Samen werken, samen beveiligen

Informatiebeveiliging bij de Nederlandse politie

maart 2007
Inspectie Openbare Orde en Veiligheid

Inhoudsopgave

Bijlage 2 t/m 8: op cd aanleveren

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 dit hoofdstuk wordt eerst ingegaan op de implementatie van informatiebeveiliging bij de politiekorpsen en de actualiteit van het huidige Stelsel voor informatiebeveiliging: een korte samenvatting, gevolgd door conclusies en aanbevelingen, daarna wordt het thema informatiebeveiliging bij interceptie belicht. Beide hoofdstukken 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 (RIP) 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 vijf 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 C-2000 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 (o.m. fysiek, personeel 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. Vaak 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 samenwerkings-verband 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 o.a. 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 vijf). 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.

<u>Beleid</u>

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 Kwetsbaarheidsanalyses) voor informatiesystemen om vast te stellen of voldoende informatiebeveiligingsmaatregelen 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 basisbeveiligingsniveau 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 incidentenregistraties op het gebied van interne onderzoeken, ICT-helpdesk, fysieke toegangsbeveiliging 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 politiemedewerkers 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 beleidsevaluatie- 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; informatiebeveiliging 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 informatiebeveiligingsplannen 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 de 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 wordt 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 werkinstructies) 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.

Hoofdstuk 1
Inleiding en aanleiding

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 verantwoordelijkheids-toedeling binnen de organisatie en de toepassing van audits. Kortom alle fases 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 de 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 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 departementale 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 managementcyclus 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 van 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:

<u>Voorbereiding:</u>
Allereerst werden de verplichtingen die voortvloeien uit 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 bij deze rapportage gevoegd.

<u>Bestuderen documentatie en houden interviews</u>
Bestuderen van beschikbare documentatie (onder meer de korps antwoorden en -documentatie uit het Inspectie onderzoek naar kwaliteit van opsporing (2005/6) 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 SLA) daaromtrent met de korpsen) en het CIP (gericht op (verdere) ontwikkeling en onderhoud van een Stelsel van informatiebeveiliging) nodig.

Schriftelijke vragenlijsten

Schriftelijke vragenlijst voor de regiokorpsen en het KLPD met betrekking tot naleving van de RIP en implementatie van het Stelsel 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 Informatie Beveiligings Functionaris (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 dit hoofdstuk een aantal zogenaamde good practices belicht. Hoofdstuk 6 gaat over informatiebeveiliging ten aanzien van interceptie. De bijlagen, die overigens op de bijgevoegde CD 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.

Hoofdstuk 2

ICT bij de politie, een terugblik

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[1] 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[2] 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[3]. 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.

Motie Rietkerk

Op 21 november 2000 heeft de Tweede Kamer de motie-Rietkerk aangenomen (Tweede Kamer, 2000-2001, nr. 48). 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 de minister van BZK verzocht om jaarlijks te rapporteren over de voortgang. De minister van BZK heeft toegezegd om deze motie uit te voeren.

[1] Tweede Kamer, vergaderjaar 2003-2004, 29 350, nrs. 1-2

[2] Tweede Kamer, 1998-1999, 26 3445, nr. 15.

[3] 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.

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.

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 publiekrechtelijke rechtspersonen. Dit is inmiddels gebeurd met de oprichting van vtsPN op 1 juli 2006.

Midterm Review
Medio 2003 heeft Het Expertisecentrum 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 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

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

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 (vts Politie Nederland) 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 vts Politie Nederland. De minister van BZK heeft bij de oprichting van de vts Politie Nederland een aantal criteria gesteld op basis waarvan hij het functioneren van vts Politie Nederland zal beoordelen. Deze criteria zijn vastgelegd in het zogenaamde Referentiekader. Er is door het opgaan van de vraagorganisatie en de aanbodorganisatie in de voorziening tot samenwerking Politie Nederland 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
Vts Politie Nederland 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.

Hoofdstuk 3

Het Stelsel voor de aanpak van de informatiebeveiliging

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 **B**eschikbaarheid (doen de systemen het als het erop aankomt?), **E**xclusiviteit (is informatie voldoende afgeschermd?) en **I**ntegriteit (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.

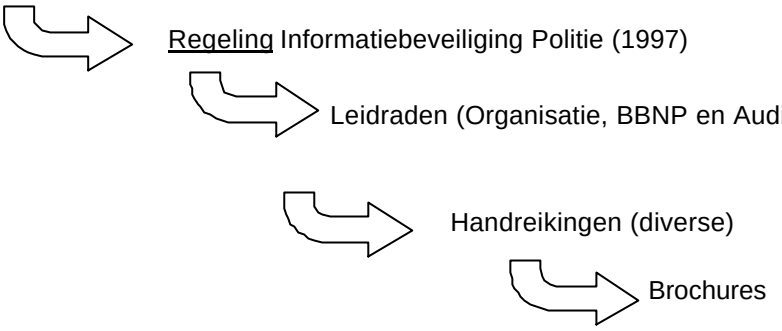
Stelsel voor de aanpak van de informatiebeveiliging
De uitwerking van de RIP is bij ministeriële regeling door de ministers van BZK en van Justitie belegd bij het Expertisecentrum Informatiebeveiliging Nederlandse Politie (ECIB). Bij beschikking (nr. EIB97/u258) van de ministers van BZK en van Justitie 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 de bijlagen bij dit rapport 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.
Politiewet 1993



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 eindigt 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).

Hoofdstuk 4
Nadat het Stelsel is overgedragen

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 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 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 informatiebeveiliging
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 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 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 BBNP te implementeren als erg zwaar ervaren, gezien het grote aantal maatregelen en het detailniveau van BBNP; bovendien is 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 informatiegestuurde 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 BBNP bedoeld als een minimumbeveiligingsniveau, waar alle korpsen aan zouden moeten voldoen. Dat minimumniveau 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 BBNP heeft ingevoerd heeft bepaald wel iets om trots op te zijn.

Hoofdstuk 5
Implementatie van informatiebeveiliging bij de Nederlandse politie

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 de bijlagen 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 overdracht van taken naar ISC (ICT-Service Coöperatie Politie, Justitie en Veiligheid en later de voorziening tot samenwerking Politie Nederland, vtsPN), de introductie van C-2000 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 (o.m. fysiek, personeel 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 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 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. Vaak 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

Overall		
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 meldkamerprocessen. 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 zich voor C2000 in het kader van interne beheersing belast is met de vereiste periodieke bijstelling van beveiligingsplannen en de daaraan gerelateerde rapportageactiviteiten.

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

[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.

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 informatiebeveiliging, 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

Beleid		
Rang	**Korpsnaam**	**Score**
1	Noord- en Oost-Gelderland	4,33
	Zaanstreek-Waterland	4,33
	Amsterdam-Amstelland	4,33
2	Fryslân	4,00
3	Groningen	3,67
	IJsselland	3,67
	Noord-Holland Noord	3,67
	Zuid-Holland-Zuid	3,67
	KLPD	3,67

4	Twente	3,33
	Haaglanden	3,33
	Hollands Midden	3,33
	Midden- en West-Brabant	3,33
	Brabant-Noord	3,33
	Brabant-Zuid-Oost	3,33
	Limburg-Zuid	3,33
5	Kennemerland	3,00
	Rotterdam-Rijnmond	3,00
	Zeeland	3,00
	Flevoland	3,00
6	Drenthe	2,67
	Gelderland-Midden	2,67
	Utrecht	2,67
7	Gelderland-Zuid	2,33
	Limburg-Noord	2,33
8	Gooi en Vechtstreek	1,00
	Gemiddeld	3,24

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'er 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 informatiebeveiligings-functionaris 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 het beveiligingsbeleid dient conform dat beleid de controle 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

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 automatiseringsorganisatie 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 betrouwbaarheid 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 informatiebeveiligingsorganisatie. Daarbij is vastgesteld of er een adequate informatiebeveiligingsorganisatie 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

	Organisatie	
Rang	**Korpsnaam**	**Score**
1	Groningen	4,60
	Rotterdam-Rijnmond	4,60
2	Amsterdam-Amstelland	4,40
	Brabant-Noord	4,40
	Brabant-Zuid-Oost	4,40
3	IJsselland	4,20
	Noord- en Oost-Gelderland	4,20
	Hollands Midden	4,20
4	Noord-Holland Noord	3,80
	Zaanstreek-Waterland	3,80

[10] Namens de leidinggevende

	Kennemerland	3,80
	Zuid-Holland-Zuid	3,80
	Midden- en West-Brabant	3,80
	Limburg-Noord	3,80
5	Fryslân	3,60
	Drenthe	3,60
	Gelderland-Midden	3,60
	Gelderland-Zuid	3,60
	Haaglanden	3,60
	Flevoland	3,60
	KLPD	3,60
6	Zeeland	3,40
7	Utrecht	3,20
8	Twente	3,00
	Gooi en Vechtstreek	3,00
	Limburg-Zuid	3,00
	Gemiddeld	3,79

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 zijn 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

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

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

	Evaluatie	
Rang	**Korpsnaam**	**Score**
1	Noord- en Oost-Gelderland	3,75
2	Kennemerland	3,50
	Amsterdam-Amstelland	3,50
	Rotterdam-Rijnmond	3,50
3	IJsselland	3,25
4	Drenthe	3,00
	KLPD	3,00

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

5	Noord-Holland Noord	2,75
	Brabant-Zuid-Oost	2,75
	Flevoland	2,75
6	Groningen	2,50
	Twente	2,50
	Zaanstreek-Waterland	2,50
	Haaglanden	2,50
	Zuid-Holland-Zuid	2,50
	Zeeland	2,50
7	Utrecht	2,00
	Midden- en West-Brabant	2,00
8	Fryslân	1,75
	Gelderland-Midden	1,75
	Gooi en Vechtstreek	1,75
	Hollands Midden	1,75
9	Gelderland-Zuid	1,50
	Brabant-Noord	1,50
	Limburg-Noord	1,50
	Limburg-Zuid	1,50
Gemiddeld		2,45

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 Kwetsbaarheidsanalyses) voor informatiesystemen om vast te stellen of voldoende informatiebeveiligingsmaatregelen 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 basisbeveiligingsniveau 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 incidentenregistraties op het gebied van interne onderzoeken, ICT-helpdesk, fysieke toegangsbeveiliging 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 politiemedewerkers in hoge mate de effectiviteit van de informatiebeveiligingsmaatregelen. Daarom is het zeer belangrijk om proactief te sturen op het juiste gedrag van de politiemedewerkers 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 beleidsevaluatie- 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; informatiebeveiliging 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 informatiebeveiligingsplannen 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.

Hoofdstuk 6
Implementatie Normstelling inrichting interceptiefaciliteiten

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 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.

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.

[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

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.

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

[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

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 bijlagen). 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 er voor 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 kwaliteitsmanagement functie 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.