwerkt. In de A&K-analyse van de interceptiefaciliteiten zijn de te nemen maatregelen vanuit de Normstelling Interceptiefaciliteiten meegenomen.
Binnen het korps ontbreekt een algemene richtlijn met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten. Voor zowel de interceptiefaciliteiten als C2000 is wel een aanzet voor een richtlijn opgesteld, maar deze zijn nog niet volledig.

Het korps onderkent dat de security awareness van de medewerkers nog bevorderd moet worden. Hiervoor is momenteel nog geen structurele aandacht, maar acties hiervoor worden momenteel bovenregionaal geïnitieerd en bij de implementatie van het BBNP zal hieraan ook aandacht geschonken worden door middel van workshops.

NALEVING

Informatiebeveiliging is door het korps nog niet verweven in het INK-proces en daardoor nog niet geborgd. Tot op heden zijn nog geen interne of externe audits uitgevoerd met betrekking tot de informatiebeveiliging bij het korps Limburg-Noord.

KORPSBEELD LIMBURG-ZUID

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Limburg-Zuid nog onvoldoende geïmplementeerd.

INFORMATIEBEVEILIGINGSBELEID

Het korps Limburg-Zuid heeft een informatiebeveiligingsbeleid, welke echter nog niet ingebed is in de organisatie. In het beleid is weinig tot geen aandacht besteed aan de aandachtspunten zoals genoemd in de RIP, omdat de organisatie in Limburg-Zuid met name wordt gestuurd op de uitvoering in plaats van op de beleidsvorming.
Voor de inrichting van de interceptiefaciliteiten zijn aparte beleidsdocumenten opgesteld aan de hand van de landelijke richtlijnen, welke niet geïntegreerd zijn in het algemene informatiebeveiligingsbeleid. Het Openbaar Ministerie is hierbij zijdelings betrokken, maar dit is niet geformaliseerd.
De informatiebeveiliging van C2000 is landelijk opgepakt. Limburg-Zuid was een pilot korps en hierdoor is C2000 operationeel in de lijn. Hiervoor zijn ook aparte beleidsdocumenten opgesteld, welke niet geïntegreerd zijn in het algemene informatiebeveiligingsbeleid.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging, de korpsbeheerder, delegeert zijn verantwoordelijkheden aan de korpschef. Het korps heeft hiernaast geen informatiebeveiligingsorganisatie. Inmiddels is formatie toegekend om de functie voor de informatiebeveiligingsfunctionaris (IBF) in te kunnen vullen en taken, verantwoordelijkheden en bevoegdheden toe te kennen. Het streven is om dit nog in 2006 ingevuld te hebben. Momenteel wordt gebruik gemaakt van de diensten van de IBF van Limburg-

Noord en wordt geconformeerd aan de gemaakte afspraken in IBF-Zuid verband. Taken, bevoegdheden en verantwoordelijkheden zijn nog niet integraal vastgelegd. Alleen voor de CIO zijn expliciet taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging opgenomen in zijn functiebeschrijving. Afstemming met het CIP en het ISC vindt plaats middels een service liaison (tactisch en operationeel) of via de CIO (strategisch). De informatiebeveiligingsfunctionarissen werken samen in IBF-Zuid verband en adviseren vanuit dit verband aan de CIO's. Door de afwezigheid van een informatiebeveiligingsorganisatie wordt geen structurele aandacht besteed aan het op peil houden van de deskundigheid hiervan.
De functiescheiding voor de interceptiefaciliteiten is niet formeel vastgelegd, maar in de praktijk wordt gewerkt met een opdrachtgever, een uitvoerende medewerker en een afdelingschef. De uitvoering en administratie zijn echter niet gescheiden. Voor de infodesk is de functiescheiding belegd door de implementatie van de landelijke regeling Infodesk.
Binnen het contractbeheer wordt niet structureel rekening gehouden met informatiebeveiligingsaspecten. Ook in de SLA met het CIP en het ISC is niet expliciet rekening gehouden met de informatiebeveiligingsaspecten. Op een beperkt aantal gebieden zijn op operationeel gebied wel afspraken gemaakt. Voor de interceptiefaciliteiten zijn alleen mondelinge afspraken gemaakt met het KLPD over de beveiligingsmaatregelen met betrekking tot de gegevensuitwisseling.

INFORMATIEBEVEILIGINGSMAATREGELEN

In IBF-Zuid verband heeft een inventarisatie van de informatiesystemen inclusief de systeem- en proceseigenaren plaatsgevonden. Dit overzicht wordt door de WijzigingsAdviesCommissie (WAC) onderhouden in samenwerking met het CIP. De maatregelen uit het BBNP zijn deels in de uitvoering geïmplementeerd, maar een structurele aanpak is hiervoor nog niet gevolgd en de status van implementatie is niet bekend. Het implementeren van het BBNP zal een taak worden van de aan te stellen IBF.
Voor het RBS is in het zuidelijke samenwerkingsverband een A&K-analyse uitgevoerd. Hoe de resultaten hiervan verwerkt worden is niet bekend aangezien dit ook door het zuidelijke samenwerkingsverband plaatsvindt. Voor de interceptiefaciliteiten is de Normstelling Inrichting Interceptiefaciliteiten als richtlijn gebruikt voor de inrichting, maar deze normstelling wordt nog niet volledig nageleefd.
Binnen het korps ontbreekt een algemene richtlijn met betrekking tot het melden, registreren en afhandelen van beveiligingsincidenten. Voor C2000 is dit wel geregeld in het beveiligingsplan C2000.
Aan de security awareness van de medewerkers wordt momenteel geen structurele aandacht geschonken.

NALEVING

Informatiebeveiliging is door het korps nog niet verweven in het INK-proces en daardoor nog niet geborgd. Tot op heden zijn nog geen interne of externe audits uitgevoerd met betrekking tot de informatiebeveiliging bij het korps Limburg-Zuid.

KORPSBEELD FLEVOLAND

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van de RIP is door het korps Flevoland ten dele geïmplementeerd. In 2005 is het korps begonnen met prioriteit te geven aan informatiebeveiliging.

INFORMATIEBEVEILIGINGSBELEID

Het korps Flevoland heeft een informatiebeveiligingsbeleid, welke in 1999 vastgesteld is voor twee jaar en vervolgens nog niet geëvalueerd is. In het beleid zijn de aandachtspunten zoals genoemd in de RIP opgenomen.
De interceptiefaciliteiten zijn niet geïntegreerd in het informatiebeveiligingsbeleid. De Normstelling Inrichting Interceptiefaciliteiten is door het korps Flevoland overgenomen en geïmplementeerd.
Het informatiebeveiligingsbeleid van C2000 is niet ingebed in het informatiebeveiligingsbeleid, omdat het gezamenlijk opgesteld is binnen de veiligheidsregio. Het beleid voor C2000 is volgens het korps wel in lijn met het informatiebeveiligingsbeleid, omdat beiden gebaseerd zijn op de RIP. Het beleid voor C2000 was al opgesteld voordat het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties het informatiebeveiligingsbeleid publiceerde.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor informatiebeveiliging, de korpsbeheerder, delegeert zijn verantwoordelijkheden aan de korpschef. De regionale beveiligingsfunctionaris is verantwoordelijk voor de coördinatie van de informatiebeveiligingsactiviteiten. De hulporganisatie van het korps Flevoland bestaat uit de informatiebeveiligingsfunctionaris, de Chef Politiële Beleidsondersteuning en de informatiebeveiliging auditor.

Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn vooral vastgelegd voor de functies welke gerelateerd zijn aan informatiebeveiliging. Naar aanleiding van een uitgevoerde nulmeting heeft het MT momenteel een actiepunt om informatiebeveiliging onderdeel te laten uitmaken van ontwikkel- en functioneringsgesprekken.
Afstemming met het CIP en het ISC vindt plaats middels overleggen op diverse niveaus (onder andere CIO's met directeur CIP, procesmanagers met de programmamanagers CIP, CIO met directeur VG ISC).
Het opleidingsplan voor de hulporganisatie wordt opgesteld aan de hand van de behoefte. Dit geldt voornamelijk voor nieuwe medewerkers, welke de gewenste opleidingen krijgen om zo snel mogelijk op het noodzakelijke kennisniveau te zitten. De deskundigheid van de informatiebeveiligingsfunctionaris wordt op peil gehouden door het volgen van opleidingen/cursussen, het bezoeken van seminars, workshops en bijeenkomsten en het bijhouden van vakliteratuur en de beschikbare informatie op internet.
De functiescheiding voor de interceptiefaciliteiten en de Infodesk worden vooral geregeld door middel van de aanwezige functiescheiding in de automatiseringssytemen. Dit is niet geformaliseerd.
In de SLA en PDC met het CIP en het ISC is rekening gehouden met de informatiebeveiligingsaspecten. Deze aspecten komen ook weer naar voren bij het service level management, waarvan de rapportages maandelijks besproken worden met het ISC.

INFORMATIEBEVEILIGINGSMAATREGELEN

Voor de overgang naar ISC-Midden is een overzicht opgesteld van de informatiesystemen/gemeenschappelijke IT-diensten, welke door middel van het proces configuration management door het ISC onderhouden wordt. In een tabel op intranet staat opgenomen wie de proceseigenaren of portefeuillehouders zijn voor de informatiesystemen.
Uit de nulmeting van voorjaar 2006 komt naar voren dat het BBNP nog niet geheel geïmplementeerd is door het korps. Van het gebruikersdeel is 45% geïmplementeerd, 30% deels, 23% niet en van 2% is de status onbekend. Het korps heeft vervolgens het Wegingsinstrument gebruikt voor het opstellen van een implementatieplan. De bedoeling is om begin 2007 de stand van zaken met betrekking tot het gebruikersdeel als volgt te laten zijn: 66% geïmplementeerd, 19% deels, 13% niet en van 2% blijft de status onbekend.
Het korps Flevoland heeft nog geen A&K-analyses uitgevoerd. Voor de interceptiefaciliteiten is de Normstelling Inrichting Interceptiefaciliteiten als richtlijn gebruikt voor de inrichting.
Binnen het korps bestaat een procedure voor het melden, registreren en afhandelen van beveiligingsincidenten. Naar aanleiding van incidenten worden vervolgens maatregelen getroffen op technisch, disciplinair en communicatief gebied.

Incidenten kunnen herkend worden door medewerkers doordat deze tijdens IBT-sessies (integrale beroepsvaardigheidstraining) en vanuit de integriteitssessies geleerd hebben wat 'afwijkend' is.
Het korps probeert aandacht te besteden aan de security awareness, waarbij vooral ingespeeld wordt op de actualiteit, maar uit de nulmeting is duidelijk geworden dat de awareness nog verder bevorderd moet worden.

NALEVING

Informatiebeveiliging is door het korps nog niet verweven in de evaluatiecyclus en daardoor nog niet geborgd. Momenteel is het korps bezig om in samenwerking met het korps Gooi en Vechtstreek te werken aan een beleid, welke voor beide korpsen zal gaan gelden. In de laatste INK-audit (2003) is informatiebeveiliging aan de orde geweest. Voor de overdracht van de automatisering in 2005 aan ISC-Midden is door een medewerker van ISC-Midden een audit uitgevoerd naar de status van hoofdstuk 3 van het BBNP. In het voorjaar van 2006 heeft het korps zelf een nulmeting uitgevoerd met betrekking tot de status van de implementatie van het BBNP. Tevens is in de Monitor Kwaliteit Gegevens van 4 april 2006 aandacht besteed aan de informatiebeveiliging binnen het korps.

KORPSBEELD KLPD

In het korpsbeeld wordt achtereenvolgens ingegaan op de volgende onderwerpen:

- Algemeen beeld en conclusie
- Informatiebeveiligingsbeleid
- Informatiebeveiligingsorganisatie
- Informatiebeveiligingsmaatregelen
- Naleving

ALGEMEEN BEELD EN CONCLUSIE

In dit onderdeel wordt antwoord gegeven op de onderzoeksvraag: 'In hoeverre is het van de RIP afgeleide Stelsel voor Informatiebeveiliging Politie door het korps geïmplementeerd, conform de toenmalige aanbevelingen van het Expertisecentrum Informatiebeveiliging Politie?'
Het Stelsel voor Informatiebeveiliging Politie zoals afgeleid van het RIP is deels door het KLPD geïmplementeerd. De technische maatregelen zijn meegenomen bij het ontwerp en de inrichting van de nieuwe infrastructuur (PROMIS en later NIS). De organisatorische maatregelen zijn grotendeels beschreven en vormen een onderdeel van het sourcing traject (overdracht IT van het KLPD aan het ISC). De implementatie van de organisatorische maatregelen moet deels nog plaatsvinden.

INFORMATIEBEVEILIGINGSBELEID

Het informatiebeveiligingsbeleid en de bijbehorende rubriceringsregeling zijn goedgekeurd door de korpsleiding en de korpschef. Er wordt gewerkt aan een nieuwe versie van het informatiebeveiligingsbeleid, waarin de opmerkingen van de auditdienst van BZK (uitgebracht 1e kwartaal 2006) mee worden genomen. Belangrijke opmerkingen van de auditdienst waren:

- het inzichtelijk maken van de samenhang tussen het voorgestelde informatiebeveiligingsbeleid en de algemene uitgangspunten en randvoorwaarden van het informatiebeleid van het KLPD;
- de volledigheid van de inventarisatie van wet- en regelgeving die een relatie heeft met het informatiebeveiligingsbeleid van het KLPD (bv. Wet Politieregisters);
- de organisatie van de informatiebeveiligingsfunctie, met name de mate van functiescheiding bij BV&I tussen het opstellen van het informatiebeveiligingsbeleid, het adviseren hierover en de controle op de uitvoering van het beleid.

De interceptiefaciliteiten van het KLPD bestaan uit diverse uitluisterstations en de Unit Landelijke Interceptie (ULI). Deze unit verzorgt de interceptie voor de meerderheid van de regionale politiekorpsen en het KLPD zelf. Het KLPD heeft aangegeven dat er aandacht wordt geschonken aan de maatregelen in de normstelling interceptie.

Een interne audit op de decentrale interceptie faciliteiten heeft echter nog niet plaatsgevonden. Voor de ULI is een afhankelijkheids- en kwetsbaarheidanalyse uitgevoerd en er loopt een onderzoek door de auditdienst van BZK naar de informatiebeveiliging van de ULI. Hierin wordt ook gekeken naar de bestuurlijke omgeving.
In de huidige versie van het informatiebeveiligingsbeleid is er geen aandacht besteed aan C2000. In de nieuwe versie van dit beleid wordt een verwijzing opgenomen naar het C2000 beleid.

INFORMATIEBEVEILIGINGSORGANISATIE

De eindverantwoordelijke voor de informatiebeveiliging is de korpsbeheerder. De korpsbeheerder heeft deze verantwoordelijkheid gemandateerd aan de korpschef van het KLPD. De korpschef heeft op zijn beurt deze verantwoordelijkheid 'doorgemandateerd' naar het hoofd van het Bureau Veiligheid en Integriteit (BV&I). Deze afdeling bestaat uit 6 fte.
Het hoofd van het Bureau Veiligheid & Integriteit (BV&I) wordt aangewezen als Beveiligingscoördinator (in lijn met het Beveiligingsvoorschrift 2005), waarmee hij de taken van Beveiligingsambtenaar uitvoert voor het KLPD en binnen de kaders zoals die door de BVA van het Ministerie van BZK zijn gesteld. Hoofd BV&I ressorteert in de uitvoering van zijn werkzaamheden rechtstreeks onder de korpschef.
Taken, bevoegdheden en verantwoordelijkheden van de beveiligingscoördinator zijn nog niet integraal vastgelegd. De functieomschrijving wordt op dit moment opgesteld en wordt opgenomen in een instructie voor de beveiligingscoördinator.
Het KLPD zit in verschillende werkgroepen van het CIP gerelateerd aan informatiebeveiliging (bv. landelijke rubriceringsregeling, werkgroep bewustwording, herziening stelsel). Daarnaast neemt het KLPD deel in het landelijk IBF overleg en diverse ad hoc samenwerkingsverbanden.
Het KLPD benadert de informatiebeveiliging integraal. Het informatiebeveiligingsbeleid maakt onderdeel uit van het Handboek integrale veiligheid KLPD.
Bij de afdeling Informatiemanagement en bij het BV&I zijn een aantal informatiebeveiligingsfunctionarissen aangesteld. De informatiebeveiligingsfunctionaris houdt zijn kennis en deskundigheid op peil door middel van opleidingen, congressen, seminars, literatuur en contacten met deskundigen. Een concreet opleidingsplan conform het Stelsel voor Informatiebeveiliging politie is niet opgesteld maar er is wel een regelmatig bijgewerkt document met opleidingen die functionarissen van het BV&I minimaal moeten hebben gevolgd.
De functiescheiding met betrekking tot de centrale interceptiefaciliteiten wordt onderzocht in het lopende onderzoek naar de ULI. Met betrekking tot de decentrale uitluisterstations van het KLPD wordt de functiescheiding om technische redenen niet nageleefd. Het systeem kan een beheeraccount in enkelvoud aanmaken. Systeembeheerders per locatie zijn hierdoor gedwongen om samen met één beheeraccount te werken. De acties van de normale gebruikers zijn wel te herleiden door het

gebruik van individuele user accounts. Het KLPD is in gesprek met de leveranciers van het systeem over deze kwestie. De leverancier heeft een oplossing voorgesteld. Deze oplossing wordt als toereikend beschouwd en zal nu door de leverancier gebouwd gaan worden.
Het KLPD is bezig om met het ISC-Midden afspraken te maken wat betreft informatiebeveiliging. De parapluovereenkomst is inmiddels geformaliseerd. De SLA, PDC en DAP zijn af en zijn groeidocumenten. In deze documenten komen beveiligingsaspecten naar voren.

INFORMATIEBEVEILIGINGSMAATREGELEN

Het korps heeft een overzicht van alle informatiesystemen. Dit overzicht wordt beheerd door de afdeling CDI. Dit overzicht wordt onderhouden in verband met de overdracht van het beheer van deze systemen naar het ISC. Voor de belangrijkste systemen, die het primaire proces ondersteunen, is een eigenaar toegewezen.
Het Korps heeft deels het BBNP ingevoerd. Ondermeer door bij de vernieuwing van de infrastructuur (project PROMIS en later NIS) rekening te houden met de technische maatregelen. De organisatorische maatregelen zijn grotendeels beschreven en vormen een onderdeel van het sourcing traject (overdracht IT van het KLPD aan het ISC). De implementatie van de organisatorische maatregelen moet deels nog plaatsvinden. De inschatting van het KLPD is dat dit traject medio 2007 wordt afgerond. Tevens is door het KLPD een beveiligingsarchitectuur opgesteld die momenteel gefaseerd wordt geïmplementeerd. Direct na het van kracht worden van het Stelsel voor Informatiebeveiliging Politie is het bijbehorende Wegingsinstrument gebruikt om per dienst van het KLPD een 'top vijf' van de te nemen maatregelen te maken. Deze top-5 werd periodiek bijgewerkt. Bij de invoering van PROMIS is deze werkwijze stil komen te liggen.
Het KLPD heeft een beperkt aantal A&K-analyses uitgevoerd. Eén op de ULI en één op het Havank systeem. Een externe partij heeft een A&K-analyse uitgevoerd op het Operationeel Centrum Driebergen. Tevens zijn er A&K-analyses uitgevoerd op het koppelvlak tussen C2000 en GMS en het koppelvlak tussen GMS en telefonie.
In het Handboek Integrale Veiligheid staan de procedures beschreven voor het afmelden, registreren en het afhandelen van beveiligingsincidenten.
Er wordt gewerkt aan de security awareness binnen de organisatie. Men heeft een presentatie gehouden voor het korpsmanagementteam en het handboek staat sinds 17-11-2006 op het intranet. Men is ook van plan om een bewustwordingscampagne op te gaan starten. Hierin wordt korpsbreed het beveiligingsbeleid onder de aandacht gebracht van de medewerkers door onder andere posters, intranet, korpsmagazine et cetera. Dit plan wordt pas opgestart nadat alle MT's van de onderdelen van het KLPD zijn geïnformeerd over het beleid en de kans hebben gehad om zelf de eerste stappen te nemen met de invoering hiervan.

NALEVING

Informatiebeveiliging is verweven in het INK-proces. In het informatiebeveiligingsbeleid staan concrete beveiligingsdoelen genoemd voor de lopende INK-cyclus. In het najaar van 2005 is er een audit uitgevoerd op het informatiebeveiligingsbeleid en de rubriceringsregeling door de departementale auditdienst van BZK. Interne audits worden niet uitgevoerd, ondermeer doordat de functie van interne auditor bij het KLPD nog niet is ingevuld. Aangegeven is dat vanwege krapte op de arbeidsmarkt deze functie niet kan worden ingevuld.

GOOD PRACTISES

Het KLPD begint nu met het uitvoeren van het informatiebeveiligingsbeleid. Onder andere door middel van verschillende pilotprojecten bij verschillende onderdelen van het KLPD. Deze geven inzicht in de haalbaarheid en de kosten (ook in manuren) van de implementatie van het beleid.

Het informatiebeveiligingsbeleid is onderdeel van het Handboek Integrale Veiligheid KLPD. Dit handboek is in de zomer van 2006 door de korpsleiding vastgesteld. Dit handboek bevat het beveiligingsbeleid van het KLPD. Bovendien bevat het een aantal regelingen, waarin het beleid is uitgewerkt in concrete maatregelen.
Met het opstellen van dit beleidskader zijn twee belangrijke stappen gezet: ten eerste dat hiermee (gedeeltelijk) wordt voldaan aan vigerende wet- en regelgeving, ten tweede dat duidelijkheid wordt verkregen over de beveiligingseisen waaraan het KLPD dient te voldoen.
Het beleidskader zet de grote lijnen van de beveiliging uiteen, stelt generieke eisen vast en geeft de verantwoordelijkheden omtrent beveiliging weer. De grote lijnen van het beleid worden uitgewerkt in regelingen en voorschriften om tot concrete maatregelen te komen. Hiermee is al een begin gemaakt met bijvoorbeeld de rubriceringsregeling, de regeling thuiswerken en de instructie voor het melden en afhandelen van beveiligingsincidenten.

Naast het Handboek Integrale Veiligheid KLPD is ook de nieuwe Beveiligingsarchitectuur KLPD vastgesteld. De ontwikkeling van de beveiligingsarchitectuur sluit nauw aan bij de bedrijfsarchitectuur en procesarchitectuur van het KLPD. Per architectuurlaag zijn de bijbehorende beveiligingsaspecten weergegeven. De beveiligingsarchitectuur is in nauwe samenwerking met ISC en CIP tot stand gekomen en wordt op dit moment gerealiseerd.

Het proces Integrale Veiligheid van het Bureau Veiligheid & Integriteit heeft structureel ingeregeld dat afstemming op beveiligingsonderwerpen plaatsvindt met Informatie Management en het Facilitair Bedrijf.

Bijlage: Toelichting scoringsmethodiek

V

Voor de verschillende onderdelen hebben alle korpsen een score gekregen van 1 tot en met 5, waarbij 1 de laagste en 5 de hoogste score is. Er zijn alleen hele getallen als score gegeven, dus 1, 2, 3, 4 of 5. De norm voor score 5 is dat geheel wordt voldaan aan de geldende wet- en regelgeving en dat het Stelsel voor Informatiebeveiliging (IB) van de Nederlandse politie geheel (conform de geldende afspraken) is geïmplementeerd. De scores 1 tot en met 5 kunnen dan ook niet worden gezien als rapportcijfers, waarbij een score vanaf de 6 al als een voldoende wordt gezien. In dit onderzoek zouden alle korpsen dus eigenlijk op alle onderdelen een 5 moeten scoren.

In de tabel hieronder is weergegeven welke criteria (op hoofdlijnen) zijn gehanteerd voor de scores 1, 3 en 5. De tussenliggende scores 2 en 4 zijn op basis van professional judgement en op basis van onderlinge vergelijking van de korpsen toegekend.

Normen	1	3	5
A. Informatiebeveiligingsbeleid			
Aanwezigheid en actualiteit informatiebeveiligingsbeleid	Geen beleid aanwezig	Concept beleid of niet actueel beleid aanwezig	Vastgesteld en actueel beleid
Interceptiebeleid[1]	Geen verwijzing en geen apart interceptiebeleid/-reglement	Geen verwijzing en apart interceptiebeleid/-reglement	Verwijzing en apart interceptiebeleid/-reglement
C2000 beveiligingsbeleid[2]	Geen verwijzing en geen apart C2000-beleid/-plan	Geen verwijzing en apart C2000-beleid/-plan	Verwijzing en apart C2000-beleid/-plan
B. Organisatie informatiebeveiligingsfunctie			
Taken, verantwoordelijkheden en bevoegdheden (TVB)	TVB voor IB zijn niet benoemd	TVB voor IB zijn alleen benoemd en beschreven voor specifieke IB-functies	TVB voor IB zijn voor alle functies benoemd en beschreven
Hulporganisatie	Geen informatiebeveiligingsorganisatie aanwezig	Discontinue (hulp)organisatie voor IB korps heeft lang zonder informatiebeveiligingsfunctionaris gefunctioneerd	Volledige (hulp)organisatie voor IB aanwezig
Functiescheiding Interceptiefaciliteit[3]	Geen aantoonbare functiescheiding aanwezig	Wel functiescheiding aanwezig, maar beperkt beschreven	Aantoonbare functiescheiding aanwezig sterke controlerende rol van Regionaal

1 Vanuit het (informatie)beveiligingsbeleid dient er een verwijzing te zijn naar het geldende beleid en de geldende reglementen met betrekking tot de interceptiefaciliteiten.
2 Vanuit het (informatie)beveiligingsbeleid dient er een verwijzing te zijn naar het geldende beleid met betrekking tot C2000.
3 De Normstelling Inrichting Interceptiefaciliteiten stelt een aantal functiescheidingen tussen beheerfuncties, gebruikersfuncties en toezichthoudende functies verplicht.

Normen	1	3	5
Functiescheiding Infodesk Afspraken gegevens-uitwisseling en ICT-dienstverlening	Geen aantoonbare functie-scheiding aanwezig Geen afspraken gemaakt met ketenpartners op het gebied van IB	Wel functiescheiding aanwezig, maar beperkt beschreven Minimale afspraken gemaakt met ketenpart-ners op het gebied van IB	Interceptie Coördinator Aantoonbare functie-scheiding aanwezig Specifieke afspraken op het gebied van IB met ketenpartners
C. Informatiebeveiliging			
Overzicht informatie-systemen	Geen overzicht van informatiesystemen, geen systeemeigenaren aangewezen	Overzicht aanwezig van informatiesystemen, geen systeemeigenaren aangewezen	Overzicht aanwezig van informatiesystemen, systeemeigenaren aangewezen
Implementatie BBNP	Status onbekend en niet aantoonbaar	Status bekend en aantoon-baar, BBNP deels geïmplementeerd	Status bekend en aantoon-baar, BBNP (nagenoeg) geheel geïmplementeerd
A&K-analyses	Geen A&K-analyses uitgevoerd	Alleen A&K-analyses voor kritische systemen uitgevoerd	A&K-analyses voor alle systemen uitgevoerd
Interceptiemaatregelen	Interceptiefaciliteiten voldoen niet aan norm-stelling, status onbekend	Interceptiefaciliteiten voldoen bijna aan norm-stelling, status bekend en aantoonbaar	Interceptiefaciliteiten voldoen aan normstelling, status bekend en aantoonbaar
Beveiligingsincidenten	Geen incidentenregistratie op het gebied van IB	Geen procedure voor incidentmelding, registratie van IB-incidenten	Procedure voor incident-melding aanwezig, registratie van IB-incidenten
Security Awareness	Geen of weinig aandacht voor security	Aandacht voor en activitei-ten op het gebied van awareness, niet planmatig	Planmatige aandacht voor en activiteiten op het gebied van awareness
D. Naleving			
Evaluatiecyclus	Geen evaluatie van IB-beleid en -maatregelen	Ad hoc evaluatie van IB-beleid en -maatregelen	Systematische evaluatie van IB-beleid en –maat-regelen– evaluatie geïntegreerd in INK
Onafhankelijk oordeel werking BBNP	Geen audits uitgevoerd	Alleen interne audits uitgevoerd	Recente externe audit uitgevoerd
Audit interceptie-faciliteiten	Geen audit uitgevoerd	Alleen interne audits uitgevoerd	Recente externe audit uitgevoerd
Systeemverwerving	Geen activiteiten op het gebied van systeem-verwerving	Steunen op landelijke ontwikkelingen van systemen	Actieve rol in (landelijke) systeemverwerving

Bijlage: Overzicht publicaties van het stelsel

VI

HET STELSEL VOOR DE AANPAK VAN DE INFORMATIEBEVEILIGING

Regelgeving:	Regeling Informatiebeveiliging Politie (RIP)
Brochure:	Uitgangspunten informatiebeveiliging
Handreiking:	Beleidsvorming informatiebeveiliging
Leidraad:	Organisatie van de informatievoorziening
Handreiking:	Beheer informatiesystemen
Bijlage 2 handreiking beheer:	Beheer ICT dienstverlening
Methode:	Afhankelijkheid- en Kwetsbaarheidanalyse (A&K-analyse)
Leidraad:	Algemene Beveiligingsmaatregelen (ABM)
Leidraad:	Basisbeveiligingsniveau Ned. Politie (BBNP)
Handreiking:	Werkplekbeveiliging
Bijlage 2	Handreiking werkplekbeveiliging: Leidinggevenden
Handreiking:	Windows NT
Leidraad	Auditing
Handreiking:	Certificering
Leidraad:	Classificeren van informatie

HULPMIDDELEN VOOR HET TOEPASSEN VAN HET STELSEL

Middelen:

Handreiking:	Sterkte – zwakte analyse
Tool:	Expertsysteem Afhankelijkheid- en Kwetsbaarheidanalyse (ESAKa)
Bijlage leidraad ABM:	Wegingsinstrument
Tool:	Wegingsinstrument ‘geautomatiseerde versie’
Bijlage 1 leidraad Auditing:	Onderzoeksinstrumenten
Bijlage 2 leidraad Auditing:	Onderzoekswijzer
Bijlage 1 handreiking werkplekbeveiliging:	Internetgebruik
Bijlage 3 handreiking werkplekbeveiliging:	Communicatiemiddelen en gegevensdragers
Bijlage 1 handreiking beheer:	Onderzoeksinstrumentarium voor beheer
Methode:	Afhankelijkheid- en Kwetsbaarheidanalyse voor de fysieke beveiliging (A&K-analyse)
Bijlage methode A&K fysieke beveiliging:	Maatregelen fysieke beveiliging

Handreiking:	Autorisatie
Handreiking:	ICT Verificatie en Analyse Test
Brochure:	Wet- en regelgeving
Folder:	Verstrekkingen uit politieregisters
Folder:	Omgaan met informatie

Bewustwording:

Workshop:	Kennismaken met informatiebeveiliging
Presentatie:	Introductie informatiebeveiliging
Presentatie:	Beveiligingssituatie informatievoorziening in de politiesector
Presentatie:	Ongeoorloofde informatieverstrekking
Presentatie:	Communicatiemiddelen en gegevensdragers
Video:	Let op je computer
Video:	De zwakke schakel in de computer-beveiliging
Video:	Computerfraude voorkomen
Video:	ISO 9000, de interne audit
Video:	Ruw materiaal
Video:	De “M” van Nico
Handleiding:	Scenario Exercitie; tactisch en operationeel niveau
Handleiding:	Scenario Exercitie; strategisch niveau
Brochure:	Beveiligingsincidenten I
Brochure:	Beveiligingsincidenten II

RANDVOORWAARDEN VOOR DE IMPLEMENTATIE VAN HET STELSEL

Handreiking:	Hulporganisatie voor de informatie-beveiliging
Opleidingsprogramma:	Seminar portefeuillehouder informatie-beveiliging Opleiding voor Informatiebeveiligings-functionarissen (IBF) Examenprogramma IBF-opleiding Opleiding voor Taakaccenthouders Informatiebeveiliging Opleiding (interne) Auditor informatiebeveiliging Examenprogramma Interne Auditor Training gebruik tool Expertsysteem Afhankelijkheid- en Kwetsbaarheidanalyse (ESAKa)

Bijlage: Relevante literatuur voor het onderdeel over het stelsel

VII

1. *Beveiligingskader voor de politiële informatievoorziening,* Beleidsadviescollege Politiële informatievoorziening (BPI), Sdu Uitgeverij, 1993.
2. *Handboek aanpak informatiebeveiliging politie,* Platform Politiële informatievoorziening (PPI), Houten, 1995.
3. *Onderzoek naar de beveiligingssituatie van de informatievoorziening*, Platform Politiële informatievoorziening (PPI), Houten, 1996.
4. *Informatiebeveiliging: 'wiens zaak is dat?',* drs. M.H.L.G. Heijnens MIM en H. Klap RI MPM, Tijdschrift van de Politie, september 1996.
5. *Informatiebeveiliging,* drs. M.H.L.G. Heijnens MIM, Handboek Politiemanagement, december 1997.
6. *Regeling Informatiebeveiliging Politie*, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Den Haag, 17 maart 1997, en zoals gewijzigd op 30-8-2004, nr. EA2004/60705.
7. *Uitgangspunten Informatiebeveiliging Brochure*, Expertisecentrum Informatiebeveiliging Nederlandse Politie, Den Haag, 4 juni 1998, eerste versie.
8. Het *stelsel voor de aanpak van de informatiebeveiliging*, diverse publicaties, Den Haag, periode 1997 tot en met 2002.
9. *Productencatalogus*, Brochure, Expertisecentrum Informatiebeveiliging Nederlandse Politie, Den Haag, 1 april 2002, tweede gewijzigde versie.
10. *De activiteiten van het Expertisecentrum Informatiebeveiliging Nederlandse Politie: een tussentijdse evaluatie,* M&I Partners, Amersfoort, 25 november 1999.
11. *Eindverslag Expertisecentrum Informatiebeveiliging Nederlandse Politie*, Den Haag, 10 april 2002.
12. *Eindevaluatie Expertisecentrum Informatiebeveiliging Nederlandse Politie*, M&I Partners, Amersfoort, 14 december 2001.

Bijlage: Samenstelling begeleidingscommissie Inspectie OOV onderzoek naar informatie-beveiliging politie

VIII

Aan deze commissie namen de volgende personen deel:

R. Gooskens	Directie Strategie, DGV, ministerie van BZK
H. Klap	namens Directie Strategie
J. Lentink	Directie Politie, DGV, ministerie van BZK
C. Schreuder	Directie Politie, DGV, ministerie van BZK
D. Meijer	Auditdienst ministerie van BZK
T. Schaap	Auditdienst ministerie van BZK
W. Schel	Directie Strategie, DGV, ministerie van BZK
W. van Andel	Inspectie OOV
L. Koolen (projectleider)	Inspectie OOV
M. van Slingerland	Inspectie OOV
I. Soeltan (secretariaat)	Inspectie OOV

Vanuit PricewaterhouseCoopers hebben de volgende personen deelgenomen aan het project:

P. Groen	Leiding van het onderzoek bij de 25 regiokorpsen, 25 korpsbezoeken en rapportage aan de Inspectie OOV
E. Zaaiman	Ondersteuning P. Groen
A.J.M. de Bruijn	Verantwoordelijk partner vanuit PricewaterhouseCoopers, advisering P. Groen