Quickscan C2000 beveiligingsplannen

Inspectie

OPENBARE ORDE
EN VEILIGHEID

Quickscan C2000 beveiligingsplannen

Inspectie Openbare Orde en Veiligheid

Den Haag

Juli 2008

INSPECTIE OPENBARE ORDE EN VEILIGHEID

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

COLOFON

Uitgave: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Inspectie Openbare Orde en Veiligheid
Lay out: Grafisch Buro van Erkelens
Foto's cover: Fons Sluiter Fotografie
Drukwerk: drukkerij Hega, Den Haag

ISBN 987-90-5414-160-0

juli 2008

Inhoudsopgave

Onze missie

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

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

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

Het oordeel van de Inspectie OOV komt onafhankelijk tot stand.

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

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

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

Samenvatting

STRATEGISCH BEHEERDER, CENTRAAL BEHEERDER

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is eindverantwoordelijk voor de beveiliging van het C2000 Systeem, stelt het Beveiligingsbeleid C2000 vast en draagt het beleid uit. Het strategisch beheer van C2000 is belegd bij en wordt uitgevoerd door de afdeling Informatiebeleid (IB) van de directie Strategie van het Directoraat Generaal Veiligheid (DGV). Het tactisch en operationeel beheer van C2000 wordt uitgevoerd door de afdeling Unit Meldkamer Systemen (UMS) van de voorziening tot samenwerking Politie Nederland (vtsPN), kortweg: de centrale beheerder.

VITAAL SYSTEEM

De minister van BZK heeft het C2000 communicatiesysteem aangewezen als vitaal systeem. Daarmee heeft C2000 het stempel van kritisch systeem en is de beveiliging ervan geen standaardwerk. Het (blijvend) waarborgen van een betrouwbaar C2000 communicatiesysteem heeft ondermeer betrekking op informatiebeveiliging. Informatiebeveiliging is geen eenmalige activiteit maar een proces dat draait om risicobeheersing.

KETENAANGELEGENHEID

Beveiliging van C2000 is een ketenaangelegenheid. De verschillende ketenpartijen dienen daartoe de spelregels van het door de minister van BZK vastgestelde Beveiligingsbeleid C2000 na te leven. Via beveiligingsplannen[1] en vereiste rapportages dragen deze partijen bij aan het beheersen van een betrouwbaar C2000. De beveiligingsplannen bevatten de gemaakte keuzes voor een samenhangend stelsel van beveiligingsmaatregelen. De vereiste rapportages maken onderdeel uit van de op organisatieniveau ingerichte en uitgevoerde periodieke interne controle. Deze rapportages dienen tevens extern (op centraal niveau) te worden aangeboden. De ketenpartijen stellen zelf het actuele beveiligingsniveau binnen de eigen organisatie vast, toetsen dit aan het voorgeschreven niveau en stellen zo nodig hun beveiligingsplannen bij om dit niveau te waarborgen.

ONDERZOEK GERICHT OP

De Inspectie heeft, mede met het oog op het beperken van de toezichtlast, een onderzoek in de vorm van een quick scan uitgevoerd naar inhoud en actualiteit van C2000 beveiligingsplannen en bijbehorende vereiste rapportages.

1 In bijlage III wordt de context van het Beveiligingsbeleid C2000 beschreven in termen van verantwoordelijkheden en uitvoering, uitvoering specifiek op operationeel niveau, en controle.

BEANTWOORDING VAN DE ONDERZOEKSVRAAG

Hebben de centrale beheerorganisatie en de gebruikersorganisaties het Beveiligingsbeleid C2000 geïmplementeerd volgens de aangegeven richtlijnen, hebben zij daartoe beveiligingsplannen opgesteld en rapporteren zij periodiek over de status van de beveiliging?

De Inspectie is van mening dat alvorens deze vraag te beantwoorden een kanttekening op zijn plaats is. In de praktijk blijken de aangegeven richtlijnen en gehanteerde definities multi-interpretabel te zijn. Daarnaast bestaat er een interpretatiebandbreedte voor de controlerende rol van de centrale beheerder.
Samengevat luidt het antwoord op de onderzoeksvraag:

Het Beveiligingsbeleid is door de verschillende partijen met wisselende diepgang geïmplementeerd. De aangetroffen beveiligingsplannen voldoen in beperkte mate aan de gestelde eisen. Geen van de gebruikersorganisaties heeft periodiek aan de centrale beheerder de vereiste rapportages aangeboden. Deze rapportages betreffen de status van de beveiliging in termen van bijstelling beveiligingplan, statusrapportage beveiliging en incidentenrapportages.

BEVEILIGINGSPLANNEN

De aangetroffen beveiligingsplannen zijn met wisselende diepgang opgesteld. Vooral de aspecten actualiteit, beheerparagraaf en calamiteitenparagraaf voldoen niet aan de door het Beveiligingsbeleid gestelde eisen. Veel beveiligingsplannen volstaan met de verwijzing naar de eerder uitgevoerde landelijke generieke Afhankelijkheids- en Kwetsbaarheids-analyses. Voornoemde plannen geven geen dan wel een beperkte toelichting op het ontbreken van de noodzaak tot het treffen van aanvullende maatregelen.

VEREISTE RAPPORTAGES

De Inspectie heeft de vereiste statusrapportages beveiliging C2000 en incidenten-rapportages C2000 niet bij de centrale beheerder aangetroffen. Hierdoor bestaat er centraal geen actueel landelijk beeld over de mate waarin de ketenpartners individueel en in gezamenlijkheid ‘in control’ zijn ten aanzien van de beveiliging van C2000. Deze rapportages zijn van belang, omdat zij het fundament vormen voor sturing en beheersing, zowel binnen iedere organisatie afzonderlijk als binnen de keten.
Navraag bij de regio's leert dat, op een enkel geval na, binnen de regio’s geen actuele statusrapportages beveiliging C2000 voorhanden zijn. Ten aanzien van interne incidenten-rapportages ligt het beeld wat genuanceerder. Ongeveer een kwart van de regio’s zegt interne incidentenrapportages op te stellen. Bij de overige regio’s onderbouwen sommige

regio's het ontbreken van interne incidentenrapportages met óf de frequentie van incidenten, óf een incidentendatabase. De daarbij gegeven toelichting luidt als volgt. Gezien het geringe aantal incidenten wordt ieder apart aan de vtsPN/UMS gemeld incident niet meer in een rapportage verwerkt. En voorts, overzichten van de in een eigen database geregistreerde incidenten kunnen via een rapportgenerator worden opgesteld. De Inspectie heeft – vanwege het ontbreken van een groot aantal van de vereiste rapportages – beperkt zicht op de mate waarin de regio's en de twee landelijke organisaties beveiliging C2000 als proces hebben ingericht en dit proces daadwerkelijk beheersen.

Aanbevelingen

Gericht aan strategisch beheerder DGV/DS/IB:

- Actualiseer het Beveiligingsbeleid naar de gewijzigde situatie waarin tactisch en operationeel beheer van de C2000 infrastructuur is uitbesteed (centrale beheerder).
- Maak, via de beheerovereenkomst, met de centrale beheerder vtsPN/UMS afspraken over de verwerking van en het rapporteren over het beveiligingsplan en de rapportages van de centrale beheerder, plus de centraal aangeboden beveiligingsplannen en rapportages van de gebruikersorganisaties. Bouw tevens een toets op naleving in.
- Maak aanvullend met de regio's en de twee landelijke organisaties afspraken over het actualiseren van beveiligingsplannen, het invulling geven aan de vereiste rapportages en het centraal aanbieden daarvan aan de centrale beheerder vtsPN/UMS. Spreek hiervoor een redelijke termijn af waarbinnen men hieraan moet voldoen.
- Stel een richtlijn op voor beveiligingsplannen voor het verbeteren van de onderlinge aansluiting tussen deze plannen. Verwerk daarin tevens een met de gebruikersorganisaties afgestemd geactualiseerd C2000 normenkader.
- Stel een verantwoordingsrichtlijn op ten behoeve van uniformering van de vereiste rapportages. Betrek hierbij tevens geactualiseerde afspraken over de scheidslijn en de interactie tussen centraal en lokaal beheer. Dit levert een bijdrage aan een transparant en integraal beeld van het (landelijke) beveiligingsniveau.

Gericht aan de gebruikersorganisaties:

- Geef invulling aan de voorgeschreven jaarlijkse actualisering van de beveiligingsplannen en bied deze aan de centrale beheerder vtsPN/UMS aan.
- Geef invulling aan de voorgeschreven jaarlijkse rapportages over de status van de beveiliging en bied deze aan de centrale beheerder vtsPN/UMS aan. Ga daarbij in op de stand van zaken bij de beveiligingsplannen, de implementatie van de beveiligingsmaatregelen en de gehouden controles.
- Geef invulling aan de voorgeschreven jaarlijkse incidentenrapportages en bied deze aan de centrale beheerder vtsPN/UMS aan.

Inleiding

1

1.1 ALGEMEEN

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is als eigenaar en strategisch beheerder van het systeem verantwoordelijk voor een betrouwbaar C2000 communicatiesysteem. Hiertoe stelt de strategisch beheerder doelen en eisen aangaande C2000[2]. De Inspectie Openbare Orde en Veiligheid (Inspectie OOV) vervult hierbij een toezichthoudende rol. Het strategisch beheer van C2000 wordt uitgevoerd door de afdeling Informatiebeleid (IB) van de directie Strategie van het Directoraat Generaal Veiligheid (DGV). Het tactisch en operationeel beheer van C2000 wordt uitgevoerd door de afdeling Unit Meldkamer Systemen (UMS) van de voorziening tot samenwerking Politie Nederland (vtsPN), kortweg: de centrale beheerder. Omdat C2000 deel uitmaakt van de vitale infrastructuur is blijvende aandacht nodig voor het 'in control' zijn betreffende de beveiliging van C2000.

De Inspectie heeft in 2005-2006 een toetsinginstrument voor gebruikersorganisaties (Aangewezen Gebruikers) ontwikkeld en uitgezet bij een tweetal pilot regio's. Bij deze toets zijn bevindingen verzameld over C2000. Op basis van deze bevindingen vermoedt de Inspectie dat op landelijk en regionaal niveau met wisselende diepgang invulling is gegeven aan onder meer de vereiste periodieke (bijstelling van) beveiligingsplannen en rapportages. Daarom is de Inspectie in 2007 een landelijk onderzoek naar de beveiligingsplannen C2000 gestart.

1.2 DOEL- EN VRAAGSTELLING

Het door de minister van BZK eind 2004 vastgestelde Beveiligingsbeleid C2000 schrijft aan de centrale beheerder vtsPN/UMS en aan de gebruikersorganisaties (Aangewezen Gebruikers) voor een beveiligingsplan op te stellen, dit jaarlijks te actualiseren en hierover te rapporteren.
De Inspectie OOV heeft in de tweede helft van 2007 bij voornoemde organisaties een onderzoek uitgevoerd naar inhoud en actualiteit van de betreffende plannen en bijbehorende rapportages. Met dit onderzoek wil de Inspectie OOV een bijdrage leveren aan een adequate beveiliging van C2000.

De doelstelling van dit onderzoek is antwoord te geven op de centrale vraag:
Hebben de centrale beheerorganisatie en de gebruikersorganisaties het Beveiligingsbeleid C2000 geïmplementeerd volgens de aangegeven richtlijnen, hebben zij daartoe beveiligingsplannen opgesteld en rapporteren zij periodiek over de status van de beveiliging?

2 Zie ook het rapport 'Toezicht C2000 stand van zaken 2005-2006' van de Inspectie.

Bij de verdere uitwerking heeft de Inspectie deze vraag vooral als beheersingsvraagstuk benaderd. Beveiligingsplannen en (verantwoordings)rapportages vormen wezenlijke en randvoorwaardelijke schakels om zicht te krijgen en te houden op het beheersen van de beveiliging van C2000 in de praktijk (de werking).

1.3 AANPAK ONDERZOEK

AFBAKENING

Het onderzoek is uitgevoerd bij de vijfentwintig regio's (politie, brandweer, ambulance), de twee landelijke organisaties: het Korps landelijke politiediensten (KLPD) en de Koninklijke Marechaussee (KMar[3]) en bij de centrale beheerder: voorzienig tot samenwerking Politie Nederland/Directie Mobiele Diensten (vtsPN/DMD[4]).
De Inspectie OOV beperkt zich bij de beantwoording van de centrale vraagstelling tot de volgende drie onderzoeksobjecten:

- Beveiligingsplan.
- Status rapportage geïmplementeerde beveiligingsmaatregelen.
- Incidentenrapportage.

Deze documenten dienen conform het Beveiligingsbeleid te zijn aangeboden aan de centrale beheerder.
In dit onderzoek blijven de beveiligingsplannen van toegelaten gelieerden vooralsnog buiten beschouwing. Deze kunnen in een vervolgonderzoek aan bod komen. Wel is het beveiligingsplan van de regio gescand op verwijzingen naar toegelaten gelieerden.

WERKWIJZE

De Inspectie baseert haar bevindingen, conclusies en aanbevelingen van dit onderzoek voornamelijk op documentonderzoek. Daartoe heeft zij via een quick scan de desbetreffende beveiligingsplannen en rapportages getoetst aan een het van het Beveiligingsbeleid afgeleid normenkader (zie bijlage IV).

De vijfentwintig regio's en twee landelijke organisaties moeten conform het Beveiligingsbeleid periodiek beveiligingsplannen en rapportages aanbieden aan de centrale beheerder. Om de toezichtlast te beperken heeft de Inspectie in eerste instantie de bij de vtsPN/UMS opgeslagen documenten in kwestie geïnventariseerd en geanalyseerd.
Per regio en per landelijke organisatie heeft de Inspectie bij contactpersonen een verificatieslag uitgevoerd op actualiteit en bestaan van de drie onderzoeksobjecten (documenten).

Bij dit onderzoek heeft de Inspectie resultaten betrokken uit haar in 2006 bij de politiekorpsen uitgevoerde onderzoek naar informatiebeveiliging: 'Samen werken, samen beveiligen'.

3 Na verkregen toestemming ook bij de Koninklijke Marechaussee (KMar).
4 Lees voor vtsPN/DMD: vtsPN/UMS.

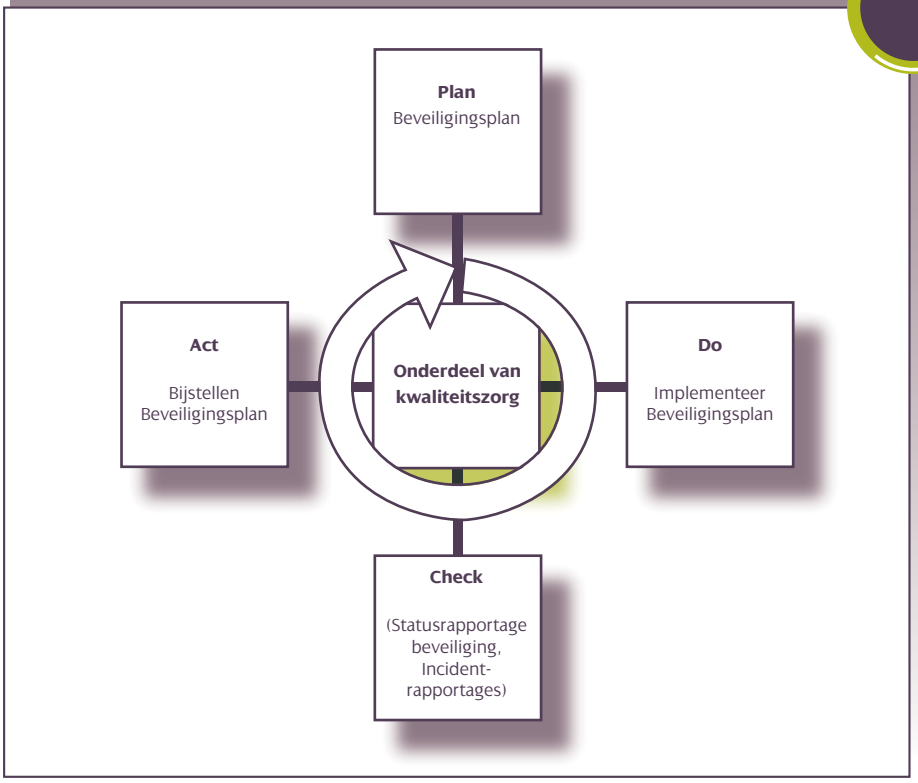
Stand van zaken (beveiligings-plannen en rapportages)

2

2.1 INLEIDING

VOORAF

Citaat uit het Beveiligingsbeleid C2000:
'Beveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de integrale kwaliteitszorg voor bedrijfs- en bestuursprocessen. Lijnfunctionarissen (leidinggevenden) hebben de primaire verantwoordelijkheid voor het kiezen, uitvoeren en handhaven van beveiligingsmaatregelen.'



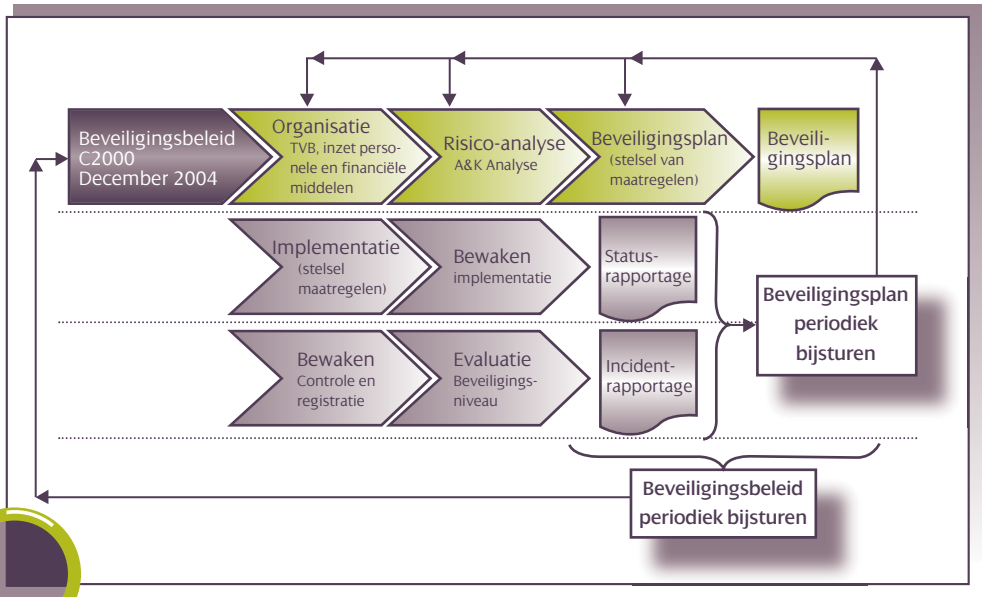
BEVEILIGING

In een beveiligingsplan staat een samenhangend stelsel van beveiligingsmaatregelen beschreven, zowel op tactisch als op operationeel niveau, waarmee een organisatie een bepaald beveiligingsniveau wil bereiken en handhaven voor één of meerdere systemen.

Om (een redelijke mate van) zekerheid te hebben of het beveiligingsniveau in werkelijkheid aan de daaraan te stellen eisen voldoet, is het noodzakelijk dat een organisatie zicht heeft op een aantal zaken. Twee zaken spelen daarbij een belangrijke rol: welke beveiligingsmaatregelen zijn al geïmplementeerd (de status van implementatie) en welke risico's hebben zich gemanifesteerd (voorgevallen incidenten). Via periodieke meetmomenten (waaronder statusrapportage beveiliging en incidentenrapportages) kan een organisatie vervolgens besluiten tot bijstelling van het beveiligingsplan ter waarborging van het vereiste beveiligingsniveau.

DE SCHAKELS IN BEELD

Hieronder volgt een schematische weergave van de bij beveiliging C2000 betrokken schakels in termen van deelprocessen en bijbehorende (verantwoordings)output. Het beveiligingsplan, de statusrapportages en de incidentenrapportages bevatten voor het management van een organisatie noodzakelijke informatie om sturing te kunnen geven aan het vereiste betrouwbaarheidsniveau. De kwaliteit van de statusrapportages is mede afhankelijk van de in het beveiligingsplan beschreven maatregelen. Met andere woorden, wanneer het beveiligingsplan in beperkte mate ingaat op de te treffen maatregelen, dan zal de bijbehorende statusrapportage beperkt inzicht verschaffen over de nog te treffen maatregelen.
Het geheel aan beveiligingsplannen en rapportages van de verschillende partijen bevat voor de strategisch beheerder belangrijke sturingsinformatie om haar Beveiligingsbeleid periodiek te kunnen bijstellen.



TOETSING

De Inspectie heeft het bij dit onderzoek gehanteerde normenkader voor beveiligingsplannen en rapportages afgeleid van de eisen uit het Beveiligingsbeleid en uitgesplitst naar formele aspecten en inhoudelijke aspecten. De formele documentaspecten hebben betrekking op vaststelling (ondertekend op het juiste managementniveau), frequentie (minimaal jaarlijks), datering (van recente datum), verwijzingen (beheer en calamiteitenplan) en op het aanbieden aan de centrale beheerder. De inhoudelijke documentaspecten (afbakening in verantwoordelijkheidsgebieden, maatregelen per verantwoordelijkheidsgebied, beheer- en calamiteitenplan) zijn rechtstreeks overgenomen uit het Beveiligingsbeleid.

2.2 BEVEILIGINGSPLANNEN GEBRUIKERSORGANISATIES

ALGEMEEN

Bij de vtsPN/UMS zijn vierentwintig[5] beveiligingsplannen aangetroffen. De Inspectie heeft daarnaast de via het onderzoek 'Samen werken, samen beveiligen' opgevraagde (multidisciplinaire) beveiligingsplannen C2000 bij het onderzoek betrokken en een verificatieslag uitgevoerd op actualiteit. In totaal heeft de Inspectie achtentwintig[6] beveiligingsplannen getoetst.

De landelijke organisaties (het KLPD en de KMar) hebben, inherent aan het type organisatie, monodisciplinaire beveiligingsplannen opgesteld. Met uitzondering van één regio[7] hebben alle veiligheids-/politieregio's een multidisciplinair beveiligingsplan opgesteld.
De Inspectie heeft in dit onderzoek niet nader onderzocht in hoeverre in deze regio's onderliggende monodisciplinaire beveiligingsplannen zijn opgesteld, omdat er geen verplichting bestaat deze onderliggende documenten centraal aan te bieden.

Vijf regio's hebben gekozen voor het opsplitsen van hun multidisciplinaire beveiligingsplan in twee afzonderlijke plannen: een voor het meldkamerdomein en een voor randapparatuur.
Vijf andere regio's hebben in hun muldisciplinaire beveiligingsplan de focus voornamelijk op het meldkamerdomein gericht. Randapparatuur kwam daarbij beperkt aan bod.
In de overige beveiligingsplannen van gebruikersorganisaties gaat naar de mening van de Inspectie meer aandacht uit naar het meldkamerdomein dan naar randapparatuur.

VIJF ONDERDELEN

De aangetroffen beveiligingsplannen zijn volgens het eerder genoemde normenkader getoetst op vijf onderdelen:

- actualiteit (vaststelling, frequentie bijstelling, datering);
- afbakening in verantwoordelijkheidsgebieden (leidinggevende, functies, relatie

5 Plannen van 21 regio's, 2 landelijke organisaties, 1 centrale beheerder.
6 Plannen van 25 regio's, 2 landelijke organisaties, 1 centrale beheerder.
7 Van deze regio ontbraken 2 monodisciplinaire plannen.

IT-systemen, maatregelen, controle);
- maatregelen per verantwoordelijkheidsgebied (locaties, randapparatuur, programmatuur, gegevens, radiobediensystemen, personen, organisatie, gelieerden);
- beheerparagraaf in beveiligingsplan (verwijzing naar afzonderlijke beheerdocumenten);
- calamiteitenparagraaf in beveiligingsplan (verwijzing naar een calamiteitenplan).

ACTUALITEIT (VASTSTELLING, FREQUENTIE BIJSTELLING, DATERING)

Bij ongeveer de helft van de beveiligingsplannen ontbreken handtekeningen van het verantwoordelijke management. De meeste regio's hebben hun beveiligingsplannen tot op heden éénmaal aangeboden aan de centrale beheerder. Eén van de voorwaarden voor het in bedrijfstellen van C2000 voor een regio of landelijke organisatie was het hebben van een beveiligingsplan. De meeste plannen dateren van 2004, enkele van 2003 en enkele van 2005. Eén beveiligingsplan dateert van december 2007 en is geactualiseerd vanwege de ingebruikname van een nieuwe meldkamer.

Het onderdeel actualiteit is getoetst op de onderdelen vaststelling, frequentie bijstelling en datering. Hieruit kwam het volgende beeld naar voren:

Onvoldoende	Beperkt voldoende	Voldoende
11	14	2

AFBAKENING IN VERANTWOORDELIJKHEIDSGEBIEDEN (LEIDINGGEVENDE, FUNCTIES, RELATIE IT-SYSTEMEN, MAATREGELEN, CONTROLE)

Bij de afbakening in verantwoordelijkheidsgebieden gaat het vooral om opzet van organisatorische en fysieke maatregelen en minder om technische maatregelen. In de beveiligingsplannen is aan het begrip verantwoordelijkheidsgebied op verschillende manieren invulling gegeven.
In de loop van 2004 heeft BZK een 'template Beveiligingsplan C2000' aan de regio's verstrekt in de vorm van een handreiking. Het merendeel van de beveiligingsplannen bevat de in deze handreiking beschreven indeling in vier verantwoordelijkheidsgebieden (de fysieke omgeving van de C2000-apparatuur, de randapparatuur, de koppelingen tussen het C2000-deel en de overige meldkamerfuncties, de meldkamer in zijn geheel (bij een calamiteit)). Enkele regio's hanteren een eigen indeling en sommige regio's gaan niet in op de verantwoordelijkheidsgebieden.
De functie van informatie-beveiligingsfunctionaris staat in een aantal beveiligingsplannen benoemd, waardoor voor deze regio's/organisaties deze functie in opzet aanwezig is.

Het onderdeel afbakening in verantwoordelijkheidsgebieden is getoetst op de onderdelen leidinggevende, functies, relatie IT-systemen, maatregelen en controle. Hieruit kwam het volgende beeld naar voren:

Onvoldoende	Beperkt voldoende	Voldoende
0	11	16

MAATREGELEN PER VERANTWOORDELIJKHEIDSGEBIED

Ter voorbereiding op het bij gebruikersorganisaties in bedrijf stellen van de technische C2000-infrastructuur heeft de Projectdirectie C2000 destijds generieke Afhankelijkheids- & Kwetsbaarheidanalyses (A&K analyses) uitgevoerd. Niet alle beveiligingsplannen bevatten een beschrijving van de voorgenomen maatregelen op tactisch en operationeel niveau in het kader van C2000. Van één regio is bekend (via een eerder uitgevoerde pilot) dat deze maatregelen in een onderliggend plan van aanpak staan beschreven. De Projectdirectie C2000 heeft in 2003 bij de vijfentwintig regio's en twee landelijke organisaties een quick scan naar de status van de beveiliging van C2000 op maatregelniveau uitgevoerd en in afzonderlijke rapporten vastgelegd. Hierbij is gerapporteerd in termen van gereed, niet van toepassing en voorzien (= nog niet geïmplementeerd). Bij deze quick scan lag de nadruk op de fysieke beveiliging van de meldkamer en minder op overige generieke beheersmaatregelen, waaronder logische toegangsbeveiliging, wijzigingsbeheer en testen. Randapparatuur en beheer- en continuïteitsaspecten kwamen daarbij eveneens beperkt aan bod.

Het onderdeel maatregelen per verantwoordelijkheidsgebied is getoetst op vastlegging. Hieruit kwam het volgende beeld naar voren:

Onvoldoende	Beperkt voldoende	Voldoende
5	22	0

BEHEERPARAGRAAF IN BEVEILIGINGSPLAN

In meer dan de helft van de beveiligingsplannen is geen verwijzing naar een beheerdocument opgenomen. In die gevallen waarin sprake is van een verwijzing naar een beheerdocument gaat het in de meeste gevallen om nog op te stellen documenten.

Het onderdeel beheerparagraaf is getoetst op aanwezigheid en bestaan van onderliggende beheerdocumenten. Hieruit kwam het volgende beeld naar voren:

Onvoldoende	Beperkt voldoende	Voldoende
16	10	1

CALAMITEITENPARAGRAAF IN BEVEILIGINGSPLAN

In meer dan de helft van de beveiligingsplannen is geen verwijzing naar een calamiteitenplan opgenomen. In die gevallen waarin sprake is van een verwijzing naar een calamiteitenplan gaat het in de meeste gevallen om nog op te stellen documenten.

Het onderdeel calamiteitenparagraaf is getoetst op aanwezigheid en bestaan van onderliggende calamiteitenplannen. Hieruit kwam het volgende beeld naar voren:

Onvoldoende	Beperkt voldoende	Voldoende
14	12	1

2.3. BEVEILIGINGSPLAN CENTRALE BEHEERDER

De centrale beheerder vtsPN/UMS draagt een specifieke verantwoordelijkheid, namelijk het uitvoeren van tactisch en operationeel beheer van de C2000 infrastructuur. Het Beveiligingsbeleid gaat beperkt in op de eisen die aan de centrale beheerder worden gesteld. Er bestaat geen vastgesteld format voor beveiligingsplannen van de centrale beheerder en de wijze van aansluiting tussen het (actuele) beveiligingsplan van de centrale beheerder en de beveiligingsplannen van de regio's.
Ten aanzien van de vijf aspecten beperkt de Inspectie zich tot opmerkingen op hoofdlijnen.

ACTUALITEIT

De centrale beheerder heeft haar beveiligingsplan in 2007 geactualiseerd en voorgelegd aan de uitvoerend strategisch beheerder DGV/DS/IB van BZK. Het vorige beveiligingsplan van de centrale beheerder dateert uit 2003. De Inspectie heeft tijdens de onderzoeksperiode geen definitieve versie ontvangen.

AFBAKENING IN VERANTWOORDELIJKHEIDSGEBIEDEN

Het beveiligingsplan gaat nader in op de afbakening in verantwoordelijkheidsgebieden. De indeling in verantwoordelijkheidsgebieden is bij de centrale beheerder gericht op de technische infrastructuur en verschilt in karakter van de bij de aangewezen gebruikers aangetroffen indelingen. Ten aanzien van de verantwoordelijkheid van de 'beveiligingsfunctionaris DMD'[8] bestaat onduidelijkheid tussen de strategisch beheerder (BZK) en de centrale beheerder (DMD) over de invulling van deze rol na de overgang van DMD naar vtsPN.

MAATREGELEN PER VERANTWOORDELIJKHEIDSGEBIED

In het beveiligingsplan is een statusoverzicht opgenomen van de eerder vastgestelde te implementeren beveiligingsmaatregelen. In dit plan wordt verwezen naar afzonderlijke A&K analyses. Deze analyses dateren uit 2005 en eerder. Uit het beveiligingsplan is niet af te leiden aan wie de destijds door de Projectdirectie uitgevoerde generieke A&K analyses zijn overgedragen. De Inspectie heeft de A&K analyses niet nader onderzocht. Het beveiligingsplan bevat tevens een terugblik op 2005/2006 en activiteiten en projecten voor 2007. Het betreft hier zowel reguliere als projectmatige werkzaamheden en enkele punten van aandacht.

BEHEERPARAGRAAF IN BEVEILIGINGS(BEHEER)PLAN

In het landelijke Beveiligingsbeleid staat beschreven dat de centrale beheerder werkt volgens de algemeen geaccepteerde IT-beheer standaard ITIL. Deze afkorting staat voor IT Infrastructure Library. Het is een raamwerk dat is gebaseerd op best practices en dat is bedoeld voor het inrichten en optimaliseren van IT-beheer. In het beveiligingsplan ontbreekt een beheerparagraaf die verwijst naar de inrichting en werkwijzen van centraal beheer, inclusief positionering ten opzichte van (decentraal) lokaal beheer.

8 Lees voor DMD: vtsPN/UMS.

CALAMITEITENPARAGRAAF IN BEVEILIGINGSPLAN

In afzonderlijke documenten zijn calamiteitenplannen geformuleerd voor de diverse onderdelen van het C2000 systeem waar de centrale beheerder verantwoordelijk voor is. Deze plannen zijn in beheer bij de informatie-beveiligingsfunctionaris van de centrale beheerder. Daarnaast is bij de centrale beheerder onder andere documentatie aangetroffen betreffende een waarneming van een in 2007 gehouden uitwijkoefening.

ALGEMEEN BEELD

Op basis van de hierboven genoemde bevindingen komt het algemene beeld naar voren dat het beveiligingsplan van de centrale beheerder vtsPN/UMS in beperkte mate voldoet. Mede gelet op de gewijzigde situatie, waarin de oorspronkelijke centrale beheerder Directie Mobiele Diensten (DMD) als onderdeel van de Projectdirectie C2000 van BZK is opgegaan in de afdeling UMS van de vtsPN, ligt hier een aandachtspunt bij de eerstvolgende bijstelling van het landelijke Beveiligingsbeleid.

2.4. STATUSRAPPORTAGES BEVEILIGING C2000 GEBRUIKERSORGANISATIES

Bij de centrale beheerder vtsPN/UMS zijn geen statusrapportages beveiliging van gebruikersorganisaties aangetroffen. Vanaf het moment van inbedrijfstelling van C2000 dienen gebruikersorganisaties deze rapportages jaarlijks op te stellen en aan te bieden aan de centrale beheerder vtsPN/UMS. Wel heeft de Inspectie bij de centrale beheerder documentatie aangetroffen over een in 2003 uitgevoerde landelijke quick scan informatiebeveiliging. Deze destijds door de Projectdirectie C2000 van BZK uitgevoerde scan had mede tot doel zicht te krijgen op de status van beveiliging C2000 bij de vijfentwintig regio's en bij de twee landelijke organisaties, alvorens over te gaan tot inbedrijfstelling. Daarnaast dienden de uitkomsten van deze scan als hulpmiddel voor de regio bij het opstellen van een (definitief) beveiligingsplan. Een aantal regio's heeft de resultaten van de scan op maatregelniveau in haar beveiligingsplan opgenomen en de status van de maatregelen tijdens het bijstellen van haar beveiligingsplan bijgewerkt. Omdat de Inspectie geen statusrapportages beveiliging heeft aangetroffen, heeft de Inspectie de aspecten:

- actualiteit (vaststelling, frequentie, datering);
- stand van zaken, controle bevindingen, aangeboden aan de DMD[9];
- afhandeling statusrapportages beveiliging centrale beheerder,

niet kunnen beoordelen.

Om toch een beeld te kunnen schetsen over de mate waarin de verschillende gebruikersorganisaties zelf inzicht hebben in de geïmplementeerde maatregelen en de nog te implementeren maatregelen, heeft de Inspectie een korte inventarisatie uitgevoerd naar de aanwezigheid van interne C2000-statusrapportages beveiliging. Een enkele regio

9 Lees voor DMD: vtsPN/UMS.

geeft aan jaarlijks een interne (monodisciplinaire) statusrapportage op te stellen. De overige regio's geven een ontkennend antwoord. In ruim een kwart van de gevallen bleek de regionale contactpersoon een monodisciplinair antwoord te geven (meestal voor de discipline politie), omdat hij of zij geen multidisciplinaire uitspraken kon doen.

2.5. INCIDENTENRAPPORTAGES C2000 GEBRUIKERSORGANISATIES

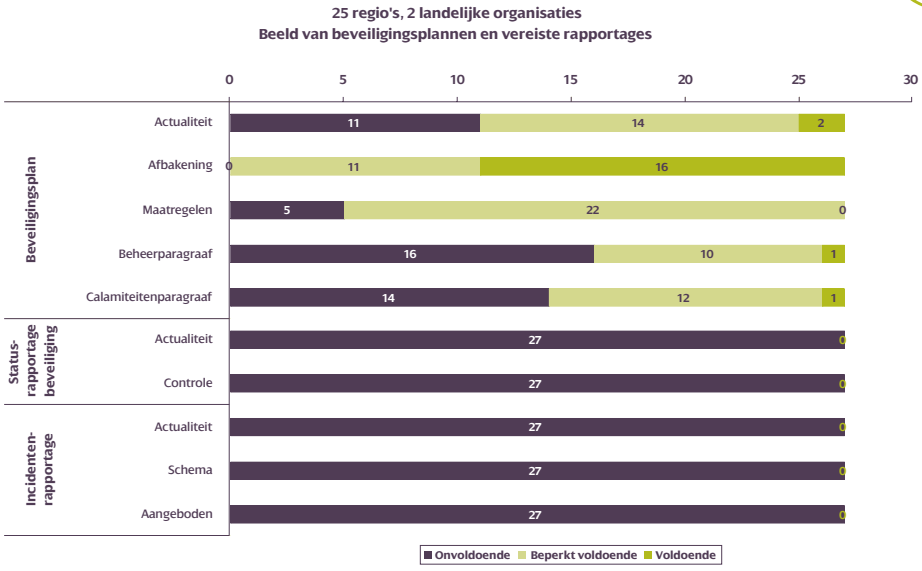
Omdat de Inspectie geen incidentenrapportages heeft aangetroffen, heeft de Inspectie de aspecten:

- incidentenrapportages beveiliging gebruikersorganisaties;
- actualiteit (vaststelling, frequentie, datering);
- conform incidenten-rapportageschema;
- aangeboden aan de DMD[10];
- afhandeling incidentenrapportages beveiliging centrale beheerder,

niet kunnen beoordelen.

De Inspectie heeft eveneens een korte inventarisatie uitgevoerd naar mogelijke interne incidentenrapportages, waarmee gebruikersorganisaties zelf inzicht hebben en houden in opgetreden incidenten. Ongeveer driekwart van de regio's hebben ontkennend geantwoord. Vier regio's geven daarbij aan dat vanwege het gering aantal incidenten men volstaat met het apart melden van incidenten bij vtsPN/UMS. In twee gevallen werd aangegeven dat incidenten in een eigen database worden opgeslagen, waarbij via een rapportgenerator overzichten kunnen worden geproduceerd. Zes regio's geven aan dat er interne incidentenrapportages worden opgesteld.
Er geldt dat in ruim een kwart van de gevallen het antwoord alleen betrekking heeft op een monodiscipline (meestal de discipline politie).
Vanwege de aard van de inventarisatie heeft de Inspectie niet nader onderzocht of de incidentenrapportages alleen betrekking hadden op randapparatuur, of dat ook meldkamer gerelateerde incidenten hierin zijn meegenomen.

10 Lees voor DMD: vtsPN/UMS.



TOELICHTING BIJ GRAFIEK

In bijgevoegde grafiek staan voor de vijfentwintig regio's en twee landelijke gebruikersorganisaties de uitkomsten van de drie hoofdvragen over beveiligingsplan, statusrapportage beveiliging en incidentenrapportage in staafdiagrammen weergegeven. Daarbij zijn de hoofdvragen uitgesplitst naar de eerder benoemde deelaspecten. De getallen in de balken hebben betrekking op aantallen regio's/organisaties verdeeld over de scores voldoende, beperkt voldoende, onvoldoende.

In één opslag valt op dat de score ten aanzien van de vereiste status-rapportages en incidentenrapportages voor alle regio's en voor beide landelijke organisaties onvoldoende is. Deze score heeft te maken met het feit dat de Inspectie deze rapportages niet heeft aangetroffen, terwijl ze wel degelijk vereist zijn.
Ten aanzien van de beveiligingsplannen valt op dat vooral actualiteit, de beheerparagraaf en de calamiteitenparagraaf aandacht vereisen.

Conclusies en aanbevelingen

3

3.1. BEVEILIGINGSPLANNEN GEBRUIKERSORGANISATIES EN CENTRALE BEHEERDER

Voldoen de beveiligingsplannen aan de in het Beveiligingsbeleid C2000 gestelde eisen?

CONTEXT BEVEILIGINGSPLANNEN

Het Beveiligingsbeleid C2000 richt de focus op gebruikersorganisaties bij het beschrijven van de gestelde eisen aan beveiliginsplannen. Voor de eisen waaraan het beveiligingsplan van de centrale beheerder van de C2000 infrastructuur moet voldoen staat de volgende verwijzing in het Beveiligingsbeleid opgenomen '... de directeur van de DMD[11] stelt het afgeleide Beveiligingsbeleid C2000 vast en draagt het (afgeleide) Beveiligingsbeleid C2000 voor de DMD uit.'

De onderzochte beveiligingsplannen zijn met wisselende diepgang opgesteld. Een gedeeltelijke verklaring hiervoor ligt in het ontbreken van een dwingend voorgeschreven richtlijn voor het opstellen van een beveiligingsplan. Daarbij zij tevens opgemerkt dat de in het Beveiligingsbeleid C2000 genoemde eisen aan een beveiligingsplan globaal van aard zijn, waardoor deze eisen zonder aanvullende afspraken voor meer uitleg vatbaar zijn. In de loop van 2004 heeft de Projectdirectie C2000 aan de gebruikersorganisatie een handreiking Beveiligingsplan C2000 verstrekt. Deze handreiking heeft geen verplichtend karakter.
De Inspectie heeft beperkt zicht op het bestaan van beveiligingsfunctionarissen, zowel binnen de meldkamers als binnen de disciplines. Uit het inspectierapport 'Samen werken, samen beveiligen' uit 2006 kwam onder andere het volgende naar voren. 'De politiekorpsen moeten voldoende personeel vrij maken dat zich met informatiebeveiliging bezighoudt'. Bij brandweer en ambulance zijn geen onderzoeksgegevens bekend. Deze beveiligingsfunctionarissen zijn van belang, omdat zij een rol hebben bij het uitvoeren van controles en het opstellen van rapportages.

Aanbevelingen voor de strategisch beheerder DGV/DS/IB

- Actualiseer het Beveiligingsbeleid naar de gewijzigde situatie waarin tactisch en operationeel beheer van de C2000 infrastructuur is uitbesteed (centrale beheerder).
- Formuleer in overleg met de betrokken partijen een richtlijn voor het opstellen van (op elkaar aansluitende) beveiligingsplannen.
- Maak, via de beheerovereenkomst, met de centrale beheerder aanvullende afspraken over de verwerking van en het rapporteren over de centraal aangeboden beveiligingsplannen en rapportages.
- Bouw tevens een toets op naleving in.

11 Lees voor DMD: vtsPN/UMS.

Actualiteit

De beveiligingsplannen zijn op een na niet actueel en in de meeste gevallen slechts eenmaal aangeboden aan de centrale beheerder. Enkele regio's hebben meerdere malen een bijgesteld beveiligingsplan aangeboden. Het meest actuele beveiligingsplan dateert van eind 2007. In de helft van de gevallen is het onduidelijk of het beveiligingsplan op bestuurlijk niveau door de regio is vastgesteld, waardoor het onduidelijk is of de in het beveiligingsplan benoemde maatregelen daadwerkelijk getroffen zijn, dan wel getroffen zullen worden.

Verantwoordelijkheidsgebieden

Het merendeel van de beveiligingsplannen is multidisciplinair van aard.
In de loop van 2004 heeft BZK in de vorm van een handreiking een indeling in vier verantwoordelijkheidsgebieden aangegeven, waarbij het zwaartepunt bij de meldkamer lag. Deze handreiking heeft geen verplichtend karakter. In het Beveiligingsbeleid wordt bij het benoemen van maatregelen gesproken over acht verantwoordelijkheidsgebieden (zie bijlage IV). Deze twee invalshoeken dragen bij aan omvang van de interpretatiebandbreedte.
Aan het begrip verantwoordelijkheidsgebied is door de gebruikersorganisaties op verschillende manieren invulling gegeven. Hierdoor is het op transparante wijze onderling vergelijken van de beveiligingsplannen niet mogelijk, waardoor de Inspectie beperkt zicht heeft op het op elkaar aansluiten van de verschillende beveiligingsplannen.
Enkele beveiligingsplannen gaan in op monodisciplinair te treffen maatregelen. Dit geldt vooral voor het verantwoordelijkheidsgebied randapparatuur.
In een aantal regio's/organisaties is de functie informatie-beveiligingsfunctionaris in opzet aanwezig. Deze functionaris speelt een belangrijke rol binnen de beveiligingsbeheersorganisatie. Uit het Inspectie onderzoek 'Samen werken, samen beveiligen' blijkt dat de politiekorpsen deze functie beperkt hebben ingevuld.

Maatregelen

Bij beveiligingsplannen gaat het om het benoemen van te treffen maatregelen op tactisch en operationeel niveau om een van tevoren bepaald beveiligingsniveau te waarborgen. In de aangetroffen beveiligingsplannen zijn niet altijd maatregelen (op operationeel niveau) opgenomen. Uit een eerder pilot onderzoek bleek dat een regio een beveiligingsplan had opgesteld dat meer als (strategisch) regionaal beleid opgevat moet worden en waarin dus geen operationele maatregelen waren opgenomen. Er bleek een onderliggend document aanwezig te zijn dat wel een stelsel van beveiligingsmaatregelen bevatte. Hieruit concludeert de Inspectie dat de definitie van beveiligingsplan voor meer uitleg vatbaar is.
Daar waar maatregelen waren opgenomen, bleken deze in de meeste gevallen te zijn gebaseerd op de eerder door de Projectdirectie C2000 uitgevoerde generieke A&K analyses. Deze analyses zijn destijds opgesteld om te komen tot een basisbeveiligingsniveau. Veel beveiligingsplannen verwijzen onder het kopje risicoanalyse naar de generieke A&K analyses, zonder daarbij verder in te gaan op mogelijke specifieke omstandigheden. Hieruit concludeert de Inspectie dat gebruikersorganisaties in beperkte mate A&K analyses hebben uitgevoerd voor het definiëren van aanvullende maatregelen. Gegeven de datering van de beveiligingsplannen heeft de Inspectie geen zicht op het bijstellingsproces van deze generieke A&K analyses.

Beheerdocumenten

In de beveiligingsplannen is beperkt aandacht voor lokaal beheer. Hierdoor heeft de Inspectie geen duidelijk zicht op de wijze waarop de regio's invulling hebben gegeven aan lokaal beheer. De scheiding tussen lokaal en centraal beheer (vtsPN/UMS) is niet scherp afgebakend, waardoor zaken tussen wal en schip kunnen vallen.

Calamiteitenplan

In de beveiligingsplannen is beperkt aandacht voor een calamiteitenplan dat voorziet in procedures en maatregelen op het gebied van backup & recovery dan wel uitwijkvoorzieningen, inclusief het aansluiten op het calamiteitenplan van de centrale beheerder. Gegeven de actualiteit van de aangetroffen beveiligingsplannen geven deze plannen beperkt uitsluitsel over de feitelijke status hieromtrent. De Inspectie heeft de indruk dat sinds 2004 en 2005, mede op basis van bevindingen tijdens twee eerder uitgevoerde pilots, in breder verband veel aandacht is uitgegaan naar uitwijk van de meldkamer[12] en buddy meldkamers.

Aanbeveling voor gebruikersorganisaties

Maak met de strategisch beheerder afspraken over het binnen redelijke termijn actualiseren, het op bestuurlijk niveau vaststellen en het aanbieden (aan de centrale beheerder) van de beveiligingsplannen.

BEELD BIJ DE CENTRALE BEHEERDER

Het Beveiligingsbeleid richt de focus op gebruikersorganisaties. Hierdoor komen de eisen die aan de centrale beheerder worden gesteld beperkt aan bod en heeft de centrale beheerder een zekere mate van vrijheid om zelf invulling te geven aan (afgeleid) Beveiligingsbeleid C2000 en onderliggende beveiligingsplannen.
Bij het overgaan van de centrale beheerder naar een organisatie buiten het ministerie van BZK is onduidelijkheid ontstaan over de rol en verantwoordelijkheid van de in het Beveiligingsbeleid genoemde ‘informatie-beveiligingsfunctionaris DMD’, waardoor het uitvoeren van controles als onderdeel van het beleidsevaluatieproces onder druk komen te staan.

12 MUST project van de vtsPN: Meldkamer Uitwijk Service voor regionale Taakondersteuning.

Aanbevelingen voor de centrale beheerder

- Zorg in samenspraak met de strategisch beheerder DGV/DS/IB voor meer transparantie over de rol van de informatie-beveiligingsfunctionaris van de centrale beheerder via de beheerovereenkomst.
  - Betrek hierbij tevens het actualiseren van uitgevoerde (deel)risicoanalyses (A&K analyses).

3.2. STATUSRAPPORTAGES GEBRUIKERSORGANISATIES

Voldoen de statusrapportages beveiliging C2000 aan de in het Beveiligingsbeleid C2000 gestelde eisen?

VOORAF

De verwerking van de statusrapportages door de centrale beheerder heeft niet kunnen plaatsvinden, omdat de centrale beheerder geen rapportages heeft binnengekregen van de gebruikersorganisaties. Het Beveiligingsbeleid gaat niet in op de wijze waarop de centrale beheerder over de statusrapportages beveiliging richting strategisch beheerder moet communiceren.

Aanbevelingen algemeen voor de strategisch beheerder DGV/DS/IB:

- Stel in overleg met betrokken partijen een verantwoordingsrichtlijn op ten behoeve van de vereiste statusrapportages beveiliging.
  - Ga daarbij tevens in op de inrichting van een beveiligingsbeheersorganisatie.

Conclusie

De Inspectie heeft geen statusrapportages beveiliging C2000 bij de centrale beheerder vtsPN/UMS aangetroffen. Daarmee hebben de regio's niet voldaan aan de gestelde eisen in het Beveiligingsbeleid. De centrale beheerder heeft hierdoor geen statusrapportages beveiliging richting strategisch beheerder kunnen communiceren.

Het Beveiligingsbeleid is nog niet aangepast op de nieuwe situatie waarin de centrale beheerder is opgegaan in de vtsPN. In deze nieuwe situatie is sprake van uitbesteding van tactisch en operationeel beheer van de C2000 infrastructuur aan de vtsPN. Dit heeft gevolgen voor het hoofdstuk rapportage uit het Beveiligingsbeleid, waarin de verantwoordingsstructuur beschreven staat.

De Inspectie heeft beperkt zicht op het bestaan van beveiligingsfunctionarissen, zowel binnen de meldkamers als binnen de kolommen. Deze functionarissen hebben een rol bij het uitvoeren van controles en het opstellen van rapportages.

Aanbevelingen voor gebruikersorganisaties:
Draag zorg voor het periodiek opstellen van statusrapportages beveiliging en draag tevens zorg voor het aanbieden van deze rapportages aan de centrale beheerder (vtsPN).

3.3 INCIDENTENRAPPORTAGES GEBRUIKERSORGANISATIES

Voldoen de incidentenrapportages C2000 aan de in het Beveiligingsbeleid C2000 gestelde eisen?

VOORAF

De verwerking van de incidentenrapportages door de centrale beheerder heeft niet kunnen plaatsvinden, omdat de centrale beheerder geen incidentenrapportages heeft binnengekregen van de gebruikersorganisaties.

Aanbevelingen algemeen voor de strategisch beheerder DGV/DS/IB
- Stel in overleg met betrokken partijen een verantwoordingsrichtlijn op ten behoeve van de vereiste incidentenrapportages.
- Ga daarbij tevens in op de inrichting van een beveiligingsbeheersorganisatie.

Conclusie
De Inspectie heeft bij de centrale beheerder geen incidentenrapportages C2000 afkomstig van gebruikersorganisaties aangetroffen. Daarmee hebben de regio's niet voldaan aan de gestelde eisen in het Beveiligingsbeleid. Incidenten worden vanuit de regio gemeld bij de helpdesk van de centrale beheerder. In hoeverre binnen gebruikersorganisaties een proces incidenten is ingericht heeft de Inspectie niet onderzocht. Vanwege het ontbreken van incidentenrapportages bij de gebruikersorganisaties is achteraf de volledigheid van meldingen bij de centrale beheerder niet vast te stellen.

Aanbevelingen voor gebruikersorganisaties
Draag zorg voor het periodiek opstellen van incident statusrapportages en draag tevens zorg voor het aanbieden van deze rapportages aan de centrale beheerder (vtsPN).

Bijlage: Afkortingen

Afkorting	*Betekenis*
A&K analyses	Afhankelijkheids- en Kwetsbaarheidsanalyses
BZK	Binnenlandse Zaken en Koninkrijksrelaties
C2000	Communicatiesysteem 2000
DGV	Directoraat Generaal Veiligheid
DMD	Directie Mobiele Diensten
DS	directie Strategie
IB	afdeling Informatiebeleid
ITIL	Information Technology Infrastructure Library
KLPD	Korps landelijke politiediensten
KMar	Koninklijke Marechaussee
MUST	Meldkamer Uitwijk Service voor regionale Taakondersteuning (project van de vtsPN)
vtsPN/UMS	voorziening tot samenwerking Politie Nederland/Unit Meldkamer Systemen

Bijlage: Begrippenlijst

II

C2000 infrastructuur

Het samenwerkend geheel van infrastructurele voorzieningen dat het transport van spraak, data en alarmering verzorgt.
De C2000 Infrastructuur is opgebouwd uit basisstations, schakelnodes een Netwerk Management Systeem, radio- en alarmeringsbediensystemen, de centrale paging installatie en Special Coverage Locations.

C2000 systeem

Het samenwerkend geheel van C2000 infrastructuur, netwerkdiensten, randapparatuur, radio- en alarmeringsbediensystemen en Special Coverage Locations.

Centraal beheer

Het centraal beheer betreft met name het technisch beheer van de zogenaamde 'vitale C2000 infrastructuur'. Hieronder wordt verstaan het samenstel van vitale onderdelen van de C2000 infrastructuur bestaande uit schakelnodes, C2000 basisstations, vaste verbindingen (waaronder NAFIN), radiobediensystemen, alarmeringsbediensystemen, radiofrequenties en de zogenaamde 'vitale' Special Coverage Locations.

Directie Mobiele Diensten

Vroeger onderdeel van de Projectdirectie C2000 van het ministerie van BZK.
Per 01-08-2006 is de Directie Mobiele Diensten opgegaan in de voorziening tot samenwerking Politie Nederland/Unit Meldkamer Systemen.

Informatiebeveiliging

Informatiebeveiliging is het inrichten en onderhouden van een stelsel van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en informatiesystemen te waarborgen (ISO, 2005).

Lokaal beheer

Lokaal beheer betreft voornamelijk functioneel beheer (subscribermanagement) van een deel van het C2000 Systeem. Dit is een verantwoordelijkheid van de gebruikersorganisatie die het functionele beheer uitvoert.
Het beheer van de randapparatuur wordt uitgevoerd door de Aangewezen Gebruikersorganisaties, die deze apparatuur aangeschaft hebben, en in gebruik zijn bij hun organisatie of bij de aan hen gelieerde organisaties.

Projectdirectie C2000

De Projectdirectie C2000, tot in 2006 onderdeel van het ministerie van BZK, heeft uitvoering gegeven aan:

- de uitrol van de landelijke infrastructuur;
- ondersteuning van gebruikers bij de regionale implementatie;
- het vormgeven van beheer- en onderhoudsfase;
- verzorging van de informatievoorziening aan de Tweede Kamer.

vtsPN/UMS

Het tactisch en operationeel beheer van C2000 wordt uitgevoerd door de afdeling Unit Meldkamer Systemen (UMS) van de voorziening tot samenwerking Politie Nederland (vtsPN), kortweg: de centrale beheerder.

Bijlage: Context Beveiligingsbeleid C2000, versie december 2004[13]

III

VERANTWOORDELIJKHEDEN EN UITVOERING

DMD[14]

De directeur van de Directie Mobiele Diensten is verantwoordelijk voor de beveiliging van zijn organisatie en het beheer van de vitale onderdelen van de C2000 Infrastructuur.
Hij stelt het afgeleide Beveiligingsbeleid C2000 vast en draagt het (afgeleide) Beveiligingsbeleid C2000 voor de Directie Mobiele Diensten uit.
De Directie Mobiele Diensten draagt het Beveiligingsbeleid C2000 uit, specifiek daar waar het gaat om beheertaken op het gebied van beveiliging van de C2000 Infrastructuur en stelt een beveiligingsplan C2000 op.
In dit kader levert de Directie Mobiele Diensten tevens een bijdrage aan de bewustwording van de beveiliging en de te nemen beveiligingsmaatregelen met betrekking tot het gebruik van de C2000 Infrastructuur.
Daarnaast draagt de Directie Mobiele Diensten zorg voor een calamiteitenplan, ten behoeve van een adequate aanpak van eventuele calamiteiten in de C2000 infrastructuur.

Regionale politiekorpsen

De korpsbeheerder is belast met het beheer over zijn regio en verantwoordelijk voor de beveiliging van zijn regio.
De korpsbeheerder is verantwoordelijk voor de uitvoering van het Beveiligingsbeleid C2000, stelt een beveiligingsplan op en draagt het Beveiligingsbeleid C2000 uit.

Brandweer Regio's

De voorzitter van het bestuur van de regionale brandweer is belast met de leiding over zijn regio en verantwoordelijk voor de beveiliging van zijn regio.
De voorzitter is verantwoordelijk voor de uitvoering van het Beveiligingsbeleid C2000, stelt beveiligingsplannen op en draagt het Beveiligingsbeleid C2000 uit.

Ambulancediensten

De voorzitter van het bestuur van de Regionale Ambulance Voorziening (RAV), bestaande uit de meldkamer ambulancezorg en de aangesloten directies van de aangesloten regionale ambulancediensten, is belast met de leiding over zijn regio en verantwoordelijk voor de beveiliging van zijn regio.
De voorzitter van het bestuur van de meldkamer ambulancezorg en de directies van de aangesloten regionale ambulancediensten zijn verantwoordelijk voor het opstellen van beveiligingsplannen en het uitdragen van het Beveiligingsbeleid C2000.

13 DGV/DS/IB is gestart met het bijstellen van het Beveiligingsbeleid en verwacht deze bijstelling medio 2008 te kunnen afronden.
14 Lees voor DMD: vtspn/UMS.

Korps landelijke politiediensten (KLPD)

De korpsbeheerder van het KLPD is belast met het beheer over het KLPD en verantwoordelijk voor de beveiliging van het KLPD.
De korpsbeheerder is verantwoordelijk voor de uitvoering van het Beveiligingsbeleid C2000, stelt beveiligingsplannen op en draagt het Beveiligingsbeleid C2000 uit.

Koninklijke Marechaussee (KMar)

De bevelhebber der Koninklijke Marechaussee is belast met de ambtelijke leiding over de KMar en verantwoordelijk voor de beveiliging van de KMar.
De bevelhebber der KMar is verantwoordelijk voor de uitvoering van het Beveiligingsbeleid C2000 binnen de KMar, stelt een beveiligingsplan op en draagt het Beveiligingsbeleid C2000 voor de KMar uit.

Gelieerden

Er worden twee categorieën gelieerden onderscheiden, namelijk landelijk gelieerden en regionaal gelieerden.
Voor beide categorieën geldt dat de leidinggevende van de gelieerde verantwoordelijk is richting de desbetreffende Aangewezen Gebruiker voor de beveiliging van zijn dienst dan wel verantwoordelijkheidsgebied.

UITVOERING OPERATIONEEL NIVEAU

Op operationeel niveau wordt uitvoering gegeven aan de vanuit het Beveiligingsbeleid C2000 vastgestelde beveiligingseisen en de hieruit voortvloeiende beveiligingsmaatregelen.
Dit brengt met zich mee dat de bij het C2000 Systeem betrokken organisaties ingericht dienen te zijn om uitvoering te kunnen geven aan de in dit document (Beveiligingsbeleid) gestelde beveiligingseisen.

CONTROLE

Binnen DMD[15] door:

- De informatie-beveiligingsfunctionaris, namens de leidinggevende, voor controle op de implementatie van beveiligingsmaatregelen.
- ... en de informatie-beveiligingsbeheerder(s) van de Directie Mobiele Diensten, namens de directeur Directie Mobiele Diensten, voor controle op de implementatie van het Beveiligingsbeleid C2000.

15 Lees voor DMD: vtspn/UMS.

Binnen Regio/KLPD/KMar door:

- De informatie-beveiligingsfunctionaris, namens de leidinggevende, voor controle op de implementatie van beveiligingsmaatregelen.
- De beveiligingsfunctionaris van de gebruikersorganisatie namens de verantwoordelijke van de gebruikersorganisatie (*en de informatie-beveiligingsbeheerder(s) van de Directie Mobiele Diensten, namens de directeur Directie Mobiele Diensten*) voor controle op de implementatie van het Beveiligingsbeleid C2000.

Bijlage: Normenkader

IV

ONDERDEEL BEVEILIGINGSPLAN

ACTUALITEIT (VASTSTELLING, FREQUENTIE BIJSTELLING, DATERING)

Elk (geactualiseerd) beveiligingsplan dient na vaststelling door de verantwoordelijke leidinggevende ter registratie uiterlijk 2 maanden voor het (gepland) operationeel gaan te worden aangeboden aan de directeur van de Directie Mobiele Diensten[16]. Tevens dient elk beveiligingsplan jaarlijks te worden geëvalueerd en geactualiseerd.

AFBAKENING IN VERANTWOORDELIJKHEIDSGEBIEDEN (LEIDINGGEVENDE, FUNCTIES, RELATIE IT-SYSTEMEN, MAATREGELEN, CONTROLE)

Per verantwoordelijkheidsgebied dient daartoe door zorg van de betrokken beveiligingscoördinator minimaal te worden vastgelegd:

- De verantwoordelijke leidinggevende.
- Welke functies door dit verantwoordelijkheidsgebied worden uitgevoerd.
- De relatie met andere informatiesystemen en/of verantwoordelijkheidsgebieden (gemeenschappelijke IT-diensten).
- De wijze van beveiliging.
- De wijze en frequentie van controle op de beveiliging.

Toelichting. Het C2000 Systeem is een gemeenschappelijke infrastructuur die door verschillende organisaties wordt gebruikt. Daarom is een verdere afbakening in verantwoordelijkheidsgebieden noodzakelijk. Per verantwoordelijkheidsgebied dient eenduidig te zijn vastgelegd voor welk deel van het C2000 Systeem (infrastructuur, radiobediensysteem, randapparatuur enz.) de betreffende organisatie verantwoordelijk is. Dit geldt met name bij overlap van verantwoordelijkheidsgebieden, waarbij bijvoorbeeld de ene organisatie verantwoordelijk is voor de C2000 apparatuur en de andere organisatie voor de locatie waar deze apparatuur is geïnstalleerd.

MAATREGELEN

Per verantwoordelijkheidsgebied vast te leggen items:

Locaties

a. Een overzicht van de voor C2000 in gebruik zijnde locaties.
b. De C2000 apparatuur die op deze locaties is geïnstalleerd / in gebruik is.
   c De afhankelijkheid van de organisatie van deze apparatuur / locatie.
   d De kwetsbaarheid van de locaties.
   e De gevoeligheid van de informatie die op de betreffende locatie aanwezig is (gerubriceerd, gemerkt of anderszins gevoelig).
   (Dan wel een verwijzing naar de generieke A&K analyse indien geen aanvullende maatregelen noodzakelijk zijn.)
f. De wijze van beveiliging van de locatie.
g. De wijze en frequentie van controle op de beveiliging.

16 Lees voor Directie Mobiele Diensten (DMD): vtsPN/UMS.

Randapparatuur

a. Een overzicht van de in gebruik zijnde / beschikbare randapparatuur.
b. De afhankelijkheid van de organisatie van de randapparatuur.
c. De kwetsbaarheid van de randapparatuur.
d. De gevoeligheid van de randapparatuur en de informatie die in de randapparatuur aanwezig is (gerubriceerd, gemerkt of anderszins gevoelig).
(Dan wel een verwijzing naar de generieke A&K analyse indien geen aanvullende maatregelen noodzakelijk zijn.)
e. De wijze van beveiliging.
f. De wijze en frequentie van controle op de beveiliging.

Programmatuur

a. Een overzicht van de op de (rand)apparatuur geïnstalleerde programmatuur.
b. De afhankelijkheid van de organisatie van de programmatuur.
c. De kwetsbaarheid van de programmatuur.
d. De gevoeligheid van de programmatuur.
(Dan wel een verwijzing naar de generieke A&K analyse indien geen aanvullende maatregelen noodzakelijk zijn.)
e. De wijze van beveiliging;
f. De wijze en frequentie van controle op de beveiliging.

Gegevens

a. De gevoeligheid van de in het verantwoordelijkheidsgebied voorkomende gegevens (classificatie);
b. De afhankelijkheid van de organisatie van deze gegevens;
c. De kwetsbaarheid van de gegevens;
(dan wel een verwijzing naar de generieke A&K analyse indien geen aanvullende maatregelen noodzakelijk zijn;)
d. De wijze van beveiliging.
e. De wijze en frequentie van controle op de beveiliging.

Radiobediensysteem

a. Een overzicht van de in gebruik zijnde radiobediensystemen.
b. De afhankelijkheid van de organisatie van de radiobediensystemen.
c. De kwetsbaarheid van de radiobediensystemen.
d. De gevoeligheid van de radiobediensystemen en de informatie die in de radiobediensystemen aanwezig is (gerubriceerd, gemerkt of anderszins gevoelig).
(Dan wel een verwijzing naar de generieke A&K analyse indien geen aanvullende maatregelen noodzakelijk zijn.)
e. De wijze van beveiliging.
f. De wijze en frequentie van controle op de beveiliging.

Personen

Namen van personen die toegang (mogen) hebben tot C2000 apparatuur binnen het verantwoordelijkheidsgebied waarvoor het beveiligingsplan van toepassing is. Dit geldt minimaal voor gebruikers / bedienaars, beheerders en onderhoudspersoneel.

Organisatie

a. Een organogram van de organisatie.
b. Taken, verantwoordelijkheden en bevoegdheden van de verschillende functionarissen op het gebied van beveiliging.
c. Functies waarvoor een antecedentenonderzoek / veiligheidsonderzoek noodzakelijk is.

Gelieerden

Voor toegelaten gelieerden geldt bovendien dat de gelieerde een beveiligingsplan indient bij de Aangewezen Gebruiker of te integreren in het beveiligingsplan van de Aangewezen Gebruiker.

De Aangewezen Gebruiker beoordeelt of met dit beveiligingsplan afdoende invulling wordt gegeven aan het Beveiligingsbeleid C2000. De Aangewezen Gebruiker biedt dit dan vervolgens aan aan de directeur van de Directie Mobiele Diensten. Tevens houdt de Aangewezen Gebruiker toezicht op het naleven van de beveiligingsvoorschriften door de gelieerde.

BEHEER:

- DMD[17]: Het door de beherende organisatie (Directie Mobiele Diensten voor de vitale C2000 infrastructuur) vastleggen van:
  - **a** De netwerkconfiguratie (schakelnodes, basisstations en de onderlinge verbindingen) en de verbindingen met radiobediensystemen en externe koppelingen.
  - **b** De afhankelijkheid van (delen van) de configuratie.
  - **c** De kwetsbaarheid van de configuratie.
  - **d** De gevoeligheid van de door het netwerk te transporteren informatie.
  - **e** De wijze van beveiliging van de (radio- en lijn-)verbindingen.
  - **f** De wijze en frequentie van controle op de beveiliging.
- Regio/KLPD/KMar

  Het vastleggen van beheeraspecten dient in afzonderlijke beheerdocumenten te geschieden. Vanuit deze paragraaf dient te worden verwezen naar deze documenten.

CONTINUÏTEIT

Een calamiteitenparagraaf verwijst naar een calamiteitenplan.

ONDERDEEL STATUSRAPPORTAGE BEVEILIGING C2000

ACTUALITEIT (VASTSTELLING, FREQUENTIE BIJSTELLING, DATERING)

Periodiek (gegeven de relatie met jaarlijkse bijstelling beveiligingsplan minimaal eenmaal per jaar)

- Het rapport dient door de verantwoordelijke leidinggevende te worden vastgesteld en vervolgens te worden aangeboden aan de beveiligingsfunctionaris (informatie-beveiligingsbeheer) van de Directie Mobiele Diensten.

STAND VAN ZAKEN, CONTROLE BEVINDINGEN, AANGEBODEN AAN DE DMD

De beveiligingsfunctionaris van een verantwoordelijkheidsgebied stelt namens zijn

17 Lees voor DMD: vtsPN/UMS.

leidinggevende een rapport op waarin de toestand van de beveiliging wordt weergeven. Dit rapport dient minimaal te bevatten:

- De stand van zaken m.b.t. het opstellen c.q. reviseren van de beveiligingsplannen.
- De stand van zaken m.b.t. de implementatie van de beveiligingsmaatregelen.
- De gehouden controles op de implementatie van de beveiligingsmaatregelen alsmede de bevindingen van deze controles.
- Het rapport dient door de verantwoordelijke leidinggevende te worden vastgesteld en vervolgens te worden aangeboden aan de beveiligingsfunctionaris (informatie-beveiligingsbeheer) van de Directie Mobiele Diensten.

ONDERDEEL INCIDENTENRAPPORTAGE C2000

ACTUALITEIT (VASTSTELLING, FREQUENTIE BIJSTELLING, DATERING)

Frequentie: Jaarlijks.

De beveiligingsfunctionaris van de betreffende organisatie dient zorg te dragen voor het opstellen van jaarlijkse rapportages van de in zijn organisatie gemelde incidenten.

CONFORM INCIDENTEN-RAPPORTAGESCHEMA

De leidinggevende stelt voor zijn verantwoordelijkheidsgebied een incidenten-rapportageschema vast. Dit schema dient de vereiste items te bevatten.

Dit incidentenrapportage-schema dient aan te geven:

- Welke veiligheidsinbreuken als een incident worden aangemerkt.
- Welke incidenten met welke frequentie aan welke functionarissen worden gerapporteerd.
- Langs welke weg de incidenten die binnen het verantwoordelijkheidsgebied plaatsvinden moeten worden gemeld en verder worden gerapporteerd. Hierbij dient minimaal te worden ingeschakeld:
  - de verantwoordelijke leidinggevende;
  - de beveiligingsfunctionaris van de leidinggevende;
  - de beveiligingsfunctionaris van de Directie Mobiele Diensten;
  - in voorkomend geval (in geval van verdenking strafbaar feit c.q. laakbaar gedrag) de officier van justitie.
- Hoe en onder wiens verantwoordelijkheid de incidenten dienen te worden afgehandeld.
- Hoe en door wie een registratie van de incidenten wordt bijgehouden.

De beveiligingsfunctionaris van de betreffende organisatie dient zorg te dragen voor het opstellen van jaarlijkse rapportages van de in zijn organisatie gemelde incidenten volgens eerder genoemd rapportageschema (definitie incident, rapportage, wijze van afhandeling, registratie).

AANGEBODEN AAN DE DMD[18]

De jaarlijkse rapportages dienen te worden aangeboden aan de directeur van de Directie Mobiele Diensten. De Directie Mobiele Diensten geeft deze informatie door aan het Ministerie van BZK tezamen met aanvullende gegevens betreffende de C2000 infrastructuur.

18 Lees voor DMD: vtsPN/UMS.

Inspectie
OPENBARE ORDE
EN VEILIGHEID