Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1994–1995

24 175 Beheersing informatiebeveiliging

Nr. 1 **BRIEF VAN DE ALGEMENE REKENKAMER**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

's-Gravenhage, 23 mei 1995

Hierbij bieden wij u het op 10 mei 1995 door ons vastgestelde rapport «Beheersing informatiebeveiliging» aan.

Algemene Rekenkamer

H. E. Koning,
president

T. A. M. Witteveen,
secretaris

S–RW
S–CM

51U2515
ISSN 0921 - 7371
Sdu Uitgeverij Plantijnstraat
's-Gravenhage 1995

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1994–1995

24 175 Beheersing informatiebeveiliging

Nr. 2

51U2515
ISSN 0921 - 7371
Sdu Uitgeverij Plantijnstraat
's-Gravenhage 1995

SAMENVATTING

De Algemene Rekenkamer onderzocht in 1994 de beheersing van de informatiebeveiliging bij alle ministeries. Zij onderzocht of de secretarissen-generaal als ambtelijk eindverantwoordelijken adequate instrumenten voor deze beheersing hadden gecreëerd en of de coördinerende activiteiten van de minister van Binnenlandse Zaken op dit terrein toereikend waren.

Hoewel er sinds een vergelijkbaar onderzoek van de Rekenkamer in 1988 verbeteringen tot stand zijn gebracht, concludeert de Rekenkamer dat de beheersing van de informatiebeveiliging bij het Rijk toch nog tekortkomingen vertoont.

De Rekenkamer meent dat de ambtelijke top van de ministeries in het algemeen onvoldoende sturing geeft aan de informatiebeveiliging. Zo constateert zij dat de meeste ministeries nog steeds onvoldoende inzicht hebben in risico's en dat ongeveer de helft van de ministeries geen actueel beleid voor informatiebeveiliging heeft vastgesteld. Voor zover het beleid voor informatiebeveiliging al is uitgewerkt in beveiligings- en calamiteitenplannen vertoont deze uitwerking vrijwel altijd zodanige tekortkomingen dat de beveiligingsmaatregelen teveel op ad hoc basis worden genomen.

Het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen vertonen bij veel ministeries ook tekortkomingen op het gebied van systeemontwikkeling en -onderhoud, toegang tot en het gebruik van gegevens, personele maatregelen, privacyreglementen en de toetsbaarheid van de fysieke maatregelen.

Ook is bij een aantal ministeries het toezicht op de informatiebeveiliging ontoereikend. Dit uit zich vooral door onvoldoende zicht op de feitelijke beveiligingssituatie en onvoldoende verantwoording over de uitvoering van het beveiligingsbeleid en geen of een te beperkte onafhankelijke controle van de informatiebeveiliging.

De situatie bij de ministeries van Algemene Zaken, van Buitenlandse Zaken, van Defensie, van Landbouw, Natuurbeheer en Visserij en bij de Belastingdienst acht de Rekenkamer toereikend. Het slechtst scoort het Ministerie van Sociale Zaken en Werkgelegenheid, dat de informatiebeveiliging volstrekt onvoldoende beheerst.

Voor de centrale regelgeving voor de gehele rijksoverheid en voor de overige coördinatie door de minister van Binnenlandse Zaken komt de Rekenkamer tot de conclusie dat de minister in belangrijke mate invulling heeft gegeven aan zijn coördinerende rol op het gebied van de informatiebeveiliging bij het Rijk. Toch constateert de Rekenkamer nog tekortkomingen op dit terrein. Zo is de beheersing van de informatiebeveiliging bij zelfstandige bestuursorganen nog niet geregeld; bovendien heeft het voorschrift voor de informatiebeveiliging bij de rijksdienst te lang op zich laten wachten. Het belang van een duidelijke vastlegging van de verantwoordelijkheid voor het bovendepartementale toezicht op de informatiebeveiliging wordt bovendien nog niet onderkend. Ook heeft het ministerie nog geen invulling gegeven aan zijn taak op het gebied van de evaluatie van de beveiligingssituatie bij de ministeries.

Door de geconstateerde tekortkomingen loopt de rijksoverheid nog steeds risico's ten aanzien van het verlies, het onbedoeld bekend worden en de ongeautoriseerde wijziging of toevoeging van gegevens. De ministeries hebben zelf onvoldoende inzicht in de omvang van deze

risico's. Evenmin heeft de coördinerend minister van Binnenlandse Zaken dit voor de rijksdienst als geheel.

De Rekenkamer acht het positief dat de ministeries in het algemeen in hun antwoorden hebben laten weten dat zij de aanbevelingen van de Rekenkamer zullen overnemen. De coördinerend minister van Binnenlandse Zaken liet in zijn antwoord wel weten dat hij niet overweegt bovendepartementaal toezicht op te zetten. Volgens hem wordt afdoende beveiliging het meest effectief gerealiseerd door een decentrale aanpak met een eigen verantwoordelijkheid van de ministeries. De Rekenkamer vindt echter dat er voor het rijk als geheel inzicht moet bestaan in de mate waarin aan die verantwoordelijkheden invulling wordt gegeven. Zij dringt daarom aan op een periodieke informatieplicht aan de minister van Binnenlandse Zaken voor de ministers. De minister zegde toe in 1997 de noodzaak van een dergelijke informatieplicht te bezien. De Rekenkamer vindt dat echter te laat.

1. INLEIDING

1.1. Aanleiding tot het onderzoek

In 1988 publiceerde de Rekenkamer het tussentijds verslag «Computerbeveiliging; Beveiliging van gegevens in geautomatiseerde systemen bij de ministeries» (Tweede Kamer, vergaderjaar 1988–1989, 20 904, nrs. 1–2). Hieruit bleek dat de ministeries onvoldoende konden waarborgen dat grote risico's met betrekking tot gegevens in geautomatiseerde systemen waren afgedekt. De ministeries namen te weinig en alleen op ad hoc-basis beveiligingsmaatregelen; inzicht in risico's ontbrak veelal en risicoafwegingen werden nauwelijks gemaakt. Voorts signaleerde de Rekenkamer problemen bij de coördinatie door de minister van Binnenlandse Zaken. Ook werd vastgesteld dat de ministeries de Aanwijzingen van de minister-president met betrekking tot persoonsgegevens en gerubriceerde gegevens nauwelijks opvolgden en dat toezicht op naleving van centrale regelgeving ontbrak.

De informatiseringssituatie bij de ministeries heeft sinds 1988 ingrijpende veranderingen ondergaan, zoals:
- decentralisatie van de zeggenschap over de informatievoorziening;
- deconcentratie van de gegevensverwerking;
- opkomst van pc's;
- opkomst netwerken voor datacommunicatie;
- toename van gegevensverkeer binnen en tussen locaties.

Door deze veranderingen is de informatiserings-situatie bij de ministeries sinds het vorige onderzoek veelal complexer en daardoor moeilijker beheersbaar geworden. Het huidige onderzoek richt zich daarom niet alleen op de nakoming van toezeggingen door de ministers, maar vormt in de eerste plaats een nieuwe rijksbrede inventarisatie van de beheersing van de informatiebeveiliging bij de ministeries.

1.2. Doel en probleemstelling

Het onderzoek had als doel een oordeel te geven over het instrumentarium dat de secretarissen-generaal[1] en de minister van Binnenlandse Zaken als coördinerend bewindspersoon hebben gecreëerd om de informatiebeveiliging bij de rijksoverheid te beheersen.

De probleemstelling luidde als volgt:
1. Hebben de secretarissen-generaal c.q. de directeur-generaal der Belastingen een instrumentarium gecreëerd waarmee ze de informatiebeveiliging bij hun ministerie c.q. de Belastingdienst kunnen beheersen?
2. Heeft de minister van Binnenlandse Zaken toereikend invulling gegeven aan zijn coördinerende taak op het terrein van informatiebeveiliging?

Bij deze probleemstelling golden de volgende onderzoeksvragen:

Ad 1
- Is de wijze waarop de secretaris-generaal c.q. de directeur-generaal der Belastingen sturing geeft aan de informatiebeveiliging toereikend?
- Zijn het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen bij de ministeries toereikend?
- Zijn de wijze waarop de lijnorganisatie verantwoording aflegt aan de hogere echelons en de wijze waarop de ambtelijke top zich een oordeel vormt over de aanvaardbaarheid van de gerealiseerde informatiebeveiliging toereikend?

[1] De Belastingdienst, hoewel deel uitmakend van het ministerie van Financiën, is afzonderlijk in ogenschouw genomen. Dit vloeit voort uit het grote financiële en maatschappelijke belang van deze dienst.

Ad 2

– Heeft de minister van Binnenlandse Zaken voldoende activiteiten ontplooid om te bevorderen dat de in 1988 gesignaleerde tekortkomingen werden opgeheven?

– Heeft de minister van Binnenlandse Zaken aanvullend een instrumentarium gecreëerd waarmee op bovendepartementaal niveau beoordeeld kan worden of de informatiebeveiliging, zowel bij de afzonderlijke ministeries als ook bij de rijksdienst als geheel, aanvaardbaar is?

1.3. Correspondentie

Eind februari 1995 zond de Rekenkamer aan elke minister de bevindingen voor het eigen ministerie. De rijksbrede vergelijking werd meegezonden als achtergrondinformatie.

De minister van Binnenlandse Zaken is daarnaast gevraagd om een reactie te geven op de bevindingen over het algemene beeld bij de ministeries en over de rijksbrede coördinatie. De minister-president is ook verzocht te reageren op de bevindingen ten aanzien van een aspect van de rijksbrede coördinatie namelijk het Voorschrift Informatiebeveiliging Rijksdienst.

De ministers reageerden in maart en april 1995. De hoofdlijnen van deze reacties zijn in dit rapport verwerkt.

2. RIJKSBREDE BEVINDINGEN

2.1. Algemeen

In dit hoofdstuk geeft de Rekenkamer een algemeen beeld van de informatiebeveiligingssituatie bij de rijksoverheid. De aangelegde normen zijn weergegeven in bijlage 1. De bevindingen en conclusies voor de afzonderlijke ministeries zijn weergegeven in bijlage 2, evenals de reacties van de bewindslieden daarop en het nawoord van de Rekenkamer. Bijlage 3 geeft een schematisch overzicht van de conclusies per ministerie.

De Rekenkamer heeft een aantal normen geformuleerd voor de beheersing van de informatiebeveiliging. Deze normen zijn gegroepeerd in de drie volgende aandachtsgebieden:

– de wijze waarop de ambtelijke top sturing geeft aan de informatiebeveiliging;

– het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen bij een ministerie;

– de wijze waarop in de lijnorganisatie verantwoording wordt afgelegd aan de hogere echelons en de wijze waarop de ambtelijke top zich een oordeel vormt over de aanvaardbaarheid van de gerealiseerde informatiebeveiliging.

2.2. Sturing informatiebeveiliging

2.2.1. Risico-afweging

De Rekenkamer constateerde dat slechts een beperkt aantal ministeries risico-afwegingen voor het gehele ministerie uitvoerde. Bij de helft van de ministeries werd wel incidenteel een risico-afweging uitgevoerd voor een afzonderlijk rekencentrum of informatiesysteem.

Bij twee ministeries werkte men aan de ontwikkeling van een basisniveau voor de informatiebeveiliging. De realisatie van een basisniveau voor beveiliging ontslaat de gebruikers van de beveiligde infrastructuur echter niet van de plicht om zelf vast te stellen of de geboden beveiliging

toereikend is voor hun specifieke informatiesystemen. Zij moeten dus (aanvullend) een risico-afweging uitvoeren.

Ook voor informatiesystemen die door derden werden beheerd, constateerde de Rekenkamer dat slechts enkele ministeries vooraf een risico-afweging uitvoerden. Een aantal ministeries had de gegevensverwerking van één of meer informatiesystemen bij RCC (het voormalige Rijks Computercentrum) ondergebracht. Deze ministeries conformeerden zich veelal aan het standaardniveau voor de beveiliging bij RCC. Een aantal van deze ministeries verwees in dit verband naar de «Third Party Mededeling» (TPM) die in maart 1994 door de EDP-Auditpool is afgegeven over het beveiligingsstelsel Mainframe bij RCC. Dit beveiligingsstelsel garandeert een minimumniveau voor de beveiliging. Ministeries met kritische systemen zullen volgens de Rekenkamer echter aanvullende wensen en eisen moeten formuleren. Ook was voor een aantal informatiesystemen een afzonderlijke TPM afgegeven. Hoewel de Rekenkamer deze TPM's van groot belang acht, blijft het noodzakelijk dat ministeries zelf risico-afwegingen uitvoeren. De TPM's kunnen daarbij wel een belangrijke informatiebron zijn.

2.2.2. Informatiebeveiligingsbeleid

Iets meer dan de helft van de ministeries had een beleid voor de informatiebeveiliging vastgesteld. Ten opzichte van de situatie uit 1988 is dit een verbetering. Bij de overige zes ministeries ontbrak echter de basis om een adequaat niveau van informatiebeveiliging te creëren omdat het beveiligingsbeleid nog in ontwikkeling of gedateerd was of zelfs volledig ontbrak. De Rekenkamer achtte dit teleurstellend.

Ondanks het feit dat niet alle ministeries over beleid voor informatiebeveiliging beschikten bleek bij een ruime meerderheid wel duidelijkheid te bestaan over verantwoordelijkheden op het gebied van informatiebeveiliging, met uitzondering van de verantwoordelijkheden voor het toezicht erop (zie paragraaf 2.4).

2.2.3. Beveiligingsplannen en calamiteitenplannen

De nadere uitwerking van het informatiebeveiligingsbeleid in beveiligings- en calamiteitenplannen vertoonde vrijwel altijd in meer of mindere mate ernstige tekortkomingen. Alleen het Ministerie van Defensie voldeed goeddeels aan de norm. In vergelijking met 1988 was er nauwelijks vooruitgang geboekt, ondanks de ontwikkeling van informatiebeveiligingsbeleid bij diverse ministeries. Daar komt nog bij dat calamiteitenplannen vrijwel nooit voldoende getest werden.

Voorts ontbraken bij de helft van de ministeries toereikende beveiligingsinstructies voor het personeel.

Iets minder dan de helft van de ministeries had in de calamiteitenplannen voldoende aandacht besteed aan de continuïteit van de bedrijfsvoering. Slechts twee ministeries hadden procedures voor noodvernietiging van gegevens opgesteld. De overige ministeries hadden niet expliciet nagegaan of er omstandigheden konden optreden die de aanwezigheid van deze noodprocedures noodzakelijk maken.

2.3. Centraal beleid en algemene richtlijnen voor beveiligingsmaatregelen

2.3.1. Systeemontwikkeling en -onderhoud

De Rekenkamer constateerde dat beveiligingsaspecten bij het ontwikkelen en onderhouden van systemen nog onvoldoende aandacht kregen.

Bij slechts enkele ministeries was zowel de rol van de beveiligings-

functionaris als die van de accountantsdienst helder aangegeven. In veel gevallen werden zij in het geheel niet betrokken bij de ontwikkeling van informatiesystemen.

De helft van de ministeries beschikte over voldoende waarborgen dat wijzigingen in applicaties op beheersbare wijze werden uitgevoerd. Iets minder dan de helft van de ministeries had voldoende waarborgen dat op elk moment de juiste versie van geautoriseerde programmatuur in de produktieomgeving was geïnstalleerd.

Meer dan de helft van de ministeries had adequate richtlijnen vastgesteld voor de fysieke en organisatorische functiescheiding tussen ontwikkel-, test- en produktie-omgeving. De ministeries die geen functiescheiding hadden voorgeschreven gaven veelal aan dat zij deze scheidingen in de praktijk wel hadden gerealiseerd.

Slechts twee ministeries hadden aandacht besteed aan procedures die gevolgd moeten worden bij het optreden van verstoringen in de gegevensverwerking.

Tenslotte beschikte slechts een beperkt aantal ministeries over toereikende richtlijnen om beveiligingsaspecten in het systeemontwerp en in de documentatie van operationele informatiesystemen te behandelen.

2.3.2. Toegang tot en het gebruik van gegevens

Het verlenen van toegang tot informatiesystemen behoorde veelal tot de decentrale verantwoordelijkheden. De Rekenkamer constateerde echter dat slechts bij enkele ministeries het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldoende duidelijkheid verschaften over de uitgangspunten die de lijnmanagers hierbij moesten hanteren. Deze situatie draagt het risico in zich dat niet in de gehele organisatie de logische toegangsbeveiliging op een adequaat niveau is gebracht.

Bij iets minder dan de helft van de ministeries waren toereikende richtlijnen aangetroffen om gegevens te differentiëren naar de mate waarin zij kwetsbaar zijn voor ongeautoriseerde toegang. Twee ministeries werkten aan een dergelijke richtlijn.

2.3.3. Personele maatregelen

De Rekenkamer acht het van belang dat elk ministerie duidelijk vaststelt hoe bepaald wordt welke functionarissen een veiligheidsonderzoek moeten ondergaan. Dit geldt vooral voor automatiseringsmedewerkers, die immers uit hoofde van hun functie veelal eenvoudig toegang hebben tot belangrijke gegevens in geautomatiseerde systemen. Dit geldt niet alleen voor het eigen personeel, maar zeker ook voor automatiseringspersoneel dat bij externe bureaus wordt ingehuurd.

De helft van de ministeries bleek helderheid te hebben geschapen over veiligheidsonderzoeken van het eigen automatiseringspersoneel. Enkele ministeries die geen beleid op dit punt hadden geformuleerd hadden wel maatregelen getroffen. Iets minder dan de helft van de ministeries nam voldoende maatregelen voor extern personeel. Deze personeelsleden werden in het algemeen niet gescreend. Meestal werden in het contract met de externe organisatie wel afspraken gemaakt over geheimhouding. De Rekenkamer acht dit een te beperkte maatregel. Een geheimhoudingsverklaring vormt op zichzelf een waardevolle maatregel maar ondervangt niet de noodzaak om automatiseringsfuncties met een veiligheidsrisico te bezetten met betrouwbaar personeel. Door screening kan dit tot op zekere hoogte worden gerealiseerd.

Op het gebied van richtlijnen voor functiescheiding was ten opzichte van het onderzoek uit 1988 een duidelijke verbetering waarneembaar. Een ruime meerderheid van de ministeries beschikte ten tijde van het nieuwe onderzoek over dergelijke richtlijnen.

2.3.4. Privacyreglementen

De Wet persoonsregistraties die 1 juli 1989 van kracht is geworden, legt de verplichting op om voor bepaalde persoonsregistraties privacy-reglementen op te stellen.

De Rekenkamer constateerde dat acht ministeries in belangrijke mate of geheel aan deze eis hadden voldaan. De overige ministeries hadden nog niet voor alle reglementsplichtige systemen een privacyreglement opgesteld of hadden hierover geen informatie. Mede gelet op de voorbeeldfunctie van de rijksoverheid acht de Rekenkamer het van groot belang dat de ministeries die in gebreke zijn gebleven op een zo kort mogelijke termijn aan de wettelijke eisen gaan voldoen en dat de ministeries die onvoldoende inzicht in de volledigheid hebben nagaan of zij aan de eisen voldoen.

2.3.5. Toetsbaarheid fysieke beveiliging

Het onderzoek heeft zich niet uitgestrekt tot de feitelijk getroffen maatregelen ten aanzien van de fysieke beveiliging. Wel is nagegaan of de getroffen maatregelen gebaseerd waren op een risico-afweging, zodat een bewuste keuze kon worden gemaakt voor een optimaal stelsel van beveiligingsmaatregelen. Deze vorm van risico-afweging richt zich op een specifiek deelgebied van de informatiebeveiliging. Onvoldoende aandacht in deze fase zal vrijwel onontkoombaar leiden tot beveiligingsrisico's (te weinig maatregelen) of tot ondoelmatigheid (teveel maatregelen).

De Rekenkamer constateerde dat minder dan de helft van de ministeries de fysieke beveiligingsmaatregelen had getroffen op grond van een expliciete risico-afweging. Wel had iets meer dan de helft van de ministeries voldoende inzicht in de vraag of er bij de diverse locaties fysieke maatregelen van kracht waren. Bij de ministeries waar dat inzicht ontbrak was dus onvoldoende gewaarborgd dat in de gehele organisatie de juiste fysieke maatregelen waren getroffen.

2.4. Toezicht

2.4.1. Verantwoording in de «lijn»

Vrijwel alle ministeries hebben belangrijke taken op het gebied van de informatiebeveiliging op decentraal niveau neergelegd. Het is wellicht een te stringente eis dat het centraal niveau beschikt over een beschrijving van de feitelijke beveiligingssituatie bij de dienstonderdelen. Echter, gelet op de grootte van de verschillende ministeries, zijn bij verantwoording over de informatiebeveiliging en bij de controle daarvan veelal schriftelijke rapportages noodzakelijk. Dergelijke overzichten verschaffen vooral duidelijkheid over de naleving van het informatiebeveiligingsbeleid. Slechts twee ministeries beschikten over een vrij volledige beschrijving van de feitelijke beveiligingssituatie. Bij de overige ministeries ontbraken dergelijke beschrijvingen of waren slechts rapportages op onderdelen beschikbaar.

Ten aanzien van de informatieverschaffing in de richting van de secretaris-generaal en de hiervoor gehanteerde rapportagelijnen voldeed een ruime meerderheid van de ministeries in opzet aan de norm. Hierbij moet worden opgemerkt dat de secretaris-generaal veelal uitsluitend werd geïnformeerd indien zich bijzondere voorvallen hadden voorgedaan.

2.4.2. Onafhankelijke controle

De departementale accountantsdiensten zijn ingevolge het Besluit taak departementale accountantsdienst (Besluit van 2 juli 1987, Stb. 384) belast met de controle van systemen die een relatie hebben met de financiële

verantwoording. Bij grotere en geautomatiseerde systemen omvat die controle ook beoordeling van continuïteit, de beveiliging, de privacybescherming en de controleerbaarheid van de systemen.

In de praktijk is maar zelden duidelijk of een accountantsdienst ook de controle op de informatiebeveiliging in brede zin als taak heeft. Hoewel bij slechts enkele ministeries de accountantsdienst een formele opdracht had gekregen om controle uit te oefenen op informatiebeveiliging in brede zin verrichtten de accountantsdiensten deze controle in de praktijk bij de helft van de ministeries wèl. Bij de andere helft bleek de controle beperkt tot de systemen die een relatie hebben met de financiële verantwoording. Het is daarom belangrijk dat deze taak formeel wordt toegewezen.

2.5. Situatie per ministerie

De Rekenkamer constateerde dat de beheersing van de informatiebeveiliging bij de Belastingdienst en bij de ministeries van Algemene Zaken, van Buitenlandse Zaken, van Defensie en van Landbouw, Natuurbeheer en Visserij op een behoorlijk niveau was gebracht. Bij de overige departementen kwalificeerde de Rekenkamer de beheersing nog als ontoereikend, en in het geval van het Ministerie van Sociale Zaken en Werkgelegenheid zelfs als volstrekt onvoldoende. Wel constateerde zij in een ruime meerderheid van de gevallen een verbetering ten opzichte van het onderzoek uit 1988. De Rekenkamer meende dat de meeste ministeries nog belangrijke inspanningen moesten verrichten om binnen de invoeringstermijn van twee jaar vanaf 1 januari 1995 aan het voorschrift voor de informatiebeveiliging bij de rijksdienst (zie paragraaf 3.3) te voldoen. Eerdere onderzoeken van de Rekenkamer onderstrepen deze conclusie (zie de rapportages over de ministeries van Verkeer en Waterstaat en van Landbouw, Natuurbeheer en Visserij).

De Rekenkamer achtte het positief dat de ministers in het algemeen in hun antwoord hebben laten weten dat zij de aanbevelingen van de Rekenkamer zullen overnemen (Voor de uitgebreide bevindingen en conclusies wordt verwezen naar bijlage 2).

2.6. Conclusies

De wijze waarop de ambtelijke top sturing gaf aan de informatiebeveiliging was in het algemeen onvoldoende. De belangrijkste tekortkomingen waren:

– de meeste ministeries hadden onvoldoende inzicht in risico's;
– bijna de helft van de ministeries had geen actueel beleid voor informatiebeveiliging;
– beleid voor informatiebeveiliging werd niet altijd uitgewerkt in beveiligings- en calamiteitenplannen, waardoor beveiligingsmaatregelen teveel op ad hoc basis werden genomen.

Het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen vertoonden bij veel ministeries tekortkomingen op het gebied van systeemontwikkeling en -onderhoud, toegang tot en het gebruik van gegevens, personele maatregelen, privacyreglementen en toetsbaarheid van de fysieke maatregelen.

Tot slot was bij een aantal ministeries het toezicht op de informatiebeveiliging ontoereikend. Dit uitte zich met name door:

– onvoldoende zicht op de feitelijke beveiligingssituatie en ontoereikende verantwoording «in de lijn»;
– ontbrekende of te beperkte reikwijdte van de onafhankelijke controle op de informatiebeveiliging.

Deze tekortkomingen hadden tot gevolg dat de beheersing van de informatiebeveiliging nog niet toereikend was, ondanks de verbeteringen sinds het vorige onderzoek.

Volgens de Rekenkamer loopt de rijksoverheid door de geconstateerde tekortkomingen nog steeds risico's van een onbekende omvang. Tot deze risico's horen met name het verlies, het onbedoeld bekend worden en de ongeautoriseerde wijziging of toevoeging van gegevens.

2.7. Antwoord minister

De minister van Binnenlandse Zaken erkende dat er bij de rijksoverheid nog veel zou moeten gebeuren om de informatiebeveiliging te verbeteren. In de ogen van de minister zouden deze activiteiten zich vooral moeten richten op de beveiliging van de datacommunicatie tussen overheidsinstanties onderling en met het bedrijfsleven en de burger.

Ten aanzien van het inzicht in de risico's die de rijksoverheid loopt door tekortkomingen in de beveiliging, stelde de minister dat er moest worden toegewerkt naar een situatie waarin de verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging helder en op het juiste niveau zijn vastgelegd. Dan zou ook op het juiste niveau bekend zijn of afdoende maatregelen zijn getroffen en of besloten is bepaalde risico's bewust te accepteren. Hij erkende dat deze situatie nog niet in de gehele rijksdienst gerealiseerd was, waardoor de situatie onbevredigend was voor de rijksoverheid als geheel.

2.8. Nawoord Rekenkamer

Door nieuwe technologische mogelijkheden zal inderdaad het gebruik van datacommunicatie in de nabije toekomst nog fors toenemen. De Rekenkamer onderkent dan ook het nut van deze prioriteit, maar vindt dat ook aandacht moet worden geschonken aan het verbeteren van de overige tekortkomingen die in dit rapport zijn vermeld.

3. COÖRDINATIE DOOR DE MINSTER VAN BINNENLANDSE ZAKEN

3.1. Algemeen

Bij het opstellen van de normen voor de beoordeling van de coördinatie door het Ministerie van Binnenlandse Zaken is gelet op de toezeggingen die de toenmalige minister in 1988 aan de Rekenkamer heeft gedaan. Daarnaast zijn de normen gebaseerd op de taken van de minister van Binnenlandse Zaken die volgens de Rekenkamer voortvloeien uit het Besluit informatievoorziening in de rijksdienst 1990 (Tweede Kamer, vergaderjaar 1990–1991, 20 644, nr. 14). Deze uitgangspunten leiden tot de volgende normen:

– de minister moet de toezeggingen uit 1988 nakomen;
– de minister moet adequate regelgeving voorbereiden;
– de taken en verantwoordelijkheden die de minister toewijst, moeten betrekking hebben op alle elementen van de beheersing van de informatiebeveiliging, dus op sturing, uitvoering, lijntoezicht en onafhankelijke controle;
– de minister moet periodiek geïnformeerd worden over de situatie ten aanzien van de informatiebeveiliging bij elk afzonderlijk ministerie, zodat hij periodiek kan evalueren of het centrale beleid door de afzonderlijke ministeries wordt nageleefd.

3.2. Nakoming toezeggingen minister

Naar aanleiding van het Rekenkameronderzoek uit 1988 zegde de minister van Binnenlandse Zaken toe een onderzoek in te stellen om na te gaan of het beveiligingsbeleid moest worden bijgesteld. Eén van de aandachtspunten hierbij was de noodzaak om te komen tot een ondersteunend bureau voor de beveiliging bij de rijksoverheid. Tevens zou de minister aandacht besteden aan de noodzaak van aanvullende voorschriften en aanbevelingen. Wat betreft de privacyreglementen verwees de minister naar het toen nog in behandeling zijnde voorstel van de Wet persoonsregistraties.

De Rekenkamer constateert dat de minister zijn toezeggingen is nagekomen: er is onderzoek uitgevoerd naar de kwetsbaarheid van bestuurlijke informatiesystemen, het informatiebeveiligingsbeleid voor de Rijksdienst is vernieuwd en er is een ondersteunend bureau voor de beveiliging bij de rijksoverheid ingesteld. Op het gebied van de persoonsregistraties is inmiddels de Wet persoonsregistraties (WPR) aangenomen en daarbij is de Registratiekamer als toezichthoudend orgaan aangewezen. De Registratiekamer heeft onlangs een advies voor de bescherming van de exclusiviteit van persoonsregistraties uitgebracht.

Vooral de instelling van de Interdepartementale Commissie Informatiebeveiliging (ICIB) en het Advies- en Coördinatiepunt Informatiebeveiliging (ACIB) in 1991 zijn als belangrijke ontwikkelingen aan te merken. Deze ontwikkelingen zijn evenwel langzaam op gang gekomen. Mede hierdoor is de daadwerkelijke ondersteuning van de ministeries tot begin 1994 zeer beperkt gebleven.
De ministeries gaven tijdens het huidige onderzoek aan dat ze een negatieve indruk van ICIB hadden en vertoonden scepsis over het nut van een instantie zoals ACIB. Daarom zal er nog een belangrijke inspanning moeten worden verricht om alsnog het vertrouwen van de ministeries te winnen en hun actieve medewerking te verkrijgen. De resultaten van de recente evaluatie van ICIB/ACIB in opdracht van het Ministerie van Binnenlandse Zaken kunnen bijdragen aan de besluitvorming over de verdere vormgeving van de coördinerende rol van dit ministerie.

3.3. Besluit voorschrift informatiebeveiliging rijksdienst

De Rekenkamer beschouwt ook het in werking treden per 1 januari 1995 van het nieuwe Voorschrift informatiebeveiliging Rijksdienst (VIR) een belangrijke stap in de goede richting. Het VIR rekent het tot de taak van de afzonderlijke ministeries de eigen informatievoorziening te beveiligen. Ook dit voorschrift en het bijbehorende Handboek Informatiebeveiliging hebben echter lang op zich laten wachten. Dit heeft stagnerend gewerkt op de ontwikkelingen bij de afzonderlijke ministeries omdat deze lang in onzekerheid bleven over de precieze bepalingen van dit voorschrift.

Bij de aanvang van het onderzoek van de Rekenkamer was het Ministerie van Binnenlandse Zaken nog bezig het VIR op te stellen. Het voorschrift is daarom niet betrokken in de overwegingen bij het opstellen van de normen voor het onderzoek. Desondanks is er een sterke parallel zichtbaar in de benadering van de beheersingsproblematiek. Er is echter niet voorzien in controle op de naleving van het voorschrift, aansluitend op de voorgeschreven controle door de ministeries zelf. Zonder dit complement van sturing vanuit het bovendepartementaal niveau is de effectiviteit van deze sturing niet voldoende gewaarborgd. Evenmin is aangegeven hoe de minister van Binnenlandse Zaken moet worden geïnformeerd ten behoeve van de evaluatie van het bovendepartementaal beleid voor de informatiebeveiliging.

Het voorschrift is gericht op de rijksdienst. Het heeft geen rechtstreekse werking op de Hoge Colleges van Staat en op zelfstandige bestuursorganen. De Rekenkamer achtte de speelruimte die het VIR de ministeries biedt bij het maken van afspraken met zelfstandige bestuursorganen te ruim, waardoor het risico bestaat dat niet in alle gevallen de beveiliging goed geregeld is. De toelichting op het voorschrift stelt namelijk de ministers ervoor verantwoordelijk dat het voorschrift of een vergelijkbaar ander stelsel van bepalingen van toepassing wordt op de bestuursorganen in kwestie, doch het voorschrift zelf schrijft dit niet expliciet voor.

3.4. Conclusies en aanbevelingen

De Rekenkamer concludeerde dat de minister van Binnenlandse Zaken in belangrijke mate invulling heeft gegeven aan zijn coördinerende rol op het gebied van de informatiebeveiliging bij het Rijk, maar wees tevens op de volgende tekortkomingen:
– de beheersing van de informatiebeveiliging bij ZBO's was nog niet geregeld; bovendien had het VIR te lang op zich laten wachten;
– het belang van een duidelijke vastlegging van de verantwoordelijkheid voor het bovendepartementale toezicht op de informatiebeveiliging werd nog niet onderkend;
– het ministerie had nog geen invulling gegeven aan zijn taak op het gebied van de evaluatie van de beveiligingssituatie bij de ministeries.

De Rekenkamer beval aan om duidelijk te maken hoe het toezicht op de informatiebeveiliging op bovendepartementaal niveau moet worden geregeld. Voorts werd aanbevolen om nader voor te schrijven op welke wijze de ministeries en de rijksdienst als geheel verantwoording moeten afleggen over de naleving van het VIR. Hierbij werd de suggestie gedaan te denken aan verantwoordingsinformatie in de automatiseringsbijlagen bij de departementale begrotingen en de jaaroverzichten informatievoorziening rijksdienst.

3.5. Antwoord minister

De minister was het niet met de Rekenkamer eens dat het VIR te lang op zich had laten wachten. Het tot stand komen van het besluit was in hoge mate een proces van consensusvorming geweest, waardoor er een goed draagvlak voor de nieuwe regelgeving gecreëerd is. De minister had ook geen aanwijzingen dat de ministeries door de duur van de voorbereiding vertraging hadden opgelopen bij hun eigen activiteiten voor de informatiebeveiliging. In de ogen van de minister zou dat ook niet kunnen omdat de hoofdlijnen van het voorschrift al vrij snel vaststonden.

Over ICIB en het uitvoerend orgaan ACIB merkte de minister op dat deze commissies een belangrijke rol hebben gespeeld bij bewustwordingsprocessen. Mede als verdienste van de ICIB was langzamerhand verandering tot stand gekomen in de zienswijze van veel betrokken partijen. In het verleden werd namelijk vaak niet ingezien dat informatiebeveiliging expliciet de aandacht van het topmanagement van de ministeries vereist. De minister deelde mee de organisatorische aspecten van de informatiebeveiliging centraal te stellen als uitgangspunt voor de interdepartementale samenwerking in de komende jaren. Daartoe zou op hoog strategisch niveau een beraad worden georganiseerd als opvolger van de ICIB. De minister was van mening dat er inmiddels voorwaarden aanwezig waren voor een ook naar buiten positieve waardering van de ministeries voor dit beraad. Hij verwachtte dat de scepsis over het nut van de ACIB bij een aantal ministeries nog in 1995 verdwenen zou zijn.

De minister was het met de Rekenkamer eens dat het van belang is dat ook bij de zelfstandige bestuursorganen (ZBO's) de informatiebeveiliging afdoende is geregeld. Hij zegde toe in 1995 een voorstel aan de Ministerraad voor te leggen om de toepassing van het VIR bij deze organisaties strakker te regelen. In dat voorstel komt ook de informatiebeveiliging bij de Hoge Colleges van Staat aan de orde. Voorts wees de minister erop dat het onderwerp ook aan de orde komt bij de reeds aangekondigde herbezinning op de wijze waarop het kabinet omgaat met ZBO's.

De minister gaf aan niet te overwegen om een vorm van bovendepartementale controle door of namens zijn ministerie op te zetten. Naar het oordeel van de minister kan de verantwoordelijkheid voor afdoende beveiliging het meest effectief gerealiseerd worden door een decentrale aanpak, waarin in ieder geval de eigen verantwoordelijkheid van de ministeries gerespecteerd dient te worden. Hierbij hoort volgens hem geen bovendepartementale controle, anders dan het toezicht dat door de Tweede Kamer (al dan niet via de Algemene Rekenkamer) wordt geïnitieerd. Eén van de redenen om af te zien van bovendepartementaal toezicht was het belang dat de minister hechtte aan de beveiliging van gegevensuitwisseling tussen ministeries en andere partijen. Hij wees erop dat het VIR al voorschrijft dat «informatische relaties» tussen ministeries en andere instanties vergezeld gaan van schriftelijken afspraken over de beveiliging. Bovendepartementale controle zou zich ook dienen uit te strekken over alle informatische relaties die de overheid, met inbegrip van de ZBO's onderhoudt. Dat zou in de ogen van de minister feitelijk neerkomen op een poging het (overheids)verkeer op de «elektronische snelweg» aan centrale controle te onderwerpen. De minister stelde dat een dergelijke controle niet past in het perspectief van een interactieve overheid.

De minister zag wel de noodzaak in van inzicht in de stand van de informatiebeveiliging bij de rijksoverheid. De minister wees in dit verband op een geplande evaluatie van de Privacy-Raamovereenkomst tussen de Staat en RCC. Deze evaluatie speelt een rol bij het nemen van een beslissing over het al dan niet continueren van deze raamovereenkomst. Voorts wees de minister op een effectrapportage over het VIR die medio 1997 zal worden opgesteld. In de huidige situatie beschikt de minister over de rapportages die jaarlijks in het kader van de raamovereenkomst worden uitgebracht over de beveiliging van persoonsgegevens die door RCC worden bewerkt.

De minister zegde toe begin 1997 te bezien of het noodzakelijk is voor de uitvoering van zijn coördinerende taak een periodieke informatieplicht aan de ministeries op te leggen.

3.6. Nawoord Rekenkamer

De Rekenkamer is het met de minister eens dat bij «informatische relaties» tussen de rijksdienst en andere instanties schriftelijke afspraken over beveiliging moeten worden gemaakt. De eigen verantwoordelijkheid die de individuele ministers voor een toereikende beveiliging dragen, laat echter onverlet dat het voor het Rijk als geheel en dus voor de coördinerend minister van belang is dat inzicht bestaat in de mate waarin aan die verantwoordelijkheden invulling wordt gegeven. Zonodig kunnen dan aanvullende maatregelen worden genomen. Dit betekent niet dat daarmee het gegevensverkeer zelf aan controle wordt onderworpen. De Rekenkamer is het daarom niet eens met de stelling van de minister dat bovendepartementale controle niet zou passen in het perspectief van een interactieve overheid.

Het bovendepartementale toezicht kan ook een basis zijn voor de Tweede Kamer om zelf tot een oordeel te komen over de toereikendheid van de informatiebeveiliging. De Rekenkamer dringt er daarom op aan als

eerste stap voor bovendepartementaal toezicht reeds nu de ministers een periodieke informatieplicht op te leggen en niet de effectrapportage van het VIR af te wachten.

BIJLAGE 1. **HET GEHANTEERDE NORMENKADER**

1. Sturing informatiebeveiliging

1.1. Risico-afweging

a. Er dient periodiek een risico-afweging op hoofdlijnen te worden gemaakt die, hoewel globaal, het gehele ministerie bestrijkt. De afweging dient te worden vastgelegd en formeel te worden vastgesteld als basis voor het beleid op het gebied van de informatiebeveiliging.
b. De risico-afweging dient zich ook uit te strekken tot informatiesystemen waarvan het beheer buiten het ministerie is gelegen.

1.2. Informatiebeveiligingsbeleid

c. Er dient periodiek een beleid voor de informatiebeveiliging te worden vastgelegd en vastgesteld, geldend voor het gehele ministerie.
d. Het beleid dient objecten aan te geven alsmede aan welke kwaliteitsaspecten belang wordt gehecht, en dient duidelijk te maken welk afbreukrisico ontstaat door eventuele tekortkomingen in de beveiliging. Voorbeelden van objecten kunnen zijn: bedrijfsprocessen, gegevensverzamelingen, informatiesystemen en/of technische infrastructuren.
e. Het beleid dient tevens aan te geven welke verantwoordelijkheden er aan functionarissen/ afdelingen worden toegedeeld met het oog op de concretisering van het beleid, de uitvoering van dat beleid en het toezicht daarop.

1.3. Beveiligingsplannen en calamiteitenplannen

f. De plannen dienen actueel te zijn.
g. In deze plannen of documenten die daar verband mee houden dienen schriftelijke beveiligingsinstructies te zijn opgenomen voor automatiseringspersoneel en eindgebruikers.
h. Procedures, met name die welke in de calamiteitenplannen zijn voorgeschreven, dienen te zijn getest en geëvalueerd.
i. Ten aanzien van de calamiteitenplannen is aanvullend de norm gehanteerd dat er aandacht dient te worden besteed aan de continuïteit van de bedrijfsvoering en aan procedures voor noodvernietiging van gegevens.

2. Centraal beleid en algemene richtlijnen voor beveiligingsmaatregelen

2.1. Systeemontwikkeling en -onderhoud

Het beleid dient:
j. duidelijkheid te verschaffen over de rollen die aan de beveiligingsfunctionaris en de accountantsdienst worden toegekend bij trajecten voor systeemontwikkeling. Mogelijke rollen kunnen zijn: adviserend, controlerend of het naar voren brengen van eigen eisen als gebruiker van het systeem (bijvoorbeeld controletotalen);
k. voor te schrijven dat er waarborgen aanwezig zijn dat alle activiteiten die leiden tot wijzigingen in applicaties op een vergelijkbare wijze beheerst worden als de trajecten voor systeemontwikkeling;
l. voor te schrijven dat er waarborgen aanwezig zijn dat op elk moment uitsluitend de juiste versies van de geautoriseerde programmatuur in een produktieomgeving geïnstalleerd zijn;
m. richtlijnen te geven voor de fysieke en organisatorische scheiding van ontwikkel-/test-/ en produktieomgeving en voor de procedures die gevolgd dienen te worden indien zich bijzondere voorvallen voordoen

(bijvoorbeeld ingeval zich de noodzaak voordoet dat systeem-programmeurs ingrijpen in een operationeel systeem);

n. richtlijnen te geven voor de wijze waarop beveiligingsaspecten worden behandeld in het systeemontwerp en in de documentatie van operationele informatiesystemen.

2.2. Toegang tot en gebruik van gegevens

Het beleid dient:

o. betrekking te hebben op alle «toegangspoorten» die gebruikers tot gegevens hebben, inclusief de relevante datacommunicatie- en besturingsprogrammatuur;

p. richtlijnen op dit gebied te geven, gedifferentieerd naar de mate waarin applicaties en/of gegevens kwetsbaar zijn voor ongeautoriseerde toegang;

q. aan te geven volgens welke uitgangspunten verantwoordelijkheden op het gebied van autorisaties toegedeeld dienen te worden. Het gaat hierbij om de verantwoordelijkheden voor respectievelijk de toekenning van autorisaties, de implementatie ervan, het inhoudelijk toezicht daarop en de controle op de juiste technische implementatie van deze autorisaties. Hiermee moet worden voorkomen dat toekenning, implementatie en toezicht ten aanzien van toegekende autorisaties in handen van één enkele functionaris kunnen komen te liggen.

2.3. Personele maatregelen

Het beleid dient:

r. duidelijk te maken of en in welke gevallen eigen automatiserings-personeel een veiligheidsonderzoek dienen te ondergaan;

s. duidelijk te maken of en in welke gevallen er maatregelen ten aanzien van extern automatiseringspersoneel noodzakelijk zijn;

t. aan te geven welke functiescheidingen vereist zijn.

2.4. Privacy-reglementen

u. het beleid dient voor te schrijven dat voor elke persoonsregistratie die daar volgens de Wet persoonsregistraties (WPR) voor in aanmerking komt, een privacyreglement wordt vastgesteld.

2.5. Toetsbaarheid fysieke beveiliging

Het antwoord op de vraag welke maatregelen in de fysieke sfeer zinvol zijn hangt samen met de specifieke kenmerken van de huisvesting als ook van de geïnstalleerde apparatuur en programmatuur op de locatie in kwestie en de aard van de gegevens die er verwerkt worden. Dit maakt het moeilijk, meer nog dan in de organisatorische sfeer, normen met algemene geldigheid aan te leggen. Toetsing wordt eerst mogelijk als bekend is welke inbreuken op de fysieke beveiliging er in de concrete situatie mogelijk zijn en welke gevolgen deze kunnen hebben. Voorts moet bekend zijn welke maatregelen betrekking hebben op welke fysieke locaties, computersystemen en/of informatiesystemen. Daarom zijn de volgende normen gehanteerd.

v. De fysieke maatregelen dienen gebaseerd te zijn op een vastgelegde risico-afweging.

w. Per fysieke locatie dient duidelijk te zijn welke voorschriften voor fysieke beveiliging gelden.

3. Toezicht

3.1. Verantwoording in de «lijn»

y.[1] Het ministerie moet op centraal niveau de beschikking hebben over een globale beschrijving van de feitelijke beveiligingssituatie binnen het gehele ministerie. Wanneer expliciet sprake is van een gedecentraliseerde verantwoordelijkheid ten aanzien van informatiebeveiliging dienen dergelijke overzichten op decentraal niveau aanwezig te zijn.

z. De secretaris-generaal dient (op structurele wijze) van informatie te worden voorzien over de hoofdlijnen van deze beveiligingssituatie.

3.2. Onafhankelijke controle

aa. De controle dient te geschieden door een afdeling die geen bemoeienis heeft met voorbereiding of vaststelling van het beleid voor de informatiebeveiliging, noch met de uitvoering van dat beleid.

ab. De controle dient formeel aan de afdeling in kwestie te zijn opgedragen.

[1] De letter x is niet gebruikt.

BIJLAGE 2. INFORMATIEBEVEILIGING PER MINISTERIE

Ministerie van Algemene Zaken

De wijze waarop de ambtelijke top sturing gaf aan de informatiebeveiliging voldeed in belangrijke mate aan de norm. Een tekortkoming was nog het ontbreken van een risico-afweging op hoofdlijnen.

Ook het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden goeddeels aan de normen. De wijze waarop beveiligingsaspecten moeten worden behandeld in het systeemontwerp en in de documentatie van operationele informatiesystemen en procedures rond het verstrekken van autorisaties verdienen nog nadere aandacht.

Voor wat betreft het toezicht concludeerde de Rekenkamer dat de wijze waarop de lijnorganisatie verantwoording aflegde grotendeels aan de normen voldeed. De onafhankelijke controle van de beveiligingssituatie beperkte zich echter tot systemen die een rol spelen bij de financiële verantwoording en strekte zich niet uit tot informatiebeveiliging in brede zin. De controle op informatiebeveiliging in brede zin was formeel nog niet opgedragen.

Samenvattend was de Rekenkamer van oordeel dat de informatiebeveiliging bij het ministerie van Algemene Zaken op een behoorlijk peil was gebracht, zeker in vergelijking met het onderzoek uit 1988. Wel moest worden geconstateerd dat het ontbreken van een risico-afweging ook toen al onder de aandacht van de toenmalige minister was gebracht.

De minister-president, minister van Algemene Zaken, deelde mee dat het ministerie een project gestart was waarbij uitwerking werd gegeven aan de aanbevelingen en opmerkingen van de Rekenkamer. Dit project zou onder meer leiden tot op schrift gestelde voorschriften en richtlijnen.

Ministerie van Buitenlandse Zaken

De wijze waarop de ambtelijke top sturing gaf aan de informatiebeveiliging bij het kerndepartement voldeed in belangrijke mate aan de normen. Wel verdiende met name de uitwerking van het beleid in decentrale calamiteiten- en beveiligingsplannen nog nadere aandacht. Nog niet alle organisatie-onderdelen hadden dergelijke plannen opgesteld. Naar aanleiding van twijfels bij het ministerie zelf over de vraag of de informatiebeveiliging bij de buitenlandse posten overal de vereiste aandacht kreeg vroeg de Rekenkamer zich af of het kerndepartement voldoende in staat was sturing te geven aan de beveiliging bij de posten.

Het centrale beleid en algemene richtlijnen voor beveiligingsmaatregelen voldeden eveneens goeddeels aan de normen. Slechts op een aantal gebieden was enige aanscherping gewenst. Het ging hierbij met name om richtlijnen voor de behandeling van beveiligingsaspecten in het systeemontwerp. Daarnaast verdienden de risico-afwegingen voor de fysieke beveiliging van de verschillende fysieke locaties, waaronder de buitenlandse posten, nog nadere aandacht. Uit de beperkte risico-afweging bleek niet of de getroffen maatregelen de meest effectieve en efficiënte waren om de bedreigingen het hoofd te bieden.

Ook het toezicht op de informatiebeveiliging binnen het ministerie was in grote lijnen toereikend. De taken die de accountantsdienst had met betrekking tot de controle van de informatiebeveiliging in brede zin (dus inclusief de niet-financiële systemen) waren echter nog niet formeel beschreven.

Samenvattend was de Rekenkamer van oordeel dat de informatiebeveiliging bij het ministerie van Buitenlandse Zaken op een behoorlijk niveau was gebracht, zeker in vergelijking met de situatie uit 1988.

Het ministerie had de afgelopen jaren veel inspanningen verricht om het beveiligingsbeleid expliciet te maken. Dit had geresulteerd in een duidelijk beleidskader dat als fundament voor een adequaat beveiligingsniveau kon worden beschouwd.

De Rekenkamer beval aan om nadere aandacht en uitwerking te geven aan de beveiligings- en calamiteitenplannen op decentraal niveau en aan de beveiligingssituatie op de buitenlandse posten.

De minister deelde mee dat hij de conclusies van de Rekenkamer onderschreef. Hij liet weten dat het beleid voor de informatiebeveiliging onlangs was bijgesteld en neergelegd in een beleidsdocument «Informatiebeveiliging» dat binnenkort zou worden vastgesteld en bekend gemaakt binnen het ministerie.

De minister kondigde wijzigingen aan in de sturing van de informatiebeveiliging door de ambtelijke top. Voorts gaf hij aan dat gewerkt werd aan richtlijnen voor de behandeling van beveiligingsaspecten in het systeemontwerp.

De minister onderschreef de conclusie van de Rekenkamer dat nog nadere aandacht geschonken diende te worden periodieke risicoafwegingen voor de beveiliging van de posten in het buitenland.

Hij berichtte ook dat de komende jaren speciale aandacht zou worden besteed aan de invoering van decentrale beveiligings- en calamiteitenplannen zowel bij het ministerie zelf als bij de posten.

Ministerie van Justitie

De wijze waarop de ambtelijke top sturing gaf aan de informatiebeveiliging was nog onvoldoende. Het ministerie had weliswaar informatiebeveiligingsbeleid geformuleerd en belangrijke verantwoordelijkheden vastgelegd maar dit leidde tot nog toe slechts in beperkte mate tot het uitvoeren van risico-afwegingen en het opstellen van beveiligings- en calamiteitenplannen.

Positief is wel dat het ministerie extra zorg besteedde aan de informatiesystemen die het ministerie van cruciaal belang achtte (de «categorie-1» systemen).

Het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden in opzet ten dele aan de norm. De Rekenkamer achtte een verdere aanscherping van het beleid vooral wenselijk bij het aandachtsgebied «toegang tot en gebruik van gegevens» en ook bij de aandachtsgebieden «systeemontwikkeling en -onderhoud», «personele maatregelen» en «toetsbaarheid fysieke beveiliging». Een belangrijke omissie in het beleid vormde het ontbreken van toezicht op naleving van de Wet persoonsregistraties. Hierdoor was bij het ministerie op centraal niveau niet bekend of voor alle reglementsplichtige systemen een privacyreglement was opgesteld.

Het centrale niveau bleek slechts beperkt te worden geïnformeerd over de feitelijke beveiligingssituatie binnen het ministerie. De accountantsdienst speelde een belangrijke rol bij het verschaffen van inzicht in de beveiligingssituatie. Deze dienst beperkte zich echter voornamelijk tot systemen die van belang waren voor de financiële verantwoording. De controle van informatiebeveiliging in brede zin was formeel niet opgedragen.

Samenvattend was de Rekenkamer van oordeel dat de algehele beheersing van de informatiebeveiliging binnen het ministerie nog onvoldoende was. Er was overigens in vergelijking met het onderzoek uit 1988 wel enige vooruitgang geboekt. Dit betrof met name de ontwikkeling

van centraal informatiebeveiligingsbeleid. De verdere concretisering van dit beleid en het toezicht op naleving ervan had echter in onvoldoende mate vorm gekregen.

De minister deelde mee dat de beveiliging van gegevens in geautomatiseerde systemen sinds ruim een jaar hoge prioriteit had. Zo werd gewerkt aan een nieuw concept voor het informatiebeveiligingsbeleid. Dit zou in juni 1995 worden vastgesteld, waarna met de invoering ervan kon worden begonnen.

De minister berichtte verder dat enkele eigen onderzoeken in samenwerking met de Binnenlandse Veiligheidsdienst hadden geleid tot een plan van aanpak dat inmiddels werd uitgevoerd. Incidenten in het arrondissement Amsterdam hadden geleid tot een gestructureerde aanpak van de (informatie)beveiligingsproblematiek bij de arrondissementen, waarover de minister medio 1995 aan de Tweede Kamer zou rapporteren.

Ministerie van Binnenlandse Zaken

De ambtelijke top van het ministerie gaf nog onvoldoende sturing aan de informatiebeveiliging. Er was vanaf 1990 weliswaar informatiebeveiligingsbeleid ontwikkeld en er waren verantwoordelijkheden vastgelegd maar de invoering van dit beleid was achtergebleven. Functionarissen die volgens het beleid een belangrijke taak dienden te vervullen bij de totstandkoming en toetsing van informatiebeveiliging waren bijvoorbeeld nooit aangesteld. Voorts vormden het grotendeels ontbreken van beveiligings- en calamiteitenplannen en de voorgeschreven decentrale risico-afwegingen een belangrijke tekortkoming.

Wel had het ministerie recentelijk activiteiten ontplooid om te komen tot het vaststellen van een basisniveau voor de beveiliging.

Het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden in opzet in belangrijke mate aan de normen. Een ernstige tekortkoming evenwel was het ontbreken van beleid om te komen tot privacyreglementen voor alle reglementsplichtige systemen in het kader van de Wet persoonsregistraties. Hierdoor bestond binnen het ministerie onvoldoende inzicht in hoeverre aan deze reglementsplicht werd voldaan. Voorts was nog nadere aandacht nodig voor autorisatieprocedures, het ontbreken van richtlijnen ten aanzien van screening van automatiseringspersoneel en verouderde voorschriften ten aanzien van fysieke beveiliging.

De wijze waarop binnen het ministerie verantwoording werd afgelegd over de beveiligingssituatie was duidelijk verbeterd en voldeed thans in belangrijke mate aan de norm. Ten aanzien van de onafhankelijke controle achtte de Rekenkamer het van belang dat duidelijkheid werd geschapen inzake de rolverdeling tussen de onderafdeling Organisatie en Informatievoorziening en de accountantsdienst.

Samenvattend was de Rekenkamer van oordeel dat de wijze waarop het ministerie van Binnenlandse zaken de informatiebeveiliging bij het eigen ministerie beheerste nog van onvoldoende niveau was. Weliswaar waren er verbeteringen zichtbaar in vergelijking met het onderzoek uit 1988, maar het informatiebeveiligingsbeleid was nog nauwelijks vertaald in een concrete en planmatige aanpak om te komen tot een voldoende niveau van informatiebeveiliging. De verbetering van de informatiebeveiliging bij de rijksdienst als geheel zou er in de ogen van de Rekenkamer mee gediend zijn indien het coördinerend ministerie zelf meer het goede voorbeeld gaf.

De recente activiteiten om te komen tot het vaststellen van een basisniveau voor de beveiliging zag de Rekenkamer overigens als een belangrijke positieve ontwikkeling.

De minister achtte het geschetste beeld van de feitelijke beveiligingssituatie op het departement weinig herkenbaar. De Rekenkamer geeft een oordeel over het gehele ministerie terwijl volgens de minister uitsluitend is gecommuniceerd over het kerndepartement. Daarnaast merkte hij op dat het belang van de basisvoorzieningen voor de informatiebeveiliging te weinig tot uiting komt in het rapport van de Rekenkamer. Op het kerndepartement is namelijk geen sprake van grote gegevensverwerkende systemen, zoals op de buitendiensten. Algemene generieke maatregelen zijn daarom voldoende om weerstand te bieden aan bedreigingen. Aansluitend op het basisniveau kunnen snel aanvullende informatiebeveiligingsplannen worden gemaakt voor de departementsonderdelen.

De minister deelde verder mee dat ten aanzien van de screening van eigen automatiseringspersoneel onlangs richtlijnen voor het kerndepartement zijn vastgesteld. Bovendien wordt gewerkt aan het opstellen van een centraal overzicht van reglementsplichtige registraties en privacyreglementen.

Ook gaf de minister uitgebreid aan welke rolverdeling bestaat tussen de directie Organisatie en Informatievoorziening en de accountantsdienst.

Tot slot berichtte de minister dat de Beveiligingsambtenaar van het departement, conform het VIR, een meerjaren-controlestrategie zal opzetten en deze jaarlijks zal actualiseren voor alle drie onderdelen van het BiZa-beveiligingsbeleid (fysieke beveiliging, informatiebeveiliging en integriteit/screening).

De Rekenkamer wijst erop dat niet alleen het kerndepartement maar ook de buitendiensten in het onderzoek betrokken zijn. Daarbij is onder meer geconstateerd dat het departementale beleid voor de informatiebeveiliging nog niet geconcretiseerd was in beveiligingsplannen van de buitendiensten.

De Rekenkamer erkent dat generieke maatregelen in de basisvoorzieningen een belangrijke bijdrage kunnen leveren aan de informatiebeveiliging. Dit was echter slechts een eerste stap op de goede weg en het ministerie was hiermee ten tijde van het onderzoek nog mee bezig.

De Rekenkamer acht de nu ter hand genomen en aangekondigde activiteiten goede ontwikkelingen op weg naar een verbeterde beheersing van de informatiebeveiliging.

Ministerie van Onderwijs, Cultuur en Wetenschappen

Het Ministerie van Onderwijs, Cultuur en Wetenschappen gaf onvoldoende sturing aan de informatiebeveiliging. Een belangrijke tekortkoming was het ontbreken van een vastgesteld beleid voor de informatiebeveiliging. Voorts was er nog onvoldoende aandacht besteed aan het uitvoeren van risico-afwegingen. Zo had bijvoorbeeld slechts een minderheid van de directies de resultaten van een risico-analyse tergugemeld aan het centrale niveau. Er was ook onvoldoende aandacht voor de ontwikkeling van plannen voor de continuïteit van de bedrijfsprocessen bij een eventuele verstoring van de gegevensverwerking.

Het centraal beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden slechts gedeeltelijk aan de normen. De gegevensverwerking en het beheer van informatiesystemen was grotendeels uitbesteed aan RCC. De Rekenkamer heeft de contracten die met deze organisatie gesloten zijn niet beoordeeld. Wel is geconstateerd dat het eigen beleidskader van het ministerie belangrijke hiaten vertoonde. Zo waren er tekortkomingen bij systeemontwikkeling en -onderhoud. Ook ontbraken algemene richtlijnen voor toegang tot en gebruik van gegevens. In de praktijk waren er verschillende maatregelen getroffen, maar er was geen algemeen beleidskader hiervoor vastgesteld.

De maatregelen voor de fysieke beveiliging waren slechts gedeeltelijk op expliciete risico-afwegingen gebaseerd.

Een sterk punt was de grote zorg die aan de privacyreglementen werd besteed.

Het toezicht dat het ministerie op de informatiebeveiliging hield was in grote lijnen toereikend. Ten tijde van het onderzoek was het ministerie bezig de onafhankelijke controle op het feitelijk bereikte niveau van beveiliging zich ook uit te laten strekken tot de informatiesystemen die geen relatie met de financiële verantwoording hebben. Met ingang van 1 januari 1994 waren de directies verplicht het beveiligingsstelsel bij hun directie elke drie jaar te laten onderzoeken door de accountantsdienst.

Samenvattend was de Rekenkamer van oordeel dat er bij het Ministerie van Onderwijs, Cultuur en Wetenschappen in vergelijking met het onderzoek uit 1988 duidelijk verbeteringen tot stand waren gebracht. Verdere verbeteringen waren echter nog steeds noodzakelijk en er zou nog een belangrijke inspanning vereist zijn om de beheersing van de informatiebeveiliging op een voldoende niveau te brengen.

De Rekenkamer beval aan met hoge prioriteit een beleid voor de informatiebeveiliging vast te stellen en daarbij vooral aandacht te schenken aan de uitgangspunten die zouden gelden bij het bepalen van beveiligingsmaatregelen. Voorts verdiende het aandacht erop toe te zien dat de controle van de informatiebeveiliging in brede zin door de accountantsdienst bij alle directies ook daadwerkelijk plaatsvindt.

De minister antwoordde dat het ministerie de afgelopen jaren hard had gewerkt aan de verbetering van de informatiebeveiliging. Hij was het er mee eens dat er verdere verbeteringen noodzakelijk waren en gaf aan dat daar al geruime tijd hard aan werd gewerkt.

Het onderzoek van de Rekenkamer legde sterk de nadruk op de wijze waarop de centrale leiding greep houdt op de informatiebeveiliging, terwijl de minister graag had gezien dat het onderzoek meer op de concrete veiligheidssituatie zou zijn gericht. Hij was voorts van mening dat het overzicht van conclusies per ministerie slechts de door de Rekenkamer gekozen formele en procedurele benadering weergaf en daardoor makkelijk onjuist kon worden geïnterpreteerd.

De minister gaf aan dat het ministerie de lijn heeft gevolgd van het aanbrengen van concrete verbeteringen op de werkplek. De aanpak was het benadrukken van de decentrale verantwoordelijkheid, gecombineerd met voorlichting door middel van brochures, workshops, artikelen. Dit leidde tot het versterken van het beveiligingsbewustzijn.

De Coördinatiegroep Beveiliging had onder leiding van de loco secretaris generaal bij deze ontwikkelingen het voortouw genomen. De coördinatiegroep had een toetsende functie ten aanzien van de directies.

De minister meldde voorts dat het informatiebeveiligingsbeleid binnenkort zou worden vastgesteld zodat de verschillende maatregelen die in de praktijk waren genomen hun inbedding kregen in een formeel vastgesteld beleidskader.

Voorts gaf de minister aan dat planmatig werd gewerkt aan de uitvoering van het Voorschrift Informatiebeveiliging Rijksdienst. Zo werd bij de hoofddirectie Centrale Financiën Instellingen en bij de Inspectie voor het onderwijs sinds medio 1994 gewerkt aan een beveiligingsplan. Hiermee werd eveneens tegemoet gekomen aan de door de Rekenkamer geconstateerde knelpunten ten aanzien van risico-afwegingen en plannen voor de continuïteit van de bedrijfsvoering.

In de ogen van de Rekenkamer is een overkoepelend beleidskader van belang voor het lijnmanagement om vast te stellen of het geheel van getroffen maatregelen op de werkplek toereikend en doelmatig is. Voorts hecht de Rekenkamer groot belang aan een goed instrumentarium voor de beheersing van de informatiebeveiliging als fundament voor een goede informatiebeveiliging, ook op langere termijn. Geconstateerd is dat

dit instrumentarium bij het Ministerie van Onderwijs, Cultuur en Wetenschappen nog tekortkomingen vertoont, vooral waar het gaat om het element van sturing.

Ministerie van Financiën

De Belastingdienst komt afzonderlijk aan de orde.

Het Ministerie van Financiën gaf nog onvoldoende sturing aan de informatiebeveiliging. Het ministerie beschikte wel over een helder beleid voor informatiebeveiliging maar dit had nog onvoldoende doorwerking gekregen naar de directies. Zo waren de beveiligingsplannen op directieniveau, die sinds 1990 volgens het beleid waren voorgeschreven, nooit tot stand gekomen. Voorts dateerde het calamiteitenplan voor het rekencentrum van het ministerie uit 1987 en was het verouderd.

Het centrale beleid en algemene richtlijnen voor beveiligingsmaatregelen voldeden goeddeels aan de normen. Bij de beoordeling hiervan is het concept-beveiligingsstatuut mee gewogen. Het centrale beleid vormde een goed uitgangspunt voor de informatiebeveiliging. Slechts op een aantal punten verdiende dit beleid enige aanscherping. Het gaat hierbij met name om de richtlijnen voor beveiligingsaspecten in het traject van systeemontwikkeling en de richtlijnen voor screening van extern personeel.

De Rekenkamer achtte het toezicht op naleving van het beveiligingsbeleid in opzet toereikend, de controle op informatiebeveiliging in brede zin was echter formeel nog niet opgedragen.

Het beleidsvoornemen om het lijnmanagement te verplichten onderzoeken te laten uitvoeren op de eigen systemen zal in de toekomst een belangrijke positieve bijdrage kunnen leveren aan het niveau van informatiebeveiliging. Er was echter nog een belangrijke inspanning nodig om deze situatie te realiseren.

Samenvattend was de Rekenkamer van oordeel dat het Ministerie van Financiën de informatiebeveiliging nog onvoldoende beheerste. De situatie was wel verbeterd in vergelijking met 1988. Het ministerie had de afgelopen jaren veel inspanningen verricht, wat heeft geresulteerd in centraal beleid en richtlijnen.

De Rekenkamer beval aan het concept-beveiligingsstatuut op korte termijn vast te stellen en hoge prioriteit te geven aan de nadere concretisering ervan binnen de directies.

De minister deelde mee dat hij de aanbeveling van de Rekenkamer zou overnemen. Het concept-beveiligingsstatuut zou op korte termijn worden vastgesteld, waarna een begin kon worden gemaakt met de nadere uitwerking en invoering ervan. In dit beleidsdocument zijn de richtlijnen voor screening van extern personeel inmiddels bijgesteld. De richtlijnen ten aanzien van de systeemontwikkeling zullen in een volgende versie van het statuut worden geactualiseerd.

Belastingdienst

De wijze waarop de Belastingdienst sturing gaf aan de informatiebeveiliging was in hoofdlijnen toereikend. Voor het opstellen van risico-afwegingen en de ontwikkeling van decentrale beveiligings- en calamiteitenplannen dienden evenwel nog nadere inspanningen te worden verricht. Het uitvoeren van risico-analyses in enigerlei vorm was noodzakelijk om tot een sluitend stelsel van beveiligingsmaatregelen te kunnen komen. In dit verband wees de Rekenkamer op haar onderzoek in 1994 naar de beveiliging van het Intra Communautair Transactiesysteem (ICT). De Rekenkamer constateerde in dat onderzoek dat voor dit

belangrijke systeem geen risico-analyse was gemaakt (Tweede Kamer, vergaderjaar 1994–1995, 24 045, nr. 2, blz. 58–61). Ze onderkende zwakke punten in de beveiliging van het systeem en kwam tot de conclusie dat de beveiliging onvoldoende passend was.

Het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden goeddeels aan de normen. Toch was nog enige aanscherping gewenst, vooral bij de richtlijnen voor de beheersing van het wijzigen van informatiesystemen.

Het toezicht op de informatiebeveiliging bij de Belastingdienst was eveneens toereikend. De controle op informatiebeveiliging in brede zin was formeel nog niet opgedragen. De accountantsdienst voerde deze taak feitelijk wel uit. Daarnaast achtte de Rekenkamer met name de rapportages van de directies over de feitelijke beveiligingssituatie van belang. Tijdens het onderzoek werd echter geconstateerd dat nog niet alle directies een dergelijke rapportage aan het concernniveau ter beschikking stelden.

Samenvattend was de Rekenkamer van oordeel dat de beheersing van de informatiebeveiliging bij de Belastingdienst in opzet toereikend was. De situatie was verbeterd in vergelijking met 1988. De Belastingdienst had de afgelopen jaren veel inspanningen verricht om het beveiligingsniveau op een hoger peil te brengen. Dit heeft geresulteerd in beleid voor de informatiebeveiliging en in een instrumentarium voor het ontwikkelen van risico-afwegingen, beveiligings- en calamiteitenplannen.

De nadere uitwerking van deze plannen vereiste evenwel nog belangrijke inspanningen. De tekortkomingen die de beveiliging van het ICT vertoonde illustreren dat een goede opzet niet zonder meer tot een adequate beveiliging in de gehele organisatie leidt.

De Rekenkamer beval aan om hoge prioriteit te blijven geven aan de voortgang van de in gang gezette activiteiten voor de verbetering van de informatiebeveiliging en de verantwoording hierover door de directies.

De staatssecretaris was met de Rekenkamer van oordeel dat aandacht nodig bleef om een in opzet en werking adequaat stelsel van maatregelen voor de informatiebeveiliging te realiseren en te handhaven. Hij deelde mee dat bij de Belastingdienst gewerkt werd aan een uitbouw van de methode voor risico-analyse, aansluitend bij het VIR. Voorts werd meegedeeld dat per ultimo 1994 het merendeel van de eenheden van de Belastingdienst beschikte over beveiligings- en calamiteitenplannen. In de eerste helft van 1995 zouden de resterende activiteiten op dit gebied worden afgerond.

Ministerie van Defensie

De wijze waarop de ambtelijke top sturing gaf aan de informatiebeveiliging voldeed in belangrijke mate aan de norm. Wel was nog een nadere inspanning gewenst op het gebied van risico-afwegingen. Het vigerende beleid voor informatiebeveiliging dateerde uit 1984 en was op onderdelen verouderd. Daarom achtte de Rekenkamer het van belang dat het reeds in ontwikkeling zijnde en deels vastgestelde Integraal Defensie Beveiligingsbeleid met prioriteit werd afgerond en ingevoerd.

Het centrale beleid en algemene richtlijnen voor beveiligingsmaatregelen voldeden nagenoeg aan de normen. De Rekenkamer achtte het gewenst om tot een eenduidige registratie van privacyreglementen te komen.

Bij het toezicht op de beveiligingssituatie binnen het ministerie werd met name gesteund op de onafhankelijke controle door de accountantsdienst. Deze controle voldeed volledig aan de norm. De wijze waarop «in de lijn» verantwoording werd afgelegd over de beveiligingssituatie diende te worden verbeterd. Deze verantwoordingsprocessen vertoonden nog

duidelijke tekortkomingen. Zo werd op centraal niveau niet nagegaan of de krijgsmachtdelen voldoende inzicht hadden in de eigen beveiligingssituatie. Voorts was de wijze waarop het lijnmanagement dient te rapporteren over de uitvoering van het beveiligingsbeleid in het beleid nog niet uitgewerkt.

Samenvattend was de Rekenkamer van oordeel dat het ministerie van Defensie in belangrijke mate voorwaarden heeft geschapen om te komen tot een adequaat beveiligingsniveau. Op dit punt is de situatie in vergelijking met 1988 ongeveer gelijk gebleven. Wat het maken van risico-afwegingen betreft zijn net als in 1988, tekortkomingen geconstateerd. De Rekenkamer beval aan om erop toe te zien dat de krijgsmachtdelen daadwerkelijk risico-afwegingen maken. Daarnaast verdiende het aanbeveling de wijze waarop verantwoordingsinformatie over de feitelijke beveiligingssituatie aan de hogere echelons wordt verstrekt te verbeteren. Tot slot beval de Rekenkamer aan het Integraal Defensie Beveiligingsbeleid met prioriteit vast te stellen en in te voeren.

De minister deelde mee dat hij kon instemmen met de conclusies van de Rekenkamer. Momenteel wordt op het departement de nodige aandacht besteed aan het uitvoeren van de aanbevelingen.

Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer

De wijze waarop het ministerie sturing gaf aan de informatiebeveiliging was nog onvoldoende. Het ontbreken van een departementaal beleid voor informatiebeveiliging was hier mede debet aan. Wel had het ministerie recentelijk beleidsuitgangspunten voor informatiebeveiliging ontwikkeld en een plan van aanpak om te komen tot een statuut voor informatiebeveiliging. Ook waren er ontwikkelingen gaande om te komen tot een basisniveau van beveiliging voor het kernministerie.

Het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden slechts in geringe mate aan de normen. Het beleid verschafte nauwelijks of geen duidelijkheid over informatiebeveiliging in de aandachtsgebieden «systeemontwikkeling en -onderhoud», «toegang tot en het gebruik van gegevens», «personele maatregelen» en «toetsbaarheid van de fysieke maatregelen».

Het toezicht op de informatiebeveiliging binnen het ministerie had nog onvoldoende gestalte gekregen. Met name de onafhankelijke controle op de informatiebeveiliging in brede zin was nog nauwelijks van de grond gekomen. Tot 1994 heeft de accountantsdienst van het ministerie zich voornamelijk beperkt tot advisering en ondersteuning aangezien er binnen het ministerie nog weinig activiteiten op het gebied van informatiebeveiliging hadden plaatsgevonden. De accountantsdienst had zich overigens wel ten doel gesteld om in de toekomst toezicht uit te oefenen op naleving van het nog vast te stellen beveiligingsstatuut. Voorts waren er ontwikkelingen in gang gezet om de verantwoording «in de lijn» vorm te geven.

Samenvattend was de Rekenkamer van oordeel dat de beheersing van de informatiebeveiliging bij het Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer nog onvoldoende was. Met name op het gebied van beleid en algemene richtlijnen voor beveiligingsmaatregelen als ook op het terrein van de onafhankelijke controle diende het ministerie nog belangrijke inspanningen te verrichten. Sinds het vorige Rekenkameronderzoek uit 1988 waren er te weinig activiteiten in gang gezet om de informatiebeveiliging beter beheersbaar te maken. Recente ontwikkelingen zoals het formuleren van beleidsuitgangspunten, het opstellen van een plan van aanpak alsmede de inrichting van een basisniveau voor informatiebeveiliging werden door de Rekenkamer overigens wel

beschouwd als belangrijke stappen in de goede richting. De Rekenkamer beval daarom aan deze activiteiten met hoge prioriteit uit te voeren.

De minister deelde mee dat het beeld dat de Rekenkamer schetst van de beveiligingssituatie op het ministerie haars inziens geen recht doet aan de feitelijke situatie. Sinds de onderzoeksperiode zijn namel0ijk grote vorderingen gemaakt op het terrein van computerhuisvesting en privacybescherming. Zo is een begin gemaakt met het ontwikkelen van een informatiebeveiligingsbeleid op basis van het VIR. Voor de gemeenschappelijke technische infrastructuur (de netwerken met alle daaraan gekoppelde automatiseringsmiddelen) zijn op centraal niveau maatregelen geformuleerd en geëffectueerd. Aanvullend hierop moeten de lijnmanagers voor de informatiesystemen die onder hun verantwoordelijkheid vallen een eigen beleid ontwikkelen, waarbij op basis van risico-afwegingen specifieke maatregelen kunnen worden getroffen.
Voorts achtte de minister een genuanceerde aanpak bij het ministerie noodzakelijk in verband met de gevarieerde omgeving van de diverse onderdelen van het ministerie en wees zij op het belang van het kostenaspect.

De Rekenkamer acht het positief dat er sinds de onderzoeksperiode kennelijk verbeteringen zijn aangebracht.

Ministerie van Verkeer en Waterstaat

De wijze waarop de ambtelijke top sturing gaf aan de informatiebeveiliging was in opzet toereikend, gelet op de besturingsfilosofie van het ministerie. Deze filosofie legt een zware verantwoordelijkheid bij de dienstonderdelen. De Rekenkamer heeft via informatie op centraal niveau niet kunnen vaststellen of de dienstonderdelen voldoende invulling geven aan deze verantwoordelijkheid. Zo schreef het beleid voor de informatiebeveiliging voor dat elk departementsonderdeel een meerjarenuitvoeringsplan voor de beveiliging van gegevens in geautomatiseerde informatiesystemen opstelt, maar het centrale niveau kon onvoldoende inzicht verschaffen in de stand van zaken rond de ontwikkeling van decentrale beveiligings- en calamiteitenplannen en in de uitvoering van risico-afwegingen.
Het centrale beleid en de algemene richtlijnen voor de informatiebeveiliging voldeden goeddeels aan de normen. Een belangrijke tekortkoming was de onzekerheid of er privacyreglementen waren vastgesteld voor alle persoonsregistraties die daarvoor in aanmerking komen volgens de WPR. Voorts was op centraal niveau niet bekend of bij alle locaties voorschriften voor de fysieke beveiliging golden. Bovendien waren deze voorschriften niet altijd op een expliciete risico-afweging gebaseerd.
Het beleid gaf voorts nog geen kaders voor de behandeling van beveiligingsaspecten in systeemdocumentatie, voor de voorkoming van mogelijke functievermenging bij het toekennen en controleren van autorisaties en voor de screening van extern automatiseringspersoneel.
Het toezicht was nog ontoereikend, zeker gezien de grote mate van verantwoordelijkheid die bij de dienstonderdelen was neergelegd. De verantwoordingsinstrumenten waren zwak ontwikkeld, waardoor het centrale niveau geen overzicht had over de naleving van het beveiligingsstatuut en over de feitelijke beveiligingssituatie. De controle van informatiebeveiliging in brede zin was formeel nog niet opgedragen. Door het ontoereikende toezicht kunnen hiaten ontstaan in de beveiliging bij onderdelen van het ministerie. Zo constateerde de Rekenkamer in een eerder onderzoek (Tweede Kamer, vergaderjaar 1993–1994, 23 555, nrs. 1–2) dat het KNMI nog niet voldeed aan de beveiligingseisen van het ministerie.
Samenvattend was de Rekenkamer van oordeel dat de beheersing van

de informatiebeveiliging bij het Ministerie van Verkeer en Waterstaat nog geen sluitend geheel vormde, hoewel de situatie in vergelijking met 1988 wel was verbeterd. De Rekenkamer beval met name aan het toezicht te versterken. Als eerste stap kon gedacht worden aan decentrale verantwoordingsrapportages van de diensten over de voortgang van de uitvoeringsplannen voor de beveiliging. Voorts achtte de Rekenkamer het van belang dat het centrale niveau zich een oordeel vormt over de toereikendheid van de beveiligingsen calamiteitenplannen en over de informatiebeveiliging bij het ministerie als geheel.

De minister stemde op hoofdlijnen in met de conclusies van de Rekenkamer. Zij zegde toe de zwak ontwikkelde verantwoordingsinstrumenten te versterken door periodieke en onafhankelijke beoordeling door de accountantsdienst van zowel het beleid als de beleidsimplementatie en de uitvoering. Een en ander is vastgelegd in het nieuwe beleid voor de informatiebeveiliging van maart 1995.

De minister stelde voorts dat de Rekenkamer algemene uitspraken had gedaan over informatiesystemen die qua omvang en complexiteit niet te vergelijken waren. Het ontbreken van kaders en voorschriften op onderdelen kon een bewuste keuze zijn. Zo leek het de minister niet zinvol om de richtlijnen voor de behandeling van beveiligingsaspecten in systeemdocumentatie verder te detailleren, gelet op de verschillen in aard en omvang van systemen. Ook achtte de minister het opstellen van uniforme kaders voor het voorkomen van mogelijke functievermenging bij het toekennen en controleren van autorisaties niet zinvol omdat de informatiesystemen grote verschillen vertoonden in omvang, complexiteit en vertrouwelijkheid van de gegevens.

Voorts lag de verantwoordelijkheid voor invulling van deze zaken veelal decentraal gelet op de decentrale besturingsfilosofie van het ministerie. Tot de verantwoordelijkheid van de integrale manager op decentraal niveau behoorde ook de zorg voor de fysieke beveiliging. Daarom werd op centraal niveau op dit gebied niets voorgeschreven.

Uit het antwoord bleek verder dat de minister inmiddels de zekerheid had dat alle volgens de WPR reglementsplichtige registraties waren aangemeld en dat screening van extern personeel werd uitgevoerd conform de geldende normen voor het intern personeel.

Tot slot zegde de minister toe dat de opmerkingen van de Rekenkamer hun weerslag zouden vinden in het beveiligingsbeleid.

De Rekenkamer is het met de minister eens dat het een bewuste keuze kan zijn om af te zien van kaders en voorschriften voor bepaalde systemen, afhankelijk van hun complexiteit en omvang. De Rekenkamer heeft echter niet kunnen vaststellen dat dergelijke keuzen inderdaad bewust gemaakt zijn.

Hoewel de Rekenkamer de keuze van de minister voor een beperkte mate van sturing van bovenaf respecteert, moet de minister volgens haar toezicht uitoefenen op de uitvoering van het beleid bij de dienstonderdelen. Zij ziet de aangekondigde onafhankelijke controle door de accountantsdienst als een belangrijke eerste stap.

Ministerie van Economische Zaken

Het Ministerie van Economische Zaken gaf nog onvoldoende sturing aan de informatiebeveiliging. Zo was er nog te weinig aandacht voor risico-afwegingen en was het beveiligingsbeleid, dat dateert uit 1990, onvoldoende nader uitgewerkt in calamiteiten- en beveiligingsplannen.

Het centrale beleid en algemene richtlijnen voor beveiligingsmaatregelen vertoonden bovendien nog belangrijke tekortkomingen. Het gaat hierbij met name om richtlijnen voor systeemontwikkeling en -onderhoud, richtlijnen ter voorkoming van ongewenste functie-

vermenging bij het toekennen van autorisaties en richtlijnen voor screening van automatiseringspersoneel.

De vereiste privacyreglementen waren nog steeds niet vastgesteld terwijl het ministerie reeds in 1987 heeft geïnventariseerd welke persoonsregistraties in het kader van de Wet persoonsregistraties reglementsplichtig waren. Voorts constateerde de Rekenkamer dat de maatregelen voor fysieke beveiliging veelal niet gebaseerd waren op een expliciete risico-afweging.

Het toezicht op de informatiebeveiliging was in hoofdlijnen toereikend, maar vertoonde toch enkele tekortkomingen. Zo was het centrale niveau niet in staat om aan de hand van documentatie aan te geven of de voorgeschreven decentrale risico-afwegingen werden uitgevoerd. Voorts had de controle van de accountantsdienst zich tot dan toe nog beperkt tot systemen die een relatie hebben met de financiële verantwoording en strekte deze controle zich dus niet uit tot de informatiebeveiliging in brede zin. De controle op informatiebeveiliging in brede zin was formeel nog niet opgedragen. De Rekenkamer achtte het daarom van belang dat het voornemen van het ministerie om in de toekomst de getroffen maatregelen op het gebied van informatiebeveiliging door een onafhankelijke instantie te laten toetsen op korte termijn gerealiseerd werd.

Samenvattend was de Rekenkamer van oordeel dat de beheersing van de informatiebeveiliging bij het Ministerie van Economische Zaken nog onvoldoende was. Er was in geringe mate vooruitgang geboekt in vergelijking met de situatie in 1988. Zo was er in 1990 weliswaar een departementaal beleid voor informatiebeveiliging tot stand gebracht maar dit beleid vertoonde nog een aantal lacunes en was bovendien onvoldoende uitgewerkt in calamiteiten- en beveiligingsplannen. De Rekenkamer beval aan de genoemde tekortkomingen weg te nemen en hoge prioriteit te geven aan de voorgenomen onafhankelijke toetsing van getroffen maatregelen op het gebied van informatiebeveiliging.

De minister deelde mee dat onlangs een start is gemaakt met de actualisering van het informatiebeveiligingsbeleid, waarbij het VIR als uitgangspunt dient. Over de algemene richtlijnen voor beveiligingsmaatregelen en het centrale beleid berichtte de minister dat mondelinge afspraken zijn gemaakt voor operationele maatregelen en dat conform deze maatregelen wordt gewerkt, maar dat die afspraken nog niet schriftelijk zijn vastgelegd. Hij zegde toe dit op korte termijn alsnog te doen. Ook deelde de minister mee dat hij opdracht heeft gegeven een checklist op te stellen, op basis waarvan verantwoordelijke functionarissen zelf controles op de informatiebeveiliging kunnen (laten) uitvoeren. Ook zal opdracht worden gegeven aan een externe organisatie om een onafhankelijke controle uit te voeren.

Ministerie van Landbouw, Natuurbeheer en Visserij

De sturing van de informatiebeveiliging door de ambtelijke top van het Ministerie van Landbouw, Natuurbeheer en Visserij was in opzet adequaat. Wel verdienden de actualisering van het beleid voor de informatiebeveiliging en de ontwikkeling van beveiligings- en calamiteitenplannen nog nadere aandacht.

Ook het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden goeddeels aan de normen. Een duidelijke tekortkoming was het ontbreken van recente risico-afwegingen voor de fysieke beveiliging. De Rekenkamer achtte het voorts van belang dat er duidelijkheid werd geschapen over de criteria om te bepalen welke personeelsleden met taken binnen de geautomatiseerde informatievoorziening in aanmerking komen voor een veiligheidsonderzoek. Tenslotte was nog aandacht gewenst voor richtlijnen die mogelijke

functievermenging tussen het toekennen en het controleren van autorisaties moeten voorkomen.

De wijze waarop het ministerie toezicht uitoefende op de informatiebeveiliging voldeed nagenoeg aan de normen. Een sterk punt was dat sinds kort jaarlijks verantwoording werd afgelegd over de voortgang van de projecten ter verbetering van de informatiebeveiliging.

Het voorafgaande heeft voornamelijk betrekking op de opzet van de instrumenten voor beheersing. Een goede opzet betekent niet automatisch dat de instrumenten ook goed worden ingezet. Dit blijkt onder meer uit het onderzoek naar de beveiliging van datacommunicatie bij het Ministerie van Landbouw, Natuurbeheer en Visserij (Tweede Kamer, vergaderjaar 1993–1994, 23 785, nrs. 1–2) dat de Rekenkamer in de periode september 1993 tot januari 1994 uitvoerde. De belangrijkste conclusie toen was dat het ministerie veel aandacht besteed had aan informatiebeveiliging en dat het normenstelsel van het ministerie in hoofdlijnen toereikend was. De daadwerkelijke uitvoering van het beleid was echter zowel op centraal niveau als bij de decentrale organisatie-eenheden nog niet voltooid. Dit laatste manifesteerde zich onder meer in het gemis aan risico-analyses en systeemclassificaties.

De minister liet de Rekenkamer in reactie op het toenmalige onderzoek weten dat de invoering van het normenstelsel in 1995 zou worden afgerond. Mede in het licht hiervan beval de Rekenkamer in het huidige onderzoek aan nadrukkelijk aandacht te (blijven) geven aan de invoering en het juiste gebruik van de instrumenten voor de beheersing van de informatiebeveiliging.

Samenvattend was de Rekenkamer van oordeel dat de beheersing van de informatiebeveiliging bij het Ministerie van Landbouw, Natuurbeheer en Visserij in hoofdlijnen toereikend was. Sinds het onderzoek uit 1988 was er duidelijke vooruitgang geboekt. Wel verdiende het aanbeveling met prioriteit een actueel beleid voor de informatiebeveiliging, uitwijkregelingen bij calamiteiten en beveiligingsrichtlijnen voor automatiseringspersoneel vast te stellen. Tenslotte verdiende het uitsluiten van functievermenging tussen toekennen en controleren van toegangsautorisaties nadere aandacht.

De minister deelde mee dat in het Jaarplan Informatiebeveiliging 1995 rekening zal worden gehouden met de conclusies en aanbevelingen van de Rekenkamer. Binnen het departement is bovendien sprake van actualisering van het beleid middels de nieuwe versie van het Algemeen Kader Informatiebeveiliging en het Handboek Systeem-Classificatie. Een risico-analyse voor de fysieke beveiliging zal impliciet worden meegenomen bij de implementatie van de Basisnormen voor Verwerkingsorganisaties. Daarnaast zal bij nieuwe huisvesting van rekencentra bij onderdelen van het departement binnen de Technische Richtlijnen voor Infrastructuur expliciet rekening worden gehouden met aspecten van fysieke beveiliging.

De minister deelde voorts mee dat hij de conclusie van de Rekenkamer dat richtlijnen voor de logische toegangsbeveiliging ontbreken, niet deelde. Volgens hem zijn deze voldoende opgenomen in de Modellen Administratieve Organisatie. De minister zegde toe erop toe te zien dat deze richtlijnen in voldoende mate worden nageleefd. Tot slot berichtte de minister dat nader onderzoek zal worden verricht naar de criteria om te bepalen welke personeelsleden met taken binnen de geautomatiseerde informatievoorziening in aanmerking komen voor een veiligheidsonderzoek. Waar het gaat om «vertrouwensfuncties» zal zo nodig aansluiting worden gezocht bij de recente handreiking van de minister van Binnenlandse Zaken «Integriteit sector Rijk: Organisatorische en Personele maatregelen».

De Rekenkamer acht het positief dat de Modellen Administratieve Organisatie maatregelen voorschrijven rond het toekennen van autorisaties. Zij mist echter nog een expliciete vastlegging bijvoorbeeld in het beveiligingsbeleid – van de uitgangspunten die aan deze maatregelen ten grondslag liggen. Een dergelijke vastlegging kan waarborgen dat de maatregelen bij alle onderdelen van het ministerie blijvend in de administratieve organisatie worden opgenomen.

Ministerie van Sociale Zaken en Werkgelegenheid

Het Ministerie van Sociale Zaken en Werkgelegenheid gaf onvoldoende sturing aan de informatiebeveiliging. Het ministerie maakte nauwelijks risico-afwegingen en beschikte noch over informatiebeveiligingsbeleid noch over beveiligingsen calamiteitenplannen.

Bovendien ontbraken centrale richtlijnen voor beveiligingsaspecten in het systeemontwikkelingstraject, voor toegang tot en het gebruik van gegevens en voor personele maatregelen.

Er was weliswaar geïnventariseerd voor welke persoonsregistraties privacyreglementen opgesteld moesten worden en er werden verschillende privacyreglementen aangetroffen, maar uit de registratie bij het ministerie kon niet worden afgeleid of alle reglementsplichtige systemen waren voorzien van een privacyreglement.

Ook het toezicht op de informatiebeveiliging was nog onvoldoende. Zo bestond er nog geen duidelijkheid over de wijze waarop de secretaris-generaal moest worden geïnformeerd over de hoofdlijnen van de beveiligingssituatie. Ook was het onduidelijk wie verantwoordelijk was voor het initiëren van onderzoeken. De controle van informatiebeveiliging in brede zin was formeel niet opgedragen.

Samenvattend was de Rekenkamer van oordeel dat het ministerie van Sociale Zaken en Werkgelegenheid de informatiebeveiliging volstrekt onvoldoende beheerste. In vergelijking met het vorige onderzoek uit 1988 had het ministerie op dit terrein nauwelijks enige vooruitgang geboekt.

Wel heeft de secretaris-generaal van het ministerie eind 1994 opdracht gegeven om het «Beveiligingsstatuut Informatievoorziening SZW» te ontwikkelen. De Rekenkamer achtte dit een belangrijk initiatief en beval aan om de ontwikkeling en invoering van dit statuut voortvarend ter hand te nemen.

De minister erkende dat er binnen het ministerie onvoldoende aandacht was geweest voor het formuleren van een departementaal informatiebeveiligingsbeleid. Hij meldde dat er in 1994 binnen zijn ministerie een herinrichtingsoperatie was uitgevoerd waarbij onder meer het technisch beheer van informatiesystemen en de verantwoordelijkheid daarvoor was neergelegd bij één directie.

Voorts antwoordde de minister dat de bestuursraad inmiddels een beleidsdocument had bekrachtigd waarmee een set van departementale beleidsen uitvoeringsrichtlijnen betreffende de beveiliging van informatie was vastgesteld. Aan de implementatie hiervan zou in de eerste helft van 1995 met voortvarendheid uitvoering worden gegeven, waarbij de door de Rekenkamer gehanteerde normen en het Voorschrift Informatiebeveiliging Rijksdienst als meetlat werden aangehouden.

Voorts gaf de minister aan dat op korte termijn een aanvang zou worden gemaakt met een bewustwordingstraject.

Tenslotte zegde de minister toe dat voor 1 juli 1995 de informatiesystemen met een hoog risiconiveau van beveiligingsplannen zouden worden voorzien en dat voor die datum ook de inventarisatie van privacyreglementen zou zijn geactualiseerd.

Ministerie van Volksgezondheid, Welzijn en Sport

Het Ministerie van Volksgezondheid, Welzijn en Sport gaf nog in onvoldoende mate sturing aan de informatiebeveiliging. De belangrijkste tekortkomingen waren het ontbreken van informatiebeveiligingsbeleid en het goeddeels ontbreken van calamiteitenplannen. Wel maakte het ministerie elke twee jaar een inventarisatie van risico's hetgeen als belangrijke basis voor een te ontwikkelen informatiebeveiligingsbeleid mag worden beschouwd. Voorts werkte het ministerie ten tijde van het onderzoek aan een basisniveau voor informatiebeveiliging.

Het centrale beleid en de algemene richtlijnen voor beveiligingsmaatregelen voldeden deels aan de norm. In het oog springende tekortkomingen waren het ontbreken van richtlijnen voor toegang tot en het gebruik van gegevens, voor personele maatregelen en voor toetsbaarheid van de fysieke beveiliging. Elementen hiervan waren weliswaar in decentrale (beveiligings)plannen aangetroffen maar er ontbrak een eenduidig beleid dat voor het gehele ministerie helderheid schept over de eisen die voor de informatiebeveiliging gelden.

Het ministerie oefende toereikend toezicht uit op de informatiebeveiliging. Het ministerie beschikte echter niet over een formele beschrijving van de feitelijke beveiligingssituatie. Ook was de controle van informatiebeveiliging in brede zin formeel niet opgedragen. Desondanks is tijdens het onderzoek geconstateerd dat de accountantsdienst deze controle wel tot haar taak rekende.

Samenvattend was de Rekenkamer van oordeel dat de beheersing van de informatiebeveiliging bij het ministerie van Volksgezondheid, Welzijn en Sport nog onvoldoende was ondanks verbeteringen in vergelijking met de situatie in 1988.

De Rekenkamer beval aan om een helder beleidskader te scheppen voor het gehele ministerie. Elementen zoals de tweejaarlijkse risico-afweging en het in ontwikkeling zijnde basisniveau voor informatiebeveiliging konden hierbij als basis dienen. Voorts werd aanbevolen om de nog ontbrekende calamiteitenplannen op korte termijn tot stand te laten komen.

De minister stemde op hoofdlijnen in met de bevindingen en conclusies van de Rekenkamer. Volgens de minister waren binnen het ministerie goede afspraken gemaakt voor de toegang tot en het gebruik van gegevens, met name voor risicovolle systemen. Zij zegde toe deze afspraken duidelijker te expliciteren en op te nemen in het centrale informatiebeveiligingsbeleid. Voorts was een begin gemaakt met de opstelling van een beleidskader Informatiebeveiliging voor het gehele ministerie, op basis van het VIR. Binnenkort zou er ook een calamiteitenplan beschikbaar komen.