Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1996–1997

25 290 Informatiebeveiliging Belastingdienst

Nr. 2 **RAPPORT**

INHOUD

SAMENVATTING

De Rekenkamer heeft als vervolg op haar onderzoek in 1991–1992 naar de informatiebeveiliging bij de Belastingdienst (Decemberverslag 1992) in augustus–september 1996 onderzocht of de destijds gedane toezeggingen van de staatssecretaris zijn nagekomen en of de informatiebeveiliging van de Belastingdienst sinds het vorige onderzoek was verbeterd.

Uit de concrete maatregelen die sedert 1992 zijn getroffen bleek duidelijk dat de informatiebeveiliging bij de eenheden de aandacht van de staatssecretaris heeft gehad. De Rekenkamer concludeerde dat de staatssecretaris zijn toezeggingen uit 1992 gestand heeft gedaan. De bestuurlijke aandacht voor de informatiebeveiliging heeft geleid tot een uitgebreid stelsel van voorschriften. De bestuurlijke beheersing en controle op de naleving van de voorschriften is naar haar mening echter nog niet voldoende effectief gebleken.

De Rekenkamer vindt dat bij de ontvlechting van de ondersteunende diensten en het faciliteitenbeheer zorg gedragen moet worden voor een eenduidige verdeling van verantwoordelijkheden voor de informatiebeveiliging. Daaromtrent bestaan thans zorgen.

De inbraakbeveiliging van gebouwen en de toegangscontrole vertoonden bij alle onderzochte eenheden gebreken. Verzoeken van deze eenheden om in het kader van renovatieprojecten de inbraakbeveiliging te verbeteren werden niet gehonoreerd.

Bij alle vijf eenheden lag niet-openbare informatie open en bloot in de niet afgesloten werkkamers, waardoor deze informatie direct toegankelijk is voor onbevoegden. De Belastingdienst loopt daarnaast onnodige risico's bij het verspreiden van papieren documenten die ook in elektronische vorm worden aangeboden aan de eenheden.

De Belastingdienst heeft de beveiliging van de toegang tot geautomatiseerde systemen in opzet goed geregeld. Bij de vijf onderzochte eenheden bleek echter dat de voortgang van het primaire proces belangrijker wordt geacht dan het voldoen aan de beveiligingseisen. Functiescheidingen worden ten behoeve van het produktieproces vaak bewust niet aangebracht, terwijl er onvoldoende compenserende interne controles worden uitgevoerd. Op veel plaatsen wordt slordig met de persoonlijke wachtwoorden omgegaan en de leesrechten van privacy-gevoelige informatie worden bij indiensttreding automatisch toegekend. De voorgeschreven back up-procedures bleken niet altijd te worden gevolgd, waardoor het risico aanwezig is dat bij calamiteiten belangrijke informatie verloren gaat.

Het feit dat én de inbraakbeveiliging, én de toegangscontrole van de gebouwen én de toegangsbeveiliging van de geautomatiseerde systemen gebreken vertonen leidt tot de conclusie dat de informatiebeveiliging bij de vijf onderzochte eenheden ernstige tekortkomingen vertoont.

Ontdekte en bestrafte inbreuken op de beveiligingsvoorschriften hebben in de praktijk niet geleid tot afdoende aanpassing van de voorschriften en werkwijzen.

De Rekenkamer komt tot de eindconclusie dat de staatssecretaris veel aandacht heeft besteed aan de informatiebeveiliging bij de Belastingdienst. Hij is er echter nog niet in geslaagd de informatiebeveiliging bij de eenheden op een aanvaardbaar peil te brengen.

Zij beveelt daarom aan om op korte termijn:

- de informatie bij de Centrale facilitaire dienst over de beveiliging van de gebouwen te actualiseren om vervolgens op basis van een accurate prioriteitstelling voortvarend achterstanden op dit gebied weg te werken; dit aspect zou in de toekomst betrokken moeten worden in de onderzoeken van de Interne Accountantsdienst Belastingen;

• de organisatie voor informatiebeveiliging en interne controle op de eenheden en de directies (de FIB-organisatie) te versterken, om daarmee af te dwingen dat beveiligingsvoorschriften daadwerkelijk worden nageleefd; gedacht kan worden aan frequent overleg binnen de FIB-organisatie, het uitvoeren van onderzoek door de directies naar de naleving van de voorschriften en het aanspreken van de hoofden van de eenheden op hun verantwoordelijkheden op dit gebied; daarbij moeten zodanige investeringen worden gedaan in de programmatuur, dat de voorschriften gemakkelijker dan nu kunnen worden nageleefd;
• de aandacht voor de betrouwbaarheid van de gegevensverwerking en voor preventie van inbreuken op de ambtelijke integriteit te versterken door extra interne controles op gevoelige functies, door verdere ontwikkeling van het sanctiebeleid bij inbreuken op de beveiligingsvoorschriften en door het treffen van Belastingdienstbrede maatregelen naar aanleiding van dit soort inbreuken, om herhaling te voorkomen.

De staatssecretaris schreef in zijn reactie op de rapportage van de Rekenkamer dat hij de slotconclusie van de Rekenkamer niet deelde. Hij was van mening dat de huidige beveiligingsrisico's, gelet op de normen en realisering daarvan, aanvaardbaar waren. Niettemin nam hij de meeste aanbevelingen van de Rekenkamer over en deed hij een aantal concrete toezeggingen om de situatie te verbeteren.

De Rekenkamer meent dat de toezeggingen van de staatssecretaris zullen bijdragen aan de noodzakelijke verbetering van de naleving van de voorschriften. Zij zal de ontwikkelingen rondom de betrouwbare en vertrouwelijke gegevensverwerking bij de Belastingdienst met aandacht blijven volgen.

1 INLEIDING

In 1991–1992 onderzocht de Algemene Rekenkamer de informatiebeveiliging bij PC's en PC-netwerken van de Belastingdienst (Decemberverslag 1992, Tweede Kamer, vergaderjaar 1992–1993, 22 960, nrs. 1–2). Uit dat onderzoek bleek onder andere dat:

- de door de Belastingdienst centraal verstrekte regelgeving en checklists op het gebied van informatiebeveiliging onvoldoende in praktijk werd gebracht;
- de standaard beveiligingsmogelijkheden van de besturings- en netwerkprogrammatuur niet volledig werden benut;
- de toegang tot bestanden ruimer was dan op grond van de opgedragen werkzaamheden en bestaande functiescheidingen wenselijk was;
- de lokale functionarissen informatiebeveiliging een kennisachterstand hadden ten opzichte van de applicatie- en systeembeheerders die zij geacht werden te controleren.

De staatssecretaris van Financiën zegde naar aanleiding van deze conclusies onder meer toe dat:

- er een automatiseringsinfrastructuur zou komen die het gewenste niveau van beveiliging zou gaan ondersteunen;
- de eenheden een methode voor risico-analyse, een model-calamiteitenplan en een lokaal handboek risicobeheersing zouden krijgen;
- het opleidingsniveau van beveiligingsmedewerkers verbeterd zou worden;
- de Interne Accountantsdienst Belastingen (IAB) meer aandacht zou gaan geven aan controles op beveiliging automatisering.

Sinds het onderzoek in 1991–1992 is de automatisering van de ondersteunende en de primaire werkprocessen bij de eenheden verder toegenomen, en dus ook het belang van een deugdelijke informatiebeveiliging. De systemen op de eenheden die in 1992 nog voornamelijk registratief van aard waren spelen een steeds grotere rol in het primaire proces. Met de introductie van het Inkomsten Belasting Systeem (IBS) is een eerste stap gezet om dit proces op de eenheden volledig te automatiseren. Ook de centrale systemen worden tegenwoordig rechtstreeks vanuit de eenheden gemuteerd.

Dit alles was voor de Rekenkamer aanleiding om een vervolgonderzoek naar de beveiliging in te stellen, om te zien of de toezeggingen van de staatssecretaris zijn nagekomen en of de informatiebeveiliging van de Belastingdienst sinds het vorige onderzoek was verbeterd. Daarbij richtte zij zich met name op de naleving van de beveiligingsvoorschriften en op het gebruik van fysieke en organisatorische maatregelen en voorzieningen in hard- en software om de betrouwbaarheid en de vertrouwelijkheid van de gegevens en de continuïteit van de gegevensverwerkende processen te beschermen. Daarbij is overigens ook aandacht geschonken aan een aantal aspecten van informatiebeveiliging die in het onderzoek uit 1991–1992 niet voorkwamen, zoals de toegang tot de gebouwen en bescherming van papieren informatie. Een goede informatiebeveiliging is mede van belang om het risico op inbreuken op de ambtelijke integriteit te verkleinen. De aandacht die de Belastingdienst geeft aan de ambtelijke integriteit is onderzocht aan de hand van klachten over en bewuste inbreuken op beveiligingsmaatregelen bij de eenheden.

Om een beeld te krijgen van de informatiebeveiliging in de praktijk is onderzoek uitgevoerd bij drie eenheden Particulieren en bij twee eenheden Ondernemingen. De resultaten van dit in omvang beperkte

onderzoek moeten worden geplaatst tegen de bevindingen van de representatieve onderzoeken van de IAB over voorgaande jaren.

De Rekenkamer zond haar bevindingen in januari 1997 aan de staatssecretaris van Financiën, met het verzoek hierop commentaar te leveren. Deze reageerde in februari 1997. Zijn reactie is op hoofdlijnen verwerkt in hoofdstuk 5.

In haar Rechtmatigheidsonderzoek 1995 (Tweede Kamer, vergaderjaar 1995–1996, 24 830, nrs. 1–2) rapporteerde de Rekenkamer over haar onderzoek naar de betrouwbaarheid van de centrale gegevensverwerking bij het Automatiseringscentrum van de Belastingdienst (BAC). Zij constateerde in dat onderzoek dat een aantal reeds jaren aanwezige ernstige tekortkomingen nog niet was opgelost. Dit betrof ondermeer de inrichting en het beheer van de toegang tot de geautomatiseerde systemen. De staatssecretaris van Financiën zegde naar aanleiding van dat onderzoek toe dat hij in 1996 hoge prioriteit zou geven aan het oplossen van de tekortkomingen. In het onderhavige onderzoek staat de situatie in 1996 bij de eenheden van de Belastingdienst centraal, waaronder ook de toegang tot geautomatiseerde systemen.

2 VERBETERINGEN OP BESTUURLIJK NIVEAU

2.1 Activiteiten sinds 1991

De directie Planning Financiën en Control (PFC) van het ministerie is verantwoordelijk voor de formulering van meerjarige doelstellingen en de toetsing van de bedrijfsresultaten daaraan. Sinds 1991 is er volgens de directie PFC door de Belastingdienst circa f 20 à 25 miljoen per jaar uitgeven voor informatiebeveiligingsactiviteiten. Dit bedrag is gebaseerd op een globale inventarisatie door PFC. De grootste component van de jaarlijkse uitgaven wordt gevormd door personeelskosten voor de beveiligingsorganisatie en projecten. In hoofdzaak zijn hiermee de volgende activiteiten bekostigd:

- er is een uitgebreide voorlichtingscampagne georganiseerd om het beveiligingsbewustzijn van de belastingambtenaren te verhogen;
- de richtlijnen voor risicobeheersing zijn verder ontwikkeld. Die kunnen in samenhang met het door PFC ontwikkelde Systeem Beveiligings Onderzoek (SBO) door de eenheid gebruikt worden om inzicht te verkrijgen in de lokale beveiligingssituatie;
- voor de centrale apparatuur op de eenheden zijn bouwkundige aanpassingen gerealiseerd;
- er wordt algemeen gewerkt met beveiligingsprogrammatuur zoals Safeguard, virusdetectieprogrammatuur en schermbeveiligingssoftware;
- er wordt alleen nog maar met door het BAC goedgekeurde programmatuur gewerkt;
- vrijwel alle diskettestations in de netwerkapparatuur zijn verwijderd;
- er is een 10-punten programma opgestart, waarmee wordt beoogd concrete verbeteringen aan te brengen in de 10 belangrijkste tekortkomingen in de informatiebeveiliging. De eenheden moeten over de voortgang hierin rapporteren;
- in 1993 en 1994 heeft het Support en expertiseteam informatiebeveiliging (STIB) eenheden ondersteuning verleend bij het ontwerp en de implementatie van een modelcalamiteitenplan en het invoeren van een gestandaardiseerde logische toegangsbeveiliging.

Een nieuw platform voor de technische infrastructuur op de eenheden is voor het grootste deel organisatorisch in 1996 ingevoerd. Dit platform zorgt voor een scheiding tussen het beheer van de automatiseringsmiddelen (faciliteitenbeheer, dit betreft apparatuur en besturingsprogrammatuur) en het beheer van de toepassingen (toepassingsbeheer, dit betreft alle programmatuur met uitzondering van besturingsprogrammatuur. Het faciliteitenbeheer zit weliswaar fysiek nog bij de eenheid, maar valt hiërarchisch en organisatorisch onder het BAC. Het toepassingsbeheer blijft hiërarchisch onder het hoofd van de eenheid vallen.

2.2 Organisatie uitvoering beveiligingstaak

Binnen de Belastingdienst zijn op drie niveaus (departementaal niveau, per doelgroepdirectie en per lokale organisatorische eenheid) staffuncties informatiebeveiliging ingesteld. De functionaris informatiebeveiliging bij de eenheid (FIB-3) heeft een adviserende rol op het terrein van de informatiebeveiliging, de interne controle en het informatiemanagement.

Er vindt geen apart gestructureerd overleg plaats tussen de functionarissen informatiebeveiliging van de directies (FIB-2) en de FIB-3's van de eenheden. De informatieverstrekking en aansturing vindt plaats via overleg met het hoofd van dienst en de controller. Informatiebeveiliging is in dat overleg geen apart onderwerp maar wordt zoveel mogelijk in verband gebracht met andere management-onderwerpen.

De directies stellen per eenheid een managementcontract op waarin de

concrete bedrijfsdoelstellingen voor het komende jaar zijn vastgelegd. Concrete bepalingen over informatiebeveiliging bevatten deze managementcontracten niet.

Het gebrek aan directe ondersteuning van de FIB-3 door de FIB-2, gekoppeld aan een zwakke positie van de FIB-3 binnen de eenheid en het ontbreken van dwingende concrete afspraken op dit gebied in het managementcontract, beperkt de bijdrage van FIB-organisatie aan de informatiebeveiliging bij de eenheden in hoge mate.

De Belastingdienst is in april 1996 begonnen met de vorming van een Centrale facilitaire dienst (CFD, voormalig Projectbureau Huisvesting), die onderverdeeld wordt in regionale diensten. De eenheden moeten service niveau overeenkomsten (SNO) sluiten met de regionale facilitaire diensten over het faciliteitenmanagement. De beveiliging is een van de onderdelen van de dienstverlening die financieel gezien onder de primaire verantwoordelijkheid van het facilitair bedrijf valt. De verantwoordelijkheid voor de naleving van voorschriften en het toezicht wordt gezien als een gedeelde verantwoordelijkheid van de eenheid en de facilitaire dienst.

Parallel aan deze ontvlechting van de ondersteunende diensten is de Belastingdienst in april 1996 begonnen met de vorming van een centraal geleide organisatie Eerstelijns Beheer en Exploitatie (EBE). Deze organisatie is per 1 oktober 1996 van kracht. Er zijn regionale teams gevormd die op grond van een Service Niveau Overeenkomst (SNO) zorg dragen voor het in stand houden van de Technische InfraStructuur. Op het gebied van beveiliging houdt dit ondermeer in dat EBE:

- op het niveau van de besturingssystemen autorisatieopdrachten van de eenheden uitvoert;
- alle software moet controleren op virussen;
- dagelijkse en wekelijkse back-ups van de systemen moet maken.

Voorheen waren dit activiteiten die werden uitgevoerd door medewerkers van de eenheid. Met de komst van EBE is de uitvoering van dit deel van het beveiligingsbeleid aan de directe verantwoordelijkheid van de eenheden onttrokken.

2.3 Managementinformatie over informatiebeveiliging

Eén van de instrumenten waarvan de hoofden van de eenheden zich kunnen bedienen om zicht te krijgen op het kwaliteitsniveau van de informatiebeveiliging is het zogenaamde Systeem Beveiligingsonderzoek (SBO-pakket). Dit pakket bevat een zeer uitgebreide lijst met vragen over de informatiebeveiliging. De scores worden verwerkt in de kwartaalrapportage aan de directie en zij worden gebruikt voor het opstellen van het eenheidsbeveiligingsplan.

De gemiddelde scores van de vijf bezochte eenheden varieerden in 1996 van ruim 70% tot bijna 100%.

De Rekenkamer heeft bij de vijf bezochte eenheden voor een aantal hoofdpunten een vergelijking gemaakt tussen de feitelijk aangetroffen situatie en de antwoorden die de eenheden op die punten hadden gegeven in de SBO-vragenlijst. Het feitelijk aangetroffen beeld bleek sterk af te wijken van het beeld dat op basis van de SBO-scores mocht worden verwacht. Volgens de Rekenkamer is dit te wijten aan het feit dat de SBO-vragenlijst slechts een formele toets vormt. De vragen missen voldoende diepgang, waardoor de antwoorden een te positief beeld geven. Bovendien dekt de SBO-vragenlijst niet alle aspecten van de informatiebeveiliging af. Essentiële vragen over bijvoorbeeld de inbraakbeveiliging ontbreken.

De discrepanties worden echter ook veroorzaakt door de wijze van beantwoorden. In enkele gevallen strookten de gegeven antwoorden niet

met de werkelijkheid. Ook het gebruiken van de antwoordcategorie «zie notitie» bij vragen waar een negatief antwoord van toepassing is geeft een positieve vertekening van het beeld.

Dit alles maakt volgens de Rekenkamer dat de SBO-vragenlijst geen volledig en juist beeld geeft van de beveiligingssituatie. Daarom is de lijst niet afdoende om als managementinstrument of als input voor verantwoordingsinformatie te dienen.

De directie PFC maakt voor haar informatievoorziening gebruik van de halfjaarlijkse rapporten van de directies van de eenheden. Deze halfjaarlijkse rapporten zijn gebaseerd op de kwartaalrapportages van de eenheden aan de directies. Het belangrijkste onderdeel van deze rapportages betreft logistieke informatie over het realiseren van de geplande produktiecijfers, maar er wordt ook aandacht besteed aan de kwaliteit van de interne controle, waar de informatiebeveiliging van de geautomatiseerde systemen een onderdeel van vormt. Naast deze kwartaalrapportages krijgen de directies summiere voortgangsrapportages over de vorderingen die zijn gemaakt met het 10-punten programma en er worden periodiek gesprekken gevoerd met de controller op de eenheden.

Op basis van deze informatie komt de directie PFC tot een vrij positief beeld van de voortgang van de verbeteringsactiviteiten op het punt van de informatiebeveiliging bij de eenheden. Deze directie acht, gelet op de normen en de realisering ervan, de risico's van het huidige beveiligingsniveau aanvaardbaar.

De EDP-audit afdeling van de IAB voert jaarlijks audits uit bij gemiddeld 35 tot 40 eenheden. Deze audits leveren een betrekkelijk negatief beeld op van het beheer en de beveiliging van de lokale automatisering en van de interne controle daarop. Volgens rapportages van de IAB van maart 1996 zijn de tekortkomingen zoals die voor 1994 werden geconstateerd bij veel eenheden nog grotendeels actueel. Zo werd het basisbeveiligingsniveau nog niet overal gehaald en werd de interne controle bij een groot aantal eenheden niet structureel uitgevoerd. Dit gold zowel de interne controle op het faciliteitenbeheer als de interne controle op de automatisering van de eenheden.

Om zich een beeld van de stand van zaken van de informatiebeveiliging bij de eenheden te vormen kan de dienstleiding dus beschikken over:

- bestuurlijke informatie over de voortgang van verbeteringsacties bij de eenheden;
- de resultaten van de IAB-audits op de feitelijke realisatie.

Het feit dat de feitelijke verbeteringen op de eenheden in een lager tempo worden gerealiseerd dan was beoogd, zoals uit de IAB-rapportages blijkt, is volgens het ministerie aanleiding geweest tot het treffen van nadere maatregelen, bijvoorbeeld het 10-puntenprogramma.

2.4 Conclusies

De Rekenkamer concludeert dat de staatssecretaris zijn toezeggingen uit 1992 gestand heeft gedaan. De bestuurlijke aandacht voor de informatiebeveiliging heeft geleid tot een uitgebreid stelsel van voorschriften. De bestuurlijke beheersing van en controle op de naleving van de voorschriften heeft naar haar mening echter niet goed gewerkt. De aansturing van de informatiebeveiligingsfunctionarissen op de eenheden laat te wensen over. De Rekenkamer concludeert verder dat de SBO-vragenlijst geen representatief beeld geeft van de beveiligingssituatie op de eenheden. De vragen missen voldoende diepgang en de lijst dekt niet alle aspecten van de informatiebeveiliging af. Dit maakt de

SBO-vragenlijst volgens de Rekenkamer niet afdoende als management-instrument.

De Rekenkamer constateerde dat de twee relevante management-informatiestromen over de informatiebeveiliging tot geheel verschillende conclusies leiden over de beveiligingstoestand op de eenheden. Zij is van mening dat het feit dat de conclusies op basis van de twee management-informatiestromen zo uiteen lopen op centraal niveau meer aandacht moet krijgen. Bovendien moeten volgens haar de conclusies van de IAB aanleiding zijn voor een grotere druk en actievere controle op de naleving van de voorschriften op de eenheden.

Tenslotte dringt de Rekenkamer er op aan bij de ontvlechting van de ondersteunende diensten en het faciliteitenbeheer zorg te dragen voor een eenduidige verdeling van de verantwoordelijkheden voor de informatiebeveiliging.

Daaromtrent bestaan thans zorgen.

3 BEVEILIGINGSSITUATIE BIJ VIJF EENHEDEN

3.1 Beveiliging gebouwen

3.1.1 Budgetten

De Centrale facilitaire dienst (CFD) beheert het jaarlijkse totaalbudget voor huisvesting van circa f 22 miljoen, waarvan ongeveer f 5 à 6 miljoen specifiek beschikbaar wordt gesteld voor beveiliging. Volgens het hoofd van de CFD is er om de beveiliging bij de eenheden in bestaande gebouwen op het gewenste niveau te brengen circa f 12 miljoen nodig. Hiervoor heeft de CFD een periode van 5 jaar uitgetrokken. f 6 miljoen is gereserveerd voor urgente gevallen in de jaren 1997 en 1998. Daarna zal er tot 2001 nog f 2 miljoen per jaar beschikbaar zijn. De CFD baseert zich voor haar plannen onder meer op een totaaloverzicht van de beveiligingstoestand op de eenheden.

3.1.2 Inbraakbeveiliging

Uit het eerder genoemde totaaloverzicht van de beveiligingstoestand bij de eenheden van CFD bleek dat bij alle bezochte eenheden inbraakdetectieapparatuur was aangebracht.

De kwaliteit van de inbraakbeveiliging bij de vijf bezochte eenheden bleek echter sterk uiteen te lopen. Eén van de bezochte eenheden was zeer goed beveiligd tegen inbraak. Het gebouw in kwestie is sedert 1995 in gebruik bij de Belastingdienst. Bij de vier andere vestigingen was de detectieapparatuur beperkt toegepast, bij twee vestigingen zelfs zo beperkt, dat het de vraag is of een inbreker zou worden gedetecteerd. Verzoeken van deze eenheden om in het kader van renovatieprojecten verbetering aan te brengen in deze situatie werden door het toenmalig verantwoordelijke Projectbureau huisvesting niet gehonoreerd.

De vijf eenheden hebben alle een contract met een beveiligingsbedrijf. De tijd waarbinnen het beveiligingsbedrijf bij alarm ter plaatse een onderzoek moet instellen is in deze contracten niet vastgelegd. In de praktijk is gebleken dat deze reactietijd kon oplopen tot een half uur.

3.1.3 Toegangscontrole

Uit het overzicht van de CFD bleek dat bij drie van de onderzochte eenheden de toegangscontrole geheel en bij twee eenheden beperkt zou zijn geïmplementeerd.

Bij geen van de vijf onderzochte eenheden bleek echter de toegangscontrole goed te functioneren, bij twee eenheden zelfs slecht. De belangrijkste tekortkomingen waren:

- de toegangscontrole was eenvoudig te omzeilen of beperkt tot oogtoezicht;
- vitale kritische ruimten werden niet altijd van extra beveiliging voorzien of de aangebrachte voorzieningen werden niet effectief gebruikt;
- de aangebrachte voorzieningen (keycard-deuren, tourniquets) blijken in technisch opzicht niet te voldoen of regelmatig defect te zijn;
- de handmatig bijgehouden registratie van afgegeven keycards was onvoldoende controleerbaar;
- het toezicht op personeel van onderhouds- en schoonmaakdiensten was onvoldoende;
- publiek werd – al dan niet voorzien van een bezoekersbadge – zonder begeleiding toegelaten in dienstruimten en kritische ruimten;
- «inwonend personeel» van andere overheidsdiensten hield zich niet aan de voorschriften voor de toegangscontrole.
- keycards van voormalig en van tijdelijk personeel en bezoekersbadges werden niet altijd geblokkeerd dan wel ingenomen. Omdat hierop geen

interne controle achteraf werd uitgevoerd had dit tot gevolg dat grote aantallen personeelsleden en tijdelijke krachten die de dienst al hadden verlaten nog steeds in bezit waren van een werkende pas.

3.2 Beveiligingsaspecten van werkprocessen

Bij alle eenheden geldt de regel dat niet-openbaar gegevensmateriaal moet worden opgeborgen en dat bureaus en kasten moeten worden afgesloten.

Bij geen enkele van de vijf eenheden hield men zich aan deze regel. Volgens de eenheden zou het primaire productieproces onvoldoende voortgang hebben als de werkdossiers en voorraden steeds aan het einde van iedere werkdag zouden moeten worden opgeborgen. Bovendien beschikken de eenheden niet over voldoende afsluitbare kasten. Twee eenheden gaven aan dat concrete voorstellen voor het aanschaffen van voldoende kastmateriaal door het toenmalig verantwoordelijke Projectbureau Huisvesting niet waren gehonoreerd.

Ondanks de toegenomen automatisering zijn de hoeveelheden papieren gegevensdragers waar de eenheden mee moeten werken nog erg groot. Dit «kritische» papier wordt bij alle bezochte eenheden gescheiden ingezameld en voor transport aangeboden aan een speciaal hiervoor gecontracteerd bedrijf.

Bij twee eenheden bleek echter dat de opslag van dit papier niet altijd voldoende is afgeschermd voor onbevoegden. Bij één eenheid werd het papier 's ochtends in niet afsluitbare containers aan de weg gezet in afwachting van het transportbedrijf. Bij een andere eenheid werd het papier wegens een te beperkte opslagcapaciteit in het archief bewaard in een niet voor onbevoegden afgeschermde kelderruimte. Overigens werkt de Belastingdienst aan een plan om de eenheden uit te rusten met afsluitbare papiercontainers.

Een bijzonder probleem vormt het toesturen van overzichten met persoonsgevoelige informatie over loon en rente-inkomsten (loon- en rente-renseignementen) door het BAC. Dit geschiedt in tweevoud: in elektronische vorm en op papier. Het gaat per eenheid om zeer grote hoeveelheden papier. Twee van de vijf eenheden boden de papieren versie ongebruikt ter vernietiging aan. Mede gelet op het probleem dat zich in het voorjaar van 1996 met deze renseignementen voordeed op de stortplaats in Hilversum (zie paragraaf 3.6) verdient het aanbeveling het rondsturen van de papieren versie te heroverwegen. De papieren versie zou uitsluitend toegestuurd moeten worden aan eenheden die aan kunnen tonen dat zij deze nodig hebben voor de uitoefening van hun taak.

3.3 Calamiteitenplan

Elke eenheid van de Belastingdienst dient te beschikken over een calamiteitenplan. Dit plan moet bestaan uit een preventieplan, ontruimingsplan, continuïteitsplan en een herstelplan. Het testen van calamiteitenplannen bleek bij de vijf eenheden nauwelijks te gebeuren. Bij twee eenheden was een ontruimingsplan getest. Bij één van deze twee eenheden bleek het calamiteitenplan alleen een ontruimingsplan te behelzen. Van het bestaan of de verplichting tot het hebben van de andere onderdelen was men bij deze eenheden niet op de hoogte. De overige drie eenheden hadden wel de beschikking over een volledig calamiteitenplan, al werd dit niet getest.

Om de continuïteit van de werkprocessen ook in gevallen van ernstige calamiteiten te waarborgen moeten er dagelijks back ups worden gemaakt van de databestanden en wekelijks van de gehele systemen. De wekelijkse

back ups moeten buiten het gebouw worden bewaard. Het maken van de back ups is een verantwoordelijkheid van EBE.

Bij één eenheid mislukte het maken van de dagelijkse back up regelmatig. Wanneer dit werd ontdekt was er onvoldoende tijd beschikbaar om alsnog een back up te maken.

Bij één eenheid werd de wekelijkse back up van het IBS – het belangrijkste produktiesysteem bij de eenheden Particulieren – buiten het gebouw bewaard. Dit betekent dat bij de andere vier eenheden bij ernstige calamiteiten informatie blijvend verloren kan raken.

3.4 Toegang tot geautomatiseerde systemen

3.4.1 Voorschriften

Het Handboek Informatiebeveiliging Belastingdienst geeft uitgebreide voorschriften om te verhinderen dat onbevoegde personen toegang krijgen tot geautomatiseerde systemen. Twee essentiële punten in de toegangsbeveiliging zijn:

- autorisaties van gebruikers van de systemen moeten worden toegekend in een fiatteringsprocedure en overeenkomen met de functies van de betrokken medewerkers;
- functiescheidingen mogen niet door het gebruik van geautomatiseerde systemen worden doorbroken.

3.4.2 Autorisaties

Geen van de door de Rekenkamer bezochte eenheden bleek te beschikken over accurate taakbeschrijvingen per functie. De eenheden werken met de oude groepsfunctie-beschrijvingen, die te globaal zijn voor het op specifieke functies toesnijden van autorisaties en die bovendien niet meer passen op de veranderde werkprocessen van de Belastingdienst.

Een actueel overzicht van de verstrekte autorisaties ontbrak bij de vijf eenheden. Dit kan worden geweten aan de veelheid van de in gebruik zijnde systemen met de eigen technische toekenningssystematieken en de verschillen in de functionele opbouw van de systemen.

Bij één van de bezochte eenheden verliep de toekenning van autorisaties via een adequate aanvraag- en fiatteringsprocedure. Bij vier eenheden werden de door de teamleiders aangevraagde autorisaties zonder toetsing aan de functie en aan al verstrekte autorisaties min of meer automatisch toegekend.

Na functie- of taakwijzigingen overbodig geworden autorisaties werden bij geen van de bezochte eenheden onmiddellijk ingetrokken, omdat de teamleiders dit niet wenselijk vonden. Medewerkers met veel autorisaties kunnen namelijk flexibel worden ingezet. Hier speelt de permanente druk op het realiseren van de contractueel vastgelegde productie een belangrijke rol.

Bij alle vijf eenheden kwam het voor dat autorisaties van vertrekkend personeel niet waren ingetrokken of geblokkeerd. Omdat interne controle achteraf ook niet werd uitgevoerd, had dit tot gevolg dat grote aantallen personeelsleden en tijdelijke krachten die de dienst al hadden verlaten nog steeds geautoriseerd waren voor één of meer systemen.

3.4.3 Functiescheiding

Alle bezochte eenheden kenden «supergebruikers», die voor bijna alle functies binnen het systeem geautoriseerd zijn. Door hun technische

kennis van het geautomatiseerde systeem en hun belastingtechnische kennis zijn zij de kurk geworden waarop de teams drijven. Het beperken van autorisaties bij deze medewerkers zou de voortgang van het primair proces volgens de teamleiders te zeer hinderen.

Dit houdt echter wel in dat functiescheidingen, die noodzakelijk zijn voor de handhaving van de betrouwbaarheid en controleerbaarheid van de gegevens, worden doorbroken door onderscheiden functies toch in één medewerker te verenigen.

Bij alle vijf eenheden is gebleken dat de toepassingsbeheerders en de medewerkers van EBE geautoriseerd zijn tot het uitvoeren van alle gebruikersfuncties in alle systemen. Dit houdt in dat zij daarin lees- en muatierechten hebben, waar zij dat voor de uitoefening van hun functie niet nodig hebben.

3.4.4 Wachtwoorden en toegangscodes

Bij alle vijf eenheden zijn situaties aangetroffen, waarin wachtwoorden voor iedereen beschikbaar waren, bijvoorbeeld door het individueel of op een afdelingslijst noteren van de wachtwoorden of door de wachtwoorden in de vorm van barcodes op de PC's te plakken, terwijl barcodereaders aanwezig zijn. Ook kwam het voor dat medewerkers elkaars of een gezamenlijke toegangscode gebruikten.

De Rekenkamer merkt hierbij op dat het zorgvuldig beheer van het wachtwoord door de individuele medewerker wordt bemoeilijkt door het grote aantal in gebruik zijnde systemen met eigen wachtwoord-eisen. Het is technisch mogelijk om medewerkers maar één keer te laten inloggen om toegang te krijgen tot alle systemen waarvoor zij geautoriseerd zijn. Deze technologie wordt bij de Belastingdienst niet toegepast, hoewel deze in het Handboek Informatiebeveiliging wordt voorgeschreven.

3.4.5 Leesrechten

Bij alle vijf eenheden is gebleken dat nagenoeg alle produktiemedewerkers en medewerkers van ondersteunende afdelingen geautoriseerd zijn tot het lezen van gegevens van belastingplichtigen in lokale maar ook in landelijke systemen. Deze leesrechten worden bij indiensttreding min of meer automatisch aan de medewerkers verstrekt. Een meer concrete op de functie toegesneden afweging van deze leesrechten – noodzakelijk gegeven het feit dat de leesrechten in vele gevallen niet beperkt blijven tot lokale bestanden maar ook betrekking hebben op landelijke bestanden – vindt in de praktijk niet plaats.

De Wet Persoonsregistraties schrijft voor dat van persoonsregistraties een reglement moet worden opgesteld waarin nadere regelgeving is opgenomen in het kader van de vertrouwelijke behandeling van de gegevens. De Belastingdienst heeft van een groot aantal van deze bestanden een dergelijk reglement opgesteld. In het onderzoek werden echter ook persoonsregistraties aangetroffen zonder een bijbehorend reglement. Het betrof de persoonsregistraties:

- exploitanten en mede-exploitanten speelautomaten;
- artiesten;
- standhouders markten;
- rijschoolhouders;
- shoarmazaken.

3.5 Interne controle

De uitvoering van de interne controle liet met name bij het afmelden van personeel dat de dienst had verlaten te wensen over (zie ook punten 3.1.3 en 3.4.2).

In het Handboek informatiebeveiliging worden geen expliciete richtlijnen gegeven voor de organisatie en uitvoering van de interne controle op de toegang tot de geautomatiseerde systemen bij de eenheden. Er zijn op het gebied van de vastlegging wel voorwaarden gesteld die interne controle mogelijk maken. Zo moet er een uitgebreide lijst van gegevens over het gebruik van geautomatiseerde functies (autorisaties), gebruikerindentificatie en transacties (lezen, muteren, verwijderen) beschikbaar zijn.

Sommige eenheden kunnen om technische redenen niet aan de voorschriften voldoen. Ten tijde van het onderzoek waren er geen goede geautomatiseerde instrumenten voorhanden om de autorisaties voor alle systemen in onderling verband en in verband met taken en functies buiten de systemen om te beheren en te beheersen. Ook waren er bij de vijf eenheden geen instrumenten voor een structurele interne controle op de vastlegging van specifieke transacties.

Van de faciliteiten die wel beschikbaar zijn, wordt echter ook weinig of in het geheel geen gebruik gemaakt. Dit geldt zowel voor de vastlegging zelf als voor het gebruik van de vastleggingen van autorisaties en van transacties voor interne-controledoeleinden. Dit laatste is met name van belang bij die transacties waarbij de voorgeschreven functiescheiding ontbreekt en er dus geen (extra) interne controle wordt uitgevoerd.

3.6 Klachten van belastingplichtigen

Bij de vijf eenheden heeft de Rekenkamer onderzoek gedaan naar de klachtenregistratie en -inhoud over de jaren 1993 tot en met 1996. Hieruit bleek dat geen van de ingediende klachten was te herleiden tot tekortkomingen in de informatiebeveiliging.

Wel deed zich tijdens de onderzoeksperiode een incident voor dat de landelijke media bereikte. Het betreft de storting van loon- en renteren-seignementen op de vuilnisplaats van Hilversum. Betrokken belastingplichtigen hebben naar aanleiding hiervan klachten ingediend bij de verantwoordelijke eenheid. Deze eenheid viel buiten het onderzoek, maar het voorval toont wel het belang aan van een zorgvuldige opzet en uitvoering van beveiligingsmaatregelen.

3.7 Bestraffingen

De Rekenkamer heeft voor 5 gevallen van inbreuk op de beveiligingsvoorschriften die een officiële bestraffing van betrokken ambtenaar tot gevolg hadden onderzocht of deze gevallen hadden geleid tot nieuwe of aanscherping van bestaande beveiligingsmaatregelen. De onderzochte bestraffingen vonden plaats bij drie eenheden.

Drie bestraffingen hadden betrekking op het onbevoegd muteren of raadplegen van gegevensbestanden. Bij de betrokken eenheden waren verder geen concrete maatregelen naar aanleiding van de bestraffingen getroffen. Er werd geen verband gelegd tussen het feit dat de inbreuk zich had voorgedaan en het treffen van structurele maatregelen om soortgelijke inbreuken te voorkomen. Dezelfde overtredingen kunnen dus nog steeds voorkomen en zullen waarschijnlijk in het merendeel van de gevallen niet ontdekt worden.

Twee bestraffingen hadden betrekking op het onbevoegd verstrekken van SoFi-nummers. De eenheid heeft naar aanleiding van deze gevallen functiescheidingen aangebracht tussen het beoordelen van de aanvrage en het verstrekken van het SoFi-nummer. Uit onderzoek is echter gebleken dat deze procedure toch nog steeds op eenvoudige wijze kan worden omzeild. Door onvoldoende controlemogelijkheden zal misbruik niet snel worden ontdekt.

De Rekenkamer constateerde dat deze problematiek zich ook bij de andere eenheden voordeed. Opmerkelijk is dan ook dat de bestraffingen geen aanleiding hebben gegeven tot het treffen van afdoende Belastingdienstbrede maatregelen.

3.8 Conclusies

De inbraakbeveiliging van het gebouw en de toegangscontrole vertoonden bij alle onderzochte eenheden tekortkomingen. Verzoeken van deze eenheden om in het kader van renovatieprojecten de inbraakbeveiliging te verbeteren werden niet gehonoreerd. Het overzicht van de Centrale facilitaire dienst van de stand van de beveiliging van het gebouw bij de eenheden bleek geen goed beeld van de werkelijkheid te geven.

Bij alle vijf eenheden lag niet-openbare informatie open en bloot in niet afgesloten werkkamers, zodat deze informatie dus direct toegankelijk is voor onbevoegden. De Belastingdienst loopt daarnaast onnodige risico's bij het verspreiden van papieren documenten die ook in elektronische vorm worden aangeboden aan de eenheden.

De Belastingdienst heeft de beveiliging van de toegang tot de geautomatiseerde systemen in opzet goed geregeld. Het gebruik van de beschikbare beveiligingsmiddelen voldoet bij de onderzochte vijf eenheden echter niet aan de eisen. In de praktijk blijkt dat het management de naleving van de beveiligingsvoorschriften ondergeschikt maakt aan de voortgang van het primaire proces. Dit gebeurt zowel op basis van impliciete als expliciete afwegingen van het management. Functiescheidingen worden ten behoeve van het produktieproces niet aangebracht, terwijl er onvoldoende compenserende interne controles worden uitgevoerd. Op veel plaatsen wordt slordig met de persoonlijke wachtwoorden omgegaan en de leesrechten van privacy-gevoelige informatie worden bij indiensttreding automatisch toegekend.

De continuïteit bij de eenheden loopt gevaar doordat aan de voorgeschreven back up-procedure onvoldoende gevolg wordt gegeven.

Ontdekte en bestrafte inbreuken op de beveiligingsvoorschriften hebben in de praktijk niet geleid tot aanpassing van de voorschriften.

Het feit dat én de inbraakbeveiliging, én de toegangscontrole van het gebouw én de toegangsbeveiliging van de geautomatiseerde systemen gebreken vertonen leidt tot de conclusie dat de informatiebeveiliging bij de vijf onderzochte eenheden ernstige tekortkomingen vertoont. Deze conclusie is in lijn met de resultaten van de veel omvangrijker jaarlijkse onderzoeken van de IAB naar de informatiebeveiliging bij de eenheden.

4 EINDCONCLUSIES EN AANBEVELINGEN

De Rekenkamer komt tot de eindconclusie dat de staatssecretaris veel aandacht heeft besteed aan de informatiebeveiliging bij de Belastingdienst. Hij is er, zoals het onderzoek blijkt, echter nog niet in geslaagd de informatiebeveiliging bij de eenheden op een aanvaardbaar peil te brengen. De bestuurlijke beheersing van en controle op de naleving van de voorschriften heeft niet geleid tot voldoende verbetering van de beveiligingspraktijk.

De voorschriften op het gebied van informatiebeveiliging zijn goed te noemen, maar zowel uit de bevindingen van de IAB als uit het eigen onderzoek van de Rekenkamer bij vijf eenheden blijkt dat de beveiligingssituatie in de praktijk nog weinig verbeterd is. De inbraakbeveiliging en toegangscontrole van het gebouw en de beveiliging van de toegang tot de geautomatiseerde systemen blijken bij de vijf onderzochte eenheden gaten te vertonen.

De vijf eenheden bleken zich onvoldoende aan de beveiligingsvoorschriften te houden. De hierdoor ontstane risico's voor de betrouwbaarheid van de gegevensverwerking worden niet voldoende door interne controles gecompenseerd. Door onvoldoende interne controles is ook het risico aanwezig dat inbreuken op de ambtelijke integriteit niet tijdig worden gesignaleerd. De Belastingdienst heeft geen volledig en juist inzicht in de werking van de voorschriften bij de eenheden. Belangrijke bouwstenen voor de managementinformatie hierover bleken een te positief beeld van de praktijk te geven. Dit gold bijvoorbeeld voor het totaaloverzicht van de beveiliging van gebouwen van de Centrale Facilitaire Dienst en voor het Systeem Beveiligings Onderzoek dat alle eenheden gebruiken om hun beveiligingssituatie te inventariseren.

De Rekenkamer dringt er op aan bij de ontvlechting van de ondersteunende diensten en het faciliteitenbeheer zorg te dragen voor een eenduidige verdeling van de verantwoordelijkheden voor de informatiebeveiliging. Daaromtrent bestaan thans zorgen.

Mede gelet op het toenemende belang van automatisering op de eenheden en daarmee van informatiebeveiliging beveelt de Algemene Rekenkamer aan om op korte termijn:

- de informatie bij de CFD over de beveiliging van de gebouwen te actualiseren om vervolgens op basis van een accurate prioriteitenstelling met kracht achterstanden op dit gebied weg te werken. Dit aspect zou in de toekomst betrokken moeten worden in de onderzoeken van de IAB;
- de organisatie voor informatiebeveiliging en interne controle op de eenheden en de directies (de FIB-organisatie) te versterken om daarmee af te dwingen dat voorschriften ook daadwerkelijk worden nageleefd. Gedacht kan worden aan frequent overleg binnen de FIB-organisatie, het uitvoeren van onderzoek door de directies naar de naleving van de voorschriften en het aanspreken van de hoofden van de eenheden op hun verantwoordelijkheden op dit gebied; daarbij moeten zodanige investeringen worden gedaan in de programmatuur, dat de voorschriften gemakkelijker dan nu kunnen worden nageleefd;
- de aandacht voor de beveiliging van informatie verder te versterken door:
  - het uitvoeren van extra interne controles op die functies die naar hun aard of door het ontbreken van functiescheidingen extra risico's inhouden;
  - het verder ontwikkelen en zonodig opleggen van sancties voor het niet-naleven van beveiligingsvoorschriften;
  - het treffen van Belastingdienstbrede maatregelen naar aanleiding van gebleken opzettelijke inbreuken op de voorschriften om herhaling te voorkomen.

5 REACTIE STAATSSECRETARIS EN COMMENTAAR REKENKAMER

5.1 Algemeen

De staatssecretaris van Financiën schreef in zijn reactie dat de conclusies van de Rekenkamer dat de toezeggingen naar aanleiding van het onderzoek in 1991–1992 zijn nagekomen en dat er veel aandacht is besteed aan de beveiliging bij de eenheden zijn oordeel bevestigden dat de Belastingdienst in het vormgeven en uitvoeren van het informatiebeveiligingsbeleid op de goede weg is. Het rapport gaf aan dat de eenheden op het moment van onderzoek nog niet op alle onderdelen voldeden aan de normen die de Belastingdienst zichzelf stelt. Dit bevestigde hem in het beleid om verder te investeren in de informatiebeveiliging op de eenheden.

De huidige beveiligingsrisico's waren, gelet op de normen en de realisering daarvan, naar de mening van de staatssecretaris aanvaardbaar.

Volgens de staatssecretaris geeft het onderzoek geen representatief beeld van de wijze waarop de Belastingdienst aandacht geeft aan het beveiligingsbeleid en de maatregelen die in dat kader zijn getroffen, omdat alleen de situatie bij de onderzochte vijf eenheden wordt weergegeven.

De Rekenkamer meende haar onderzoek ter plaatse tot vijf eenheden te kunnen beperken, omdat de resulterende bevindingen beoordeeld konden worden tegen de achtergrond van de bevindingen van de IAB, die jaarlijks bij 35 à 40 eenheden onderzoek doet. Alleen voor haar bevindingen over de fysieke beveiliging gaat dit niet op, omdat dit niet in de IAB-onderzoeken wordt meegenomen. Deze bevindingen moeten inderdaad op zichzelf beschouwd worden en zijn niet noodzakelijkerwijs representatief.

5.2 Informatievoorziening

Volgens de staatssecretaris is de conclusie over de ontoereikendheid van de SBO-vragenlijst als managementinformatie niet juist, omdat de lijst bedoeld om de opzet van de beveiliging te inventariseren en niet zo zeer de werking.

Van de door de Rekenkamer bedoelde tegenstellingen in managementinformatiestromen op dit gebied was volgens hem geen sprake.

De conclusie van de Rekenkamer dat de Belastingdienst onvoldoende zicht had op de werking van de voorschriften kon de staatssecretaris niet plaatsen. Hij kreeg hierover voldoende informatie van de IAB.

De Rekenkamer wijst erop dat de opzet van de beveiliging beschreven is in het Handboek informatiebeveiliging. In het onderzoek is gebleken dat de eenheden de SBO-vragenlijst gebruiken als bron voor de periodieke rapportering aan de doeldirectie over de beveiligingssituatie in de zin van het implementeren van de in de opzet voorgeschreven maatregelen. Verder wijst de Rekenkamer erop dat de IAB in haar rapporten constateert dat de eenheden een veel gunstiger beeld geven van de feitelijke beveiligingssituatie dan op basis van haar bevindingen gerechtvaardigd zou zijn.

5.3 Ontvlechting

De ontvlechting van het faciliteitenbeheer en ondersteunende diensten leidde volgens de staatssecretaris tot een versterking van de beheersbaarheid van beheer en beveiliging. Gezien het complexe karakter van

deze operatie vond hij het voorstelbaar dat in de onderzoeksperiode nog sprake was van onduidelijkheden.

5.4 Beveiligingssituatie bij vijf eenheden

Naar de mening van de staatssecretaris waren er ten aanzien van de fysieke beveiliging afgewogen keuzen gemaakt. De fysieke beveiliging (inclusief de inbraakbeveiliging) werd volgens een meerjarige planning ingevoerd, waarbij de minst beveiligde gebouwen en nieuwbouwprojecten de hoogste prioriteit hebben gekregen. Ultimo augustus 1996 was ruim 60% van het brutovloeroppervlak overeenkomstig de eisen beveiligd, terwijl circa 25% gedeeltelijk beveiligd was.

De staatssecretaris meende dat het als ontoereikend beoordeelde gebruik van middelen voor de logische toegangsbeveiliging (functiescheidingen, persoonlijke wachtwoorden) in het juiste perspectief moest worden geplaatst. In de cultuur van de Belastingdienst is de geheimhoudingsverplichting in combinatie met een goed ontwikkelde sociale controle sterk geworteld. Een dergelijke werkcultuur stimuleert een open wijze van samenwerking en veronderstelt veel onderling vertrouwen. Ondanks dat heeft de Belastingdienst gezorgd voor een goede logische toegangsbeveiliging en structurele maatregelen om het beheer van de autorisaties te ondersteunen.

De Rekenkamer is van mening dat informele mechanismen op zich onvoldoende zijn om een goede beveiliging te waarborgen en dat deze te allen tijde ondersteund moeten worden door sluitende procedures.

5.5 Eindconclusies en aanbevelingen

De staatssecretaris kon zich niet vinden in de eindconclusie dat de bestuurlijke aandacht niet heeft geleid tot het op een aanvaardbaar niveau brengen van de informatiebeveiliging. Hij plaatste dit standpunt in het perspectief van historische ontwikkelingen, het integrale management en de risicobeheersing. Tegen deze achtergrond achtte hij de situatie op de eenheden ten opzichte van 1992 verbeterd.

Dat de Belastingdienst nog niet op alle punten voldeed aan het geformuleerde beleid hing volgens hem samen met het hoge niveau van de beleidsdoelen.

De Belastingdienst heeft vanwege de aard van de processen gekozen voor een relatief hoog niveau van beveiliging, dat redelijk en daarmee aanvaardbaar is ten opzichte van de processen, gegevens en risico's. Bij een grote organisatie als de Belastingdienst zullen er volgens de staatssecretaris echter altijd incidenten plaatsvinden, bijvoorbeeld door menselijk falen en onvoorziene bedreigingen.

Als reactie op de aanbevelingen van de Rekenkamer merkte de staatssecretaris het volgende op:

- De informatie bij de CFD is inmiddels geactualiseerd. Er is een aanvullend budget aan CFD toegekend, zodat eind 1998 wordt voldaan aan de bouwkundige richtlijnen uit het Handboek Informatiebeveiliging. De interne controle op de fysieke beveiliging zal in samenwerking tussen de CFD en de IAB nader worden uitgewerkt;
- De aanbevolen versterking van de FIB-organisatie past in de reeds ingezette verbetering van de lokale informatiemanagementfunctie. Het lijnmanagement zal nadrukkelijk rekening moeten houden met adviezen uit de FIB-organisatie. De interne controle zal worden versterkt met extra onderzoeken, die meer dan voorheen op de werking van informatiebeveiliging op de werkvloer zijn gericht. De beveiligingsorganisatie wordt nadrukkelijk bij deze maatregelen betrokken.

Voor de investeringen in de programmatuur ter verbetering van de dagelijkse beveiligingspraktijk zijn reeds enige concrete projecten van start gegaan;

- De interne controle op gevoelige functies zal worden versterkt. De staatssecretaris was van mening dat het huidige sanctiebeleid toereikend is voor overtredingen op het gebied van de informatiebeveiliging. In het kader van het Voorschrift Informatiebeveiliging Rijksdienst zal een incidenten-registratie verder worden vormgegeven. Dit zal zo nodig leiden tot aanpassing van de richtlijnen in het handboek informatiebeveiliging.

6 NAWOORD REKENKAMER

De door de staatssecretaris toegezegde maatregelen, zoals het aanvullend budget voor de Centrale Facilitaire Dienst, de versterking van de informatiebeveiligingsorganisatie, de verdieping van de interne controle en de investeringen in programmatuur, zullen zeker bijdragen aan een noodzakelijke verdere verbetering van de naleving van de in opzet al goede beveiligingsmaatregelen.

De Rekenkamer wijst nog eens op het belang van inperking van de rechten op toegang tot geautomatiseerde systemen met vertrouwelijke informatie van belastingplichtigen. Zij onderstreept haar aanbevelingen om het sanctiebeleid bij niet naleving van voorschriften aan te scherpen en bij signalering van opzettelijke inbreuken Belastingdienstbrede maatregelen te treffen.

De Rekenkamer ziet met genoegen dat de staatssecretaris een hoog beveiligingsniveau nastreeft. Het hoge beveiligingsniveau acht zij zeer gewenst, niet alleen omdat de primaire processen bij de Belastingdienst in toenemende mate afhankelijk zijn geworden van betrouwbaar werkende geautomatiseerde systemen, maar ook om de belastingplichtigen de vertrouwelijke behandeling van hun gegevens te kunnen garanderen. Gelet op het grote maatschappelijke belang hiervan zal de Rekenkamer de ontwikkelingen dienaangaande aandachtig blijven volgen.