Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1999–2000

26 887 Omgaan met vertrouwelijke gegevens bij de Belastingdienst

Nr. 2 **RAPPORT**

Inhoud

KST42106
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 1999

Samenvatting

De Algemene Rekenkamer heeft in de periode juli – oktober 1999 op verzoek van de staatssecretaris van Financiën onderzoek gedaan naar het omgaan met vertrouwelijke gegevens van belastingplichtigen bij de Belastingdienst. Aanleiding tot het verzoek was het aan het licht komen van de verkoop van vertrouwelijke gegevens aan een incassobureau. De Rekenkamer heeft in haar onderzoek de werking van zowel het informatiebeveiligingsbeleid als van het integriteitsbeleid van de Belastingdienst betrokken. Het onderzoek is uitgevoerd bij vier eenheden van de directie Particulieren en Ondernemingen, waaronder de eenheid waar de aanleiding tot het onderzoek zich heeft voorgedaan. Tevens is gebruik gemaakt van informatie afkomstig van interne onderzoeken van de Belastingdienst.

Het beleid van de Belastingdienst voor *informatiebeveiliging* is gebaseerd op een drietal beveiligingsmaatregelen die onderling samenhangen. Het betreft ten eerste maatregelen die ervoor zorgen dat onbevoegden geen toegang tot Belastingdienstgebouwen hebben, ten tweede dat de gegevensuitwisseling geïsoleerd is van de buitenwereld en ten derde dat medewerkers van de Belastingdienst slechts toegang hebben tot gegevens waartoe zij geautoriseerd zijn. Uitgangspunt hierbij is het «need-to-know» beginsel waardoor medewerkers slechts geautoriseerd worden voor toegang tot die gegevens die noodzakelijk zijn voor het uitvoeren van hun taak. Het onderzoek richtte zich met name op de derde maatregel, de toegang tot de gegevens.
Het *integriteitsbeleid* van de Belastingdienst is gebaseerd op regelgeving en communicatie over integriteit. Er is een integriteitsprogramma opgezet dat onder andere bevat het volgen van dilemmatraining voor alle medewerkers van de Belastingdienst, het aanstellen van een vertrouwenspersoon integriteit Belastingdienst en het bespreekbaar maken van de basiswaarden van de Belastingdienst (geloofwaardigheid, verantwoordelijkheid, zorgvuldigheid).

Aanscherping van beveiligingsregels en intensivering van het integriteitsbeleid zijn voorbeelden van de inspanningen die de Belastingdienst de laatste jaren heeft gepleegd om het omgaan met vertrouwelijke gegevens te waarborgen. Deze inspanningen hebben in de praktijk echter nog onvoldoende effect gesorteerd. Daar bestaat een spanningsveld tussen enerzijds voldoen aan productie-eisen (aangiftenverwerking) en klantgerichtheid (zoals direct antwoord op een vraag) en anderzijds aandacht voor informatiebeveiliging en integriteit. De hoofdconclusie van de Rekenkamer is dat dit heeft geleid tot een situatie waarin risico's bestaan voor het onbevoegd raadplegen van vertrouwelijke gegevens en waarbij het integrale inzicht in die risico's bij de Belastingdienst ontbreekt.
Naar de mening van de Rekenkamer zou een integrale benadering waarin controle op en verantwoording over informatiebeveiliging als volwaardige elementen in de bedrijfsvoering worden meegenomen het eerder genoemde spanningsveld kunnen verkleinen. De integrale verantwoordelijkheid hiervoor is nu bij de eenheden gelegd, maar wordt onvoldoende ingevuld. Aan de achtergronden daarvan dient de Belastingdienst meer aandacht te besteden opdat er meer inzicht in en een betere beheersing van risico's voor het omgaan met vertrouwelijke gegevens komt. Dit is naar de mening van de Rekenkamer nu nog onvoldoende het geval.

Het onderzoek van de Rekenkamer wees uit dat er op het gebied van informatiebeveiliging nog tekortkomingen zijn. Zo is de verdeling van verantwoordelijkheden tussen de eenheden en andere organisatieonderdelen van de Belastingdienst onduidelijk en vertoont de interne controle op beheer en beveiliging bij drie van de vier onderzochte

eenheden achterstand. Voor wat betreft toegang tot gegevens heeft de Rekenkamer geconstateerd dat vrijwel alle medewerkers vertrouwelijke gegevens van vrijwel alle belastingplichtigen kunnen raadplegen. Het autorisatieregime (toekennen en intrekken van rechten) vergroot de risico's op onbevoegd raadplegen omdat medewerkers te ruim geautoriseerd zijn. Of er onbevoegd wordt geraadpleegd is bovendien slecht controleerbaar. Uit eigen onderzoeken van de Belastingdienst is gebleken dat beveiligingsregels worden overtreden en dat er onvoldoende aandacht van medewerkers en management was voor informatiebeveiliging. De registratie van beveiligingsincidenten is daarnaast niet compleet.

Uit het Rekenkameronderzoek en uit onderzoek van de Belastingdienst zelf bleek dat er bij toegestane nevenwerkzaamheden risico's van belangenverstrengeling aanwezig zijn. Daarnaast bleek tijdelijk personeel niet altijd over een verklaring omtrent gedrag te beschikken en/of een geheimhoudingsverklaring te hebben getekend. De communicatie over integriteit bleek in de praktijk nog onvoldoende effect te hebben. Uit het Rekenkamer onderzoek kwam naar voren dat medewerkers niet bekend waren met de basiswaarden van de Belastingdienst en met de in februari van dit jaar aangestelde vertrouwenspersoon integriteit. Bij de vier onderzochte eenheden had slechts een klein deel van de medewerkers dilemmatraining gevolgd. Voorts bleek dat maatregelen om het bewustzijn te vergroten nauwelijks werden benut en dat er binnen de Belastingdienst onvoldoende communicatie is over integriteitsinbreuken die zich hebben voorgedaan. Tenslotte is uit gesprekken met medewerkers naar voren gekomen dat er binnen grote delen van de Belastingdienst een cultuur heerst waarin medewerkers elkaar niet aanspreken op gedrag en verantwoordelijkheid daarvoor uit de weg gaan. Dit heeft ook tot gevolg dat wanneer zich integriteitsinbreuken voordoen deze in bepaalde gevallen niet gemeld worden.

De aanbevelingen van de Rekenkamer richten zich op verbeteringen op het gebied van de organisatie, van de toegang tot gegevens en op het gebied van bewustzijn en cultuur. Zo zou bij de beleidsvorming rekening gehouden moeten worden met de gevolgen van nieuwe maatregelen voor de primaire processen zodat op de werkvloer aandacht aan informatiebeveiliging en integriteit kan worden gegeven en zouden eenheden het kerndepartement moeten informeren over eventuele neveneffecten van nieuw beleid.
Voor de toegang tot gegevens heeft de Rekenkamer een groot aantal technische en organisatorische aanbevelingen gedaan om onder andere het «need-to-know» beginsel te ondersteunen. Deze variëren van technische inperking in informatiesystemen tot de wijze van autoriseren. Ook zijn suggesties gedaan om de controlemogelijkheden te vergroten. Op het gebied van bewustzijn en cultuur zijn mogelijkheden voor verbetering aangegeven die samengevat neerkomen op het bespreekbaar maken van problemen. De Rekenkamer denkt dan aan het bespreken van uitkomsten van onderzoeken met medewerkers, inventariseren waar onduidelijkheid bestaat over richtlijnen en integriteitsinbreuken geanonimiseerd bekend maken binnen de Belastingdienst.

De staatssecretaris van Financiën sprak in zijn reactie op het rapport waardering uit voor het bereikte resultaat en hij gaf aan de eindconclusie te onderschrijven. De aanbevelingen bieden naar zijn mening een goede basis om het ingezette beleid binnen de Belastingdienst op het gebied van informatiebeveiliging en integriteit verder uit te bouwen en te verbeteren. Voor de aanbevelingen om de problemen rond het omgaan met wachtwoorden weg te nemen en om de onduidelijkheden over voorschriften en richtlijnen weg te nemen kiest de staatssecretaris voor een tweesporen-

aanpak. Deze houdt in dat op korte termijn de voorgestelde aanbevelingen zullen worden gerealiseerd maar ook dat toekomstige ontwikkelingen worden meegenomen.
Om de onafhankelijke positie van een laagdrempelige vertrouwenspersoon te waarborgen zou hij ervoor willen kiezen deze functie op directieniveau in te stellen en in een enkel geval op eenheidsniveau. Voor de overige aanbevelingen gaf hij aan zich hierin te kunnen vinden.
Tenslotte merkte de staatssecretaris op dat – hoewel procedures inzake beveiliging en integriteit nog niet altijd vlekkeloos verlopen – hij ervan overtuigd is dat de medewerkers van de dienst in het algemeen gesproken op uiterst prudente wijze omgaan met vertrouwelijke gegevens.

De Rekenkamer heeft met genoegen kennis genomen van het voornemen van de staatssecretaris haar aanbevelingen over te nemen. Alleen ten aanzien van het instellen van een vertrouwenspersoon pleit de Rekenkamer, in afwijking van wat de staatssecretaris voorstaat, voor het aanwijzen van functionaris voor deze rol op eenheidsniveau. Naar haar mening hoeft dit de onafhankelijkheid van de functie niet aan te tasten, terwijl er toch een laagdrempelige toegang is.

1 ONDERZOEK

1.1 Inleiding

De staatssecretaris van Financiën heeft naar aanleiding van het verkopen van vertrouwelijke gegevens door medewerkers van de Belastingdienst de Rekenkamer het verzoek gedaan bij de Belastingdienst een onderzoek uit te voeren naar en nadere aanbevelingen te doen op bestaande beveiligingsmaatregelen ter bescherming van vertrouwelijke gegevens. Met dit onderzoek wordt deels een vervolg gegeven aan het in 1997 gepubliceerde rapport Informatiebeveiliging Belastingdienst[1].

Daarnaast is «integriteit» een vast aandachtspunt bij Rekenkameronderzoek zodat ook dit aspect expliciet is toegevoegd aan het onderzoek. Het onderzoek heeft onder meer tot doel de werking van het bestaande beleid en maatregelen op het gebied van bescherming van vertrouwelijke gegevens te toetsen.

Het betreft zowel het beleid voor informatiebeveiliging als het beleid voor integriteit. De bevindingen voor het algemeen beleid zijn gebaseerd op eigen onderzoek en informatie afkomstig van interne onderzoeken van de Belastingdienst. Aanvullend onderzoek is uitgevoerd bij twee eenheden Particulieren, waaronder de eenheid waar de aanleiding tot het onderzoek heeft plaatsgevonden, een eenheid Ondernemingen en een gemengde eenheid Particulieren en Ondernemingen. Eenheden van de directies Douane en Grote Ondernemingen zijn in het onderzoek buiten beschouwing gelaten.

1.2 Onderwerp

De Belastingdienst beschikt over een veelheid aan vertrouwelijke gegevens van belastingplichtige ingezetenen, die de Belastingdienst nodig heeft voor de uitvoering van zijn wettelijke taak, namelijk heffing, controle en inning van rijksbelastingen. Echter, voor andere organisaties en bedrijven vormt het gegevensbestand van de Belastingdienst een schat aan informatie. De burger mag verwachten dat deze informatie niet uitlekt. Beveiliging van en het zorgvuldig omgaan met vertrouwelijke gegevens wordt bovendien vereist op grond van de Wet Persoons-

[1] Informatiebeveiliging Belastingdienst, publicatiedatum 9 april 1997, Tweede Kamer 1996–1997, 25 290, nrs. 1–2.

registraties[1] en de Algemene Wet inzake Rijksbelastingen. Aan de stringente geheimhoudingsplicht die voor medewerkers van de Belastingdienst geldt, ligt ten grondslag dat belasting-plichtigen niet van het verstrekken van gegevens moeten worden weerhouden door de vrees dat die gegevens voor andere doeleinden worden gebruikt dan voor de eigenlijke taak van de Belastingdienst.

1.2.1 Risico's

Indien de Belastingdienst risico's ten aanzien van het zorgvuldig omgaan met vertrouwelijke gegevens onvoldoende beheerst, kan het vertrouwen van belastingplichtigen in de Belastingdienst worden geschaad en kan dit de bereidheid van belastingplichtigen om vrijwillig aan hun verplichtingen te voldoen nadelig beïnvloeden. Het belang van informatiebeveiliging neemt nog verder toe door:

- de klantgerichte benadering van de Belastingdienst. Dit betekent ondermeer integratie van processen en daardoor concentratie van taken bij één of meerdere medewerkers;
- toenemende elektronische gegevensuitwisseling met intermediairs en belastingplichtigen. Hierbij is het van belang de betrouwbaarheid en vertrouwelijkheid van gegevens te waarborgen;
- toenemende automatisering in combinatie met decentralisatie van processen. Dit kan verhoging van risico's van het onbevoegd kennis nemen dan wel manipuleren van gegevens betekenen.

Informatiebeveiliging, het waarborgen van integriteit en de wijze waarop medewerkers van de Belastingdienst dit in praktijk brengen, zijn daarom noodzakelijke voorwaarden voor het zorgvuldig omgaan met gegevens.

In haar eerdere onderzoek concludeerde de Rekenkamer dat de informatiebeveiliging bij de vijf onderzochte eenheden – waarvan één eenheid in het huidige onderzoek is betrokken – ernstige tekortkomingen vertoonde. Het betrof onder andere het slordig omgaan met wachtwoorden, het bij indiensttreding automatisch toekennen van leesrechten van vertrouwelijke gegevens aan medewerkers en vaak bewust niet aangebrachte functiescheidingen ten behoeve van het productieproces.

De Rekenkamer heeft ook eerder onderzoek gedaan naar het integriteitsbeleid bij de Rijksoverheid. In het in 1996 gepubliceerde rapport[2] over integriteit en het vervolg daarop in 1998[3] wees de Rekenkamer op de noodzaak van toenemende aandacht voor integriteit in de openbare sector en de ontwikkelingen – zoals versterkte aandacht voor klantgerichtheid – die daaraan ten grondslag lagen. In het vervolgonderzoek 1998 concludeerde de Rekenkamer dat de invoering van het integriteitsbeleid in alle sectoren van de rijksdienst vrij moeizaam verliep. Preventieve maatregelen bleken in opzet aanwezig te zijn, maar in de praktijk niet steeds uitgevoerd te worden.

1.2.2 Onderzoeksvragen

De Rekenkamer heeft de opzet en de uitvoering van het beleid ten aanzien van het omgaan met vertrouwelijke gegevens onderzocht. In het onderzoek zijn de volgende vragen aan de orde gekomen:

- welk beleid op het gebied van integriteit en informatiebeveiliging hanteert de Belastingdienst voor de bescherming van vertrouwelijke gegevens en welke maatregelen zijn er (voor)genomen ter uitvoering van dit beleid?
- op welke manier krijgt de uitvoering van bovengenoemde maatregelen in de praktijk gestalte en zijn daarbij tekortkomingen te onderkennen?
- op welke wijze heeft de organisatie inzicht in de werking van de

[1] Op ambtelijk niveau is gebruik gemaakt van de expertise van de Registratiekamer op dit terrein.
[2] «Integriteitsbeleid bij het Rijk: stand van zaken» TK 1995–1996, 24 655, nrs. 1–2.
[3] TK 1997–1998, 26 100, nrs. 1–2.

maatregelen en eventuele tekortkomingen en welke mogelijkheden zijn er om deze tekortkomingen op te heffen?

Tevens is voor informatiebeveiliging onderzocht of toezeggingen die de staatssecretaris in 1997 heeft gedaan zijn gerealiseerd. De toezeggingen hadden betrekking op de versterking van de beveiligingsorganisatie en van de interne controle en verbetering van de dagelijkse beveiligingspraktijk door investeringen in programmatuur.

1.3 Organisatie van de Belastingdienst

De staatssecretaris van Financiën is politiek verantwoordelijk voor het (functioneren van) het Directoraat-Generaal der Belastingen (DG der Belastingen). De Belastingdienst wordt geleid door de Directeur Generaal, daarbij ondersteund door 7 stafdirecties. Bij de Belastingdienst werken meer dan 30 000 mensen, verdeeld over ruim 80 eenheden en 7 douanedistricten. Onder de directies Particulieren en Ondernemingen ressorteren (landelijk gespreid) respectievelijk 15 – waaronder de eenheid Particulieren Buitenland – en 30 eenheden en 11 gecombineerde eenheden P/O. Behalve de vier onderzochte eenheden zijn de belangrijkste actoren in het kader van het onderzoek:

- DG der Belastingen, stafdirectie Planning, Financiën en Control, stafdirectie Personeel en Organisatie en stafdirectie Interne Accountantsdienst Belastingen;
- Belastingdienst Automatiseringscentrum en afdeling Eerstelijns Beheer & Exploitatie;
- Belastingdienst/Centrum voor Facilitaire dienstverlening;
- Belastingdienst/Centrum voor Kennis en Communicatie, verzorgt onder meer de zogenoemde dilemmatrainingen.

2 BELEID

2.1 Inleiding

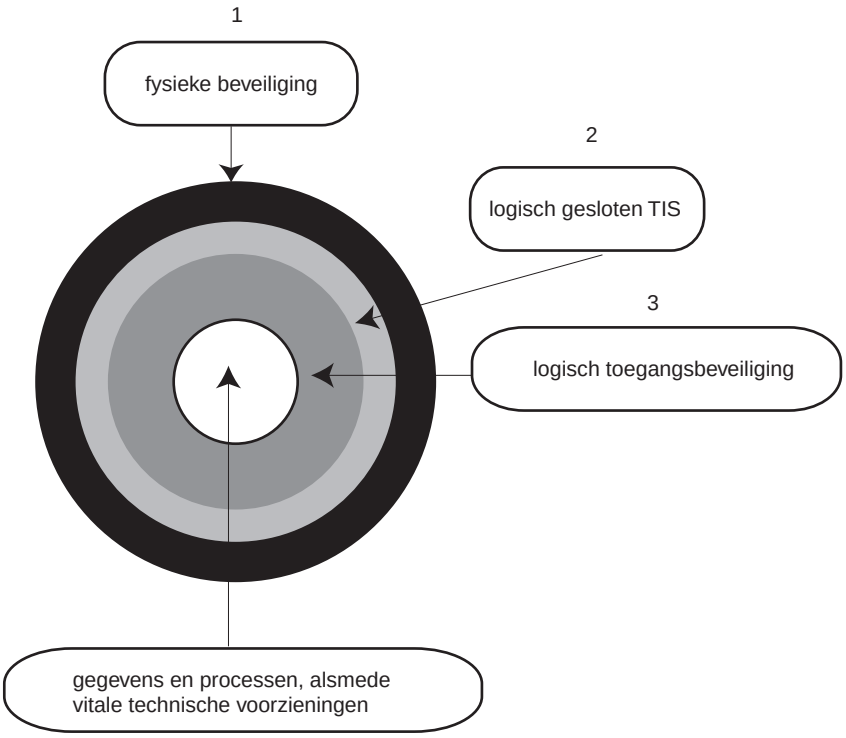
Met het beleid inzake het zorgvuldig omgaan met vertrouwelijke gegevens wordt in het kader van dit onderzoek bedoeld het beleid voor informatiebeveiliging en het integriteitsbeleid van de Belastingdienst. Het doel van informatiebeveiliging is de risico's ten aanzien van betrouwbaarheid, beschikbaarheid en vertrouwelijkheid van gegevens en gegevensverwerkende processen te beheersen en daardoor de privacy van belastingplichtigen te waarborgen. De legitimiteit van het openbaar bestuur berust op het vertrouwen van de burger, een vertrouwen dat gebaseerd is op de integriteit van het handelen van (medewerkers van) overheidsorganen. Voor de Belastingdienst geldt dat het bevorderen van integriteit betekent het scheppen van duidelijkheid over basiswaarden en uitgangspunten van de organisatie en het ertoe bijdragen dat medewerkers verantwoordelijkheid nemen voor professioneel handelen.

2.2 Beleid informatiebeveiliging

Het beleid voor informatiebeveiliging is vastgelegd in het Handboek Informatiebeveiliging Belastingdienst[1] (HIB). Het HIB geeft het strategisch beleidskader – het geformuleerde en het gewenste beleid op het gebied van informatiebeveiliging – en nadere richtlijnen ter invulling van dit kader.

De samenhang tussen de beveiligingsmaatregelen kan worden geïllustreerd aan de hand van het zogenaamde schillenmodel.

[1] HIB december 1996. Aanvullend beleid is later geformuleerd voor electronisch berichtenverkeer en voor de koppeling van ppc's aan netwerken.



Bron: Handboek Informatiebeveiliging Belastingdienst

De eerste beveiligingsschil wordt gevormd door de fysieke beveiliging. Deze is vooral gericht op het weren van onbevoegden uit gebouwen van de Belastingdienst. Onbevoegden mogen geen kennis nemen van de in de dossiers opgeslagen informatie en geen toegang krijgen tot de computerruimten en de daarin opgestelde apparatuur.
De tweede beveiligingsschil bestaat uit de logisch gesloten technische infrastructuur (TIS), die ervoor zorgt dat gegevensuitwisseling binnen de Belastingdienst wordt geïsoleerd van de buitenwereld. Onder de TIS wordt verstaan alle apparatuur, systeemprogrammatuur, netwerk- en datacommunicatie-faciliteiten. De derde beveiligingsschil bestaat uit de logische toegangsbeveiliging: de medewerker heeft slechts tot die gegevens toegang die nodig zijn voor het uitvoeren van zijn taak (het «need to know»-beginsel). Voor toepassing van dit beginsel is van belang dat medewerkers slechts toegangsrechten krijgen tot die informatiesystemen waarin de gegevens die nodig zijn voor de taak zich bevinden (autorisatiestructuur) en binnen de informatiesystemen slechts toegang hebben tot die gegevens die noodzakelijk zijn voor het uitvoeren van de taak. In het kader van dit onderzoek zijn alleen de rechten tot het raadplegen van gegevens en niet de rechten tot het muteren van gegevens als onderwerp van onderzoek meegenomen.

In het HIB staat een aantal aspecten genoemd dat het beveiligingsbewustzijn van de medewerkers moet ondersteunen:
- informatiebeveiliging dient in een functioneringsgesprek te worden besproken;
- bij het verstrekken van informatie dient het Voorschrift informatievoorziening (VIV) te worden toegepast;
- medewerkers zijn verplicht hun wachtwoorden en gebruikersnamen strikt geheim te houden, omdat anders anderen alle bevoegdheden van de medewerker krijgen.

Andere maatregelen om de (informatie)beveiliging te verbeteren zijn:
- alle medewerkers en bezoekers zijn verplicht een identificatiebewijs te dragen om onbevoegden in belastinggebouwen zichtbaar te maken;
- de clean-desk policy. Deze maatregel is integraal van toepassing op alle gegevens en documenten, die zich bij afwezigheid van de medewerker in een afgesloten ruimte dienen te bevinden;
- het instellen van een schermbeveiliging met wachtwoord. Dit is een waarborg om te voorkomen dat – wanneer de medewerker de werkplek verlaat – onbevoegden kennis kunnen nemen van de gegevens in (openstaande) informatiesystemen.

2.3 Beleid integriteit

De Belastingdienst is in 1985 gestart met de ontwikkeling van een integriteitbeleid en heeft dit in 1995 geïntensiveerd door meer integraal beleid te formuleren. Dit beleid is gebaseerd op regelgeving en communicatie over integriteit.

2.3.1 Regelgeving

Het betreft in eerste instantie regelgeving die voor alle rijksambtenaren geldt en waaraan de Belastingdienst in eigen voorschriften (Reglement Personeelsvoorschriften Belastingdienst) nadere invulling heeft gegeven.
- Plichtsverzuim
  Het overtreden van beveiligingsregels, het schenden van de geheimhoudingsplicht en het verrichten van bepaalde nevenwerkzaamheden (in geval van belangenverstrengeling) leiden tot plichtsverzuim. Het hoofd van de eenheid dient – conform het voorschrift buitengewone voorvallen – de directie in te lichten indien zich een ernstige integriteitsinbreuk heeft voorgedaan.
- Nevenwerkzaamheden
  Uitgangspunt is dat de integriteit van de ambtenaar en de dienst gewaarborgd moeten worden. Dit houdt in dat er geen sprake mag zijn van belangenverstrengeling en dat het aanzien van het ambt en de organisatie niet beschadigd mogen worden. Ten aanzien van nevenwerkzaamheden die de belangen van de dienst kunnen raken (belangenverstrengeling) bestaat een meldingsplicht: de medewerker die nevenwerkzaamheden verricht of voornemens is te gaan verrichten dient dit aan het Hoofd van de eenheid te melden. De eenheid dient van de beschikkingen (zowel toestemming als afwijzing) een registratie bij te houden en ieder jaar dient de beschikking getoetst te worden aan het bestaand beleid.
- Verklaring omtrent gedrag
  In 1996 heeft de Belastingdienst besloten dat het aanstellen van nieuwe medewerkers pas mag plaatsvinden als een verklaring omtrent gedrag is overlegd. Deze maatregel geldt ook voor tijdelijke medewerkers, zoals uitzendkrachten en stagiaires.
- Geheimhoudingsverklaring
  Ambtenaren zijn verplicht tot geheimhouding over wat hen in hun functie ter kennis is gekomen. Bij aanstelling wordt een geheimhoudingsverklaring getekend en recent is het afleggen van de eed of gelofte bij de Belastingdienst wederom ingesteld. De geheimhoudingsplicht geldt ook voor tijdelijke medewerkers, zoals uitzendkrachten en stagiaires.

2.3.2 Communicatie over integriteit

Naast voorschriften heeft de Belastingdienst zijn integriteitsbeleid gebaseerd op communicatie over integriteit, omdat regels alleen

onvoldoende het gedrag van medewerkers bepalen. Gedrag moet gestuurd worden door elkaar hierop aan te spreken.

- integriteitsprogramma
  Het rapport «Integriteit: een zaak van professionele verantwoordelijkheid» was in 1995 de basis voor het integriteitsprogramma. De uitvoering van het programma dient onder andere gestalte krijgen door het volgen van dilemmatrainingen en door communicatie over integriteit.
- Basiswaarden Belastingdienst
  Eind 1997 zijn de «Basiswaarden Belastingdienst» vastgesteld. Deze basiswaarden – geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid – vormen de kern van de wijze waarop de Belastingdienst ambtelijke integriteit benadert.
- Vertrouwenspersoon Integriteit Belastingdienst
  Bij de Belastingdienst wordt het waarborgen van de integriteit primair als een verantwoordelijkheid van de medewerker en van het lijnmanagement gezien. Ter uitvoering van de motie Kamp heeft de minister van BZK[1] de ministeries als richtlijn gegeven een vertrouwenspersoon integriteit aan te stellen. Per februari 1999 heeft de Belastingdienst een vertrouwenspersoon integriteit aangesteld in de persoon van een voormalig doelgroepdirecteur.

2.3.3 Maatregelen op personeelsgebied

Daarnaast heeft de Belastingdienst maatregelen op personeelsgebied getroffen om integriteit te bevorderen of onder de aandacht te brengen van nieuwe en/of tijdelijke medewerkers. Het betreft:

- Functieroulatie
  Functieroulatie is één van de maatregelen om aantasting van de integriteit te voorkomen. Het mobiliteitsstreven van de Belastingdienst is erop gericht om medewerkers eens in de drie jaar (deurwaarders en klantmanagers) en eens in de vijf jaar (medewerkers behandelteams) van functie of ambtsgebied te laten wisselen.
- Opleidingen
  Integriteit is als apart aspect in de startopleiding van nieuwe medewerkers opgenomen.

2.4 Nieuwe instrumenten

De conclusie van de Rekenkamer in haar rapport 1997 dat het beleid in opzet goed te noemen was, maar dat de werking van de maatregelen voor verbetering vatbaar was, heeft geleid tot een aantal nieuwe instrumenten zoals de speerpuntonderzoeken en de beveiligingsmonitor.

- in 1997 en in 1998 zijn speerpuntonderzoeken gehouden naar onder meer de logische toegangsbeveiliging en de logisch gesloten technische infrastructuur (TIS). Deze onderzoeken zijn gericht op de werking van de beveiligingsmaatregelen en worden uitgevoerd door FIB-2 (functionaris informatiebeveiliging doelgroepdirectie) en FIB'S-3 (functionarissen informatiebeveiliging eenheid).
- de Beveiligingsmonitor is een instrument waarmee door middel van een aantal (subjectieve) vragen het beveiligingsbewustzijn van medewerkers wordt gemeten. De Beveiligingsmonitor geeft een representatief landelijk beeld van kennis, attitude en gedrag van medewerkers van de Belastingdienst ten aanzien van beveiliging.

[1] Bij brief van 19 februari 1997.

3 UITVOERING BELEID INFORMATIEBEVEILIGING

3.1 Inleiding

De Rekenkamer heeft onderzocht hoe het beleid voor informatiebeveiliging in de praktijk gestalte heeft gekregen. De bevindingen hebben betrekking op informatie afkomstig van de vier in het Rekenkameronderzoek betrokken eenheden en op informatie afkomstig van interne onderzoeken van de Belastingdienst zelf, zoals de speerpuntonderzoeken en de Beveiligingsmonitor.

3.2 Beveiligingsorganisatie

Het lijnmanagement van een eenheid is verantwoordelijk voor het informatiebeveiligingsbeleid en -niveau. Ter versterking van de beveiligingsorganisatie zijn de volgende toezeggingen van de staatssecretaris uit 1997 gerealiseerd:

- het aspect informatiebeveiliging is opgenomen in de verschillende basisopleidingen (teamleider, management, controller, pfc-medewerker);
- de functie lokaal informatiemanagement is bij het plaatsvervangend hoofd van de eenheid neergelegd. De invoering van nieuwe systemen op de eenheid, inclusief aanpassingen in de organisatie en aspecten beveiliging en AO/IC vallen onder zijn verantwoordelijkheid.

Overleg

Er zou aandacht komen voor meer en gestructureerd overleg tussen de beveiligingsfunctionarissen (FIB). Dit bleek bij de twee onderzochte eenheden ressorterend onder de directie Particulieren op eenheidsniveau geen gestalte te hebben gekregen. De FIB'S-3 op de eenheden hadden noch onderling met andere FIB'S-3 uit de regio gestructureerd overleg, noch met de beveiligingsfunctionaris op directieniveau (FIB-2).
Uit informatie van de Belastingdienst zelf bleek dat bij geen van de 15 eenheden Particulieren overleg tussen beveiligingsfunctionarissen is ingesteld. Volgens de Belastingdienst bestaat een dergelijk overleg wel voor de eenheden Ondernemingen respectievelijk de gecombineerde eenheden Ondernemingen/Particulieren.

Lokaal beveiligingsplan

De eenheden dienen een lokaal informatiebeveiligingsplan op te stellen. Van de vier onderzochte eenheden beschikten twee eenheden over een recent informatiebeveiligingsplan, één eenheid over een beveiligingsplan uit 1995 en één eenheid gaf aan dat met de directie afspraken waren gemaakt in de vorm van speerpunten. Daarnaast bleek dat twee van de vier onderzochte eenheden een beveiligingschecklist of – kaart hadden ontwikkeld. De twee andere eenheden hadden «huisregels» opgesteld waarin aspecten van informatiebeveiliging aan de orde kwamen.

Verantwoordelijkheden eenheid – Belastingdienst Automatiseringscentrum (BAC)/ Eerstelijns Beheer & Exploitatie (EBE)

Iedere eenheid is zelf verantwoordelijk voor de mate van informatiebeveiliging, maar steunt daarbij op de kwaliteit van werkzaamheden van andere organisatieonderdelen zoals het BAC/EBE. Zo worden de interne controles op informatiebeveiliging voor 70% uitgevoerd door het BAC/EBE, voor 10% door Belastingdienst/Centrum voor Facilitaire Dienstverlening (B/CFD) en voor 20% door de eenheden zelf.
De Interne Accountantsdienst Belastingen (IAB) heeft medio 1999

aangegeven dat er nog steeds onduidelijkheid bestaat met name op het gebied van de interne controle tussen de eenheden en het BAC/EBE. De noodzaak om opzet en uitvoering van de interne controle verder op elkaar af te stemmen werd nogmaals onderstreept. Voorts beschouwde de IAB de logische toegangsbeveiliging als nog niet optimaal waardoor risico's ten aanzien van de vertrouwelijkheid van gegevens hoger zijn dan het voorgestane niveau. Er bestaat op dit punt verschil van mening of dit de verantwoordelijkheid van de eenheid of van BAC/EBE is.

Interne controle op beheer en beveiliging

De versterking van de interne controle heeft geleid tot speerpunt-onderzoeken die in 1997 en in 1998 zijn gehouden naar onder meer de logische toegangsbeveiliging en de logisch gesloten technische infrastructuur (TIS). Deze onderzoeken zijn gericht op de werking van de beveiligingsmaatregelen en worden uitgevoerd door FIB-2 en FIB'S-3 op de eenheden. Uit de conclusie van de eindrapportage speerpuntonderzoek 1998[1] blijkt dat in dat jaar:

- eenheden voor de toegangscontrole geen overzicht hadden over de juistheid en volledigheid van de aangevraagde en toegekende autorisaties;
- medewerkers zich mogelijk onvoldoende bewust waren van de vertrouwelijke aard van de gegevens waarmee ze dagelijks werken;
- de naleving van clean desk policy en de draagplicht van identificatiebewijzen door medewerkers in de meeste gevallen te wensen overliet. Daarnaast bleek dat op veel werkplekken de schermbeveiliging niet was geactiveerd en indien dit wel het geval was dan veelal niet in combinatie met een wachtwoord.

Bij drie van de vier onderzochte eenheden is gebleken dat de uitvoering van interne controles op beheer en beveiliging achterstanden vertonen, dan wel niet of nauwelijks worden uitgevoerd. Bij twee van deze onderzochte eenheden is de FIB-3 functie langere tijd vacant geweest. FIB'S-3 zijn de eerst aangewezenen om deze controles uit te voeren.

De Rekenkamer stelt vast dat in het kader van de versterking van de interne controle het uitvoeren van de speerpuntonderzoeken een toegevoegde waarde heeft. Tegelijkertijd blijkt uit de resultaten van deze speerpuntonderzoeken alsmede uit de resultaten van de hiervoor vermelde IAB-controles duidelijk dat de beoogde versterking van de interne controle nog niet in voldoende mate tot stand is gekomen.

3.3 Toegang tot gegevens

3.3.1 Fysieke toegang

Om te waarborgen dat onbevoegden geen toegang hebben tot vertrouwelijke gegevens is het van belang de fysieke toegangsbeveiliging door middel van toegangsbeperkende maatregelen te regelen. De noodzaak tot fysieke toegangsbeveiliging is mede afhankelijk van het belang en de kwetsbaarheid van de opgeslagen en te verwerken gegevens en informatiesystemen en apparatuur. Daarom wordt er onderscheid gemaakt in zones: openbare ruimten, gemeenschappelijke ruimten, dienstruimten met afzonderlijke zones per eenheid en kritische ruimten. De laatste zone betreft bijvoorbeeld de computerruimte en de technische ruimten die noodzakelijk zijn voor het primaire proces.

Bij vrijwel alle gebouwen van de Belastingdienst worden de fysieke beveiligingswerkzaamheden uitbesteed. De ingehuurde medewerkers hebben meestal – met uitzondering van de computerruimte – volledige

[1] Eindrapportage speerpuntenonderzoek 1998, datum 19 november 1998. De (eind)-rapportage 1999 was ten tijde van het onderzoek nog niet beschikbaar.

toegang. Voor de directies Particulieren en Ondernemingen is het beeld als volgt:

Directie	Aantal gebouwen	Beveiliging uitbesteed	Volledige toegang	Toegang tot computer-ruimte
Particulieren	52	49 (94%)	48 (92%)	28 (54%)
Ondernemingen	42	40 (95%)	39 (93%)	22 (52%)

Volgens de Rekenkamer wordt het risico van het raadplegen van vertrouwelijke gegevens door onbevoegden hierdoor vergroot. Om de beveiliging te waarborgen zijn volgens de Belastingdienst aanvullende maatregelen genomen. Het beveiligingsbedrijf zorgt ervoor dat medewerkers een geheimhoudingsverklaring hebben getekend en dat zij beschikken over een verklaring omtrent gedrag. Op dit moment vindt nog geen controle op naleving van deze regeling plaats.

Uit het speerpuntonderzoek 1998 is gebleken dat het risico van onbevoegd binnentreden bestaat doordat het beleid niet wordt afgedwongen door technische voorzieningen en doordat deuren te lang openstaan.
Bij de in het onderzoek betrokken eenheden zijn toegangsbeperkende maatregelen aangetroffen. Uit eigen waarneming bleek dat niet overal even strak de hand wordt gehouden aan de toepassing van de regels.

3.3.2 Logische toegangsbeveiliging

Voor het raadplegen van vertrouwelijke gegevens blijkt het «need to know» beginsel niet afdoende door de systemen te worden ondersteund. Dit heeft te maken met de volgende zaken:
- de centrale informatiesystemen[1], waartoe bijna alle medewerkers toegang hebben, bevatten gegevens van alle belastingplichtigen in Nederland, terwijl medewerkers deze gegevens slechts incidenteel nodig hebben voor hun functie;
- een beperking tot het takengebied is door de structuur en opbouw van huidige systemen niet mogelijk. Het is dan ook niet mogelijk een medewerker slechts toegang te geven tot die gegevens in het systeem die hij voor zijn taakuitoefening nodig heeft.

Door de wijze van autoriseren wordt het «need-to-know» beginsel voor het raadplegen van gegevens niet toegepast:
- raadpleegrechten worden – in tegenstelling tot muteerrechten – vrijwel aan alle medewerkers automatisch toegekend.

Daardoor is het, met uitzondering van de gegevens van een beperkte groep belastingplichtigen die afgeschermd zijn, zeer eenvoudig voor alle medewerkers in behandelteams en in de ondersteunende teams om vertrouwelijke gegevens te raadplegen.

Ter verbetering van de dagelijkse beveiligingspraktijk heeft de staatssecretaris in 1997 toegezegd dat er investeringen in de programmatuur zouden plaatsvinden. Deze hebben betrekking op:
- synchronisatie van wachtwoorden waardoor medewerkers minder wachtwoorden nodig hebben of zelfs met één wachtwoord toekunnen. De huidige stand van zaken is dat hiervoor nu voorbereidende werkzaamheden zijn getroffen;
- het invoeren van een auditprogramma voor UNIX. Dit auditprogramma is vrijwel operationeel. Het in 1994 aangeschafte programma kampt echter nog steeds met problemen.

De vertraging in de uitvoering hangt volgens de Belastingdienst samen met de inspanningen in het kader van de euro- en milleniumproblematiek.

[1] Zie bijlage I waarin voor de belangrijkste vigerende informatiesystemen wordt aangegeven welke gegevens deze bevatten.

3.3.2.1 Autorisatieregime

De logische toegangsbeveiliging (LTB) wordt ondersteund door de autorisatiestructuur en het autorisatieregime. Met dit laatste wordt gedoeld op de naleving van procedures voor het aanvragen, toekennen, implementeren, intrekken van en controleren hierop van autorisaties. De teamleider kent een autorisatie toe en dient de aanvraag in bij de toepassingsbeheerder, die na controle EBE de opdracht geeft de medewerker te autoriseren. De FIB-3 wordt in voorkomende gevallen geconsulteerd. Controle vindt plaats door de FIB-3 en door middel van interne controles.

Medewerkers hebben voor de drie meest gebruikte informatiesystemen zeven wachtwoorden nodig. De aard, omvang en complexiteit van de informatiesystemen leiden in de praktijk tot (te) ruime autorisaties en maakt het onderhouden van de autorisatiestructuur een moeizame aangelegenheid. Enkele jaren geleden is om het onderhoudsprobleem te ondervangen de Logische Toegangsbeveiligings (LTB)-tool ontwikkeld. Deze bleek niet in alle gevallen te werken wegens beperkingen in het aantal te verwerken autorisaties. Eenheden werken daarom soms met een eigen toepassing. Recentelijk is gebleken dat bij de omzetting van de LTB-tool eerdere bevindingen en voorgestelde nieuwe functionaliteiten niet zijn meegenomen, waardoor het instrument niet gebruikersvriendelijk dan wel onbruikbaar is. Volgens de Belastingdienst is in een nieuwe tool nog niet voorzien. Prioriteit wordt gegeven aan het afstemmen van verschillen in autorisatiestructuur van de informatiesystemen.

Ten aanzien van het autorisatieregime waren de belangrijkste bevindingen:
- bij de vier eenheden waren bevoegdheden van medewerkers overeenkomstig functies en taken vastgelegd in autorisatietabellen. De aanwezige autorisatietabellen bleken bij twee van de onderzochte eenheden niet actueel te zijn. Bij alle onderzochte eenheden zijn de medewerkers te ruim geautoriseerd;
- autorisaties van medewerkers die niet meer in dienst zijn of op een andere eenheid danwel in een ander team zijn geplaatst, worden (te) laat uit autorisatietabellen verwijderd en autorisaties worden in enkele gevallen niet eens geblokkeerd;
- bij alle eenheden bleken toepassingsbeheerders en soms ook faciliteitenbeheerders geautoriseerd voor toegang tot gebruikersfuncties en productiegegevens, waardoor zij beschikken over ruimere autorisaties dan zij voor de uitoefening van hun functie nodig hebben;
- de controles hierop vertonen bij drie van de vier onderzochte eenheden achterstanden en/of laten te wensen over;
- recentelijk is men bij de vier eenheden gestart met opschoningsacties van gebruikersautorisaties. Ten tijde van het onderzoek waren deze acties nog gaande.

3.3.2.2 Authenticiteit

Het vaststellen van de authenticiteit van de gebruiker wordt bemoeilijkt indien gemeenschappelijke wachtwoorden en gebruikersnamen worden gebruikt. Dit bleek bij alle onderzochte eenheden het geval te zijn, bijvoorbeeld bij bepaalde informatiesystemen waarvoor per eenheid slechts enkele autorisaties zijn afgegeven en bij tijdelijke medewerkers (vanwege de lange aanvraagprocedure). Ten aanzien van de groep tijdelijke medewerkers bleek bovendien dat bij drie van de vier eenheden geen duidelijke bevoegdheidsafbakening was vastgelegd in de functiebeschrijving. Het hoge ziekteverzuim op enkele eenheden (10–12%) brengt

voorts met zich mee dat collega's (tijdelijk) op autorisaties van zieke medewerkers werken.

3.3.2.3 Controleerbaarheid van raadplegen van vertrouwelijke gegevens

Van groot belang is dat er een controlespoor achterblijft (logging) waardoor kan worden nagegaan of medewerkers onbevoegd vertrouwelijke gegevens raadplegen. Geen van de huidige lokale systemen maakt het mogelijk om achteraf vast te stellen welke medewerkers welke informatie hebben geraadpleegd. Voor de centrale systemen zou dit wel mogelijk zijn, zij het dat de controlegegevens moeilijk toegankelijk zijn en daarom niet worden teruggekoppeld naar de eenheden.

3.4 Omgaan met beveiliging

De effectiviteit van beveiligingsregels wordt niet alleen bepaald door de mate waarin de medewerkers deze regels kennen, maar meer nog door de mate waarin zij zich er naar gedragen. Uit de Beveiligingsmonitor 1998 is naar voren gekomen dat:

- 71% van de medewerkers wel eens de werkplek verlaat zonder beveiliging van de pc;
- 52% van de medewerkers wel eens aan het eind van de dag dossiers niet vergrendelt (clean desk);
- 36% van de medewerkers wel eens gebruik maakt van wachtwoord van een collega en
- 27% van de medewerkers wel eens onbevoegd bestanden raadpleegt.

Uit de Beveiligingsmonitor kwam ook naar voren dat de indruk bestond dat aan beveiliging weinig prioriteit wordt verleend, zowel door medewerkers als management. Ook vertoonden leidinggevenden onvoldoende voorbeeldgedrag.
Voor de divisie Ondernemingen[1] gaven deze resultaten aanleiding vervolgacties te starten om het beveiligingsbewustzijn van management en personeel te verbeteren.

Voor de in het onderzoek betrokken eenheden is in het overzicht weergegeven het percentage van de medewerkers dat in 1998 aangaf het betreffende gedrag te vertonen.

Eenheid	Laten rondslingeren wachtwoorden	Gebruik wachtwoord van collega's	Onbevoegd bestanden raadplegen	Werkplek verlaten zonder schermbeveiliging
1	27%	30%	15%	13%
2	17%	43%	20%	11%
3	14%	17%	15%	25%
4	26%	32%	21%	21%

De uitvoering van het informatiebeveiligingsbeleid op een aantal andere aspecten kreeg bij de vier onderzochte eenheden op de volgende wijze gestalte:

- bij één van de vier onderzochte eenheden was informatiebeveiliging een aandachtspunt in het functioneringsgesprek;
- drie van de vier eenheden hebben het Voorschrift Informatieverstrekking vertaald in eigen voorschriften. Bij de onderzochte eenheden bleek dat aan de naleving van het voorschrift in de praktijk over het algemeen redelijk tot de goed de hand wordt gehouden en dat er regelmatig controles op worden gehouden;
- de toepassing van de procedure voor het gebruik van wachtwoorden bij afwezigheid/ziekte van collega's was niet waterdicht en wachtwoorden van collega's waren bekend of makkelijk te achterhalen.

[1] Nota Risicobeheersing, mei 1999.

Uit de Beveiligingsmonitor kwam naar voren dat de voorschriften voor clean desk policy en vergrendeling van pc's als onvoldoende werkbaar worden beschouwd. Ook uit eigen waarneming op de eenheden is gebleken dat deze maatregelen in de praktijk niet altijd worden nageleefd. Bij bepaalde informatiesystemen zoals Inkomstenbelasting-systeem (IBS), Geautomatiseerde Ontvangersadministratie (GOA) en Beheer van relaties (BVR) werkt de schermbeveiliging vaak niet omdat deze wordt geblokkeerd door het systeem zelf. Het probleem hierbij is dat medewerkers dit vaak niet weten en bij het verlaten van de werkplek vertrouwen op de ingestelde schermbeveiliging en niet het werkstation hebben afgesloten. Dit probleem is bekend binnen de Belastingdienst en zal met de volgende opschoningsactie worden meegenomen.
Bij het niet naleven van de cleandeskpolicy werd als voornaamste belemmering genoemd dat men niet de beschikking had over afsluitbare kasten of dat de kasten open moesten blijven vanuit hygiënisch (schoonmakers) of veiligheidsoogpunt (brandweer). Medewerkers – gewezen op de clean desk policy – reageerden vaak met de vraag naar het nut van het opbergen van gegevens in kasten die niet afsluitbaar zijn. Dit maakte het moeilijker voor de leidinggevenden om de naleving van deze maatregel te handhaven.

Ten slotte is het van belang dat bekend is welke zwakke punten tot incidenten hebben geleid. Bij DG der Belastingen bestaat de indruk dat de registratie hiervan – waarmee men in 1998 is begonnen – bij de eenheden niet goed loopt. Er worden enerzijds doublures geconstateerd en anderzijds bestaat er twijfel of alle incidenten gemeld worden. Dat betekent dat er een onduidelijk beeld is, waardoor de beoogde leereffecten niet bereikt worden en waardoor het onzeker is of verbeteracties zullen plaatsvinden.

3.5 Conclusie

Ten opzichte van de situatie waarover de Rekenkamer in 1997 heeft gerapporteerd is een aantal positieve ontwikkelingen te constateren. Deze hebben betrekking op verbeteringen in de organisatie van de informatiebeveiliging en nieuwe maatregelen en instrumenten als de speerpuntonderzoeken en het in gebruik nemen van de Beveiligingsmonitor. Tegelijkertijd geven de uitkomsten van zowel de speerpuntonderzoeken als de Beveiligingsmonitor aan dat de in gang gezette maatregelen nog onvoldoende weerslag in de praktijk hebben gekregen. De Rekenkamer heeft in het onderzoek bij de eenheden tekortkomingen in de uitvoering van het beleid voor informatiebeveiliging geconstateerd. Deze hebben betrekking op de organisatie van de informatiebeveiliging, zoals onduidelijkheid rond verantwoordelijkheden en achterstanden bij interne controle, en op de toegang tot gegevens. Er wordt te ruim geautoriseerd mede om productiedoelstellingen te realiseren. Het autorisatieregime wordt op vrij grote schaal in de praktijk om praktische redenen omzeild. Over de authenticiteit van gebruikers is niet in alle gevallen zekerheid te geven. Deze tekortkomingen en de inrichting van de informatiesystemen houdt in dat vrijwel alle medewerkers vertrouwelijke gegevens van vrijwel alle belastingplichtigen kunnen raadplegen. Het risico dat vertrouwelijke gegevens onbevoegd kunnen worden geraadpleegd is door bovengenoemde tekortkomingen en de wijze waarop medewerkers omgaan met beveiliging in de praktijk aanwezig.

Tengevolge van het ontbreken van controle op onbevoegd raadplegen en een incomplete incidentenregistratie is er naar de mening van de Rekenkamer sprake van onvoldoende risicobeheersing.

4 UITVOERING INTEGRITEITSBELEID

4.1 Inleiding

De Rekenkamer heeft onderzocht op welke wijze het integriteitsbeleid in de praktijk gestalte heeft gekregen. De bevindingen hebben betrekking op informatie afkomstig van de vier in het Rekenkameronderzoek betrokken eenheden en op informatie afkomstig van de Belastingdienst zelf, zoals de audits uitgevoerd door de IAB en onderzoek van de directie Personeel en Organisatie van de Belastingdienst (POB).

4.2 Regelgeving

4.2.1 Plichtsverzuim

Uit de afschriften van disciplinaire maatregelen die de Rekenkamer van het ministerie ontvangt, is af te leiden dat in de periode 1996–1998 in relatie tot dit onderzoek:

- in zes gevallen het verstrekken van vertrouwelijke informatie heeft geleid tot een disciplinaire maatregel, variërend van een berisping tot ontslag;
- in dertien gevallen nevenwerkzaamheden werden verricht die niet waren toegestaan of waarbij de voorwaarden werden overtreden. Dit werd in het algemeen bestraft met ontslag danwel voorwaardelijk ontslag.

Bij beide vormen van plichtsverzuim bleek in tien van de negentien gevallen dat het plichtsverzuim door klachten van derden of anonieme tips was ontdekt.

> *Ernstige integriteitsinbreuken bleken zich – naast de inbreuk die de aanleiding voor het Rekenkameronderzoek vormde – ook bij twee andere in het onderzoek betrokken eenheden voor te doen of in het recente verleden te hebben voorgedaan. In één geval blijkt het eveneens te gaan om het onbevoegd raadplegen van vertrouwelijke gegevens ten eigen bate. Bij de derde eenheid ging het om een andere vorm van plichtsverzuim, waarbij wel speelde dat in eerste instantie de (verboden) nevenwerkzaamheden niet bekend waren.*

Daarnaast is geconstateerd dat alle onderzochte eenheden de nieuwsgierigheid van nieuwe of tijdelijke medewerkers naar vertrouwelijke gegevens van familie, kennissen of buren in veel gevallen door de vingers wordt gezien. De gedachte erachter is dat het toch niet gecontroleerd kan worden en dat bovendien de nieuwsgierigheid na een paar maanden bevredigd is. Deze gegroeide praktijk is overigens geen beleid van de Belastingdienst.

Tevens is bij de onderzochte eenheden naar voren gebracht dat er behoefte aan duidelijkheid over de richtlijnen bestaat en dat maatschappelijk achterhaalde richtlijnen zouden moeten worden aangepast. Met dit laatste wordt bijvoorbeeld gedoeld op het verbod om bedrijfsmiddelen, zoals laptop, telefoon en kopieerapparaat, voor privé-doeleinden te gebruiken. Bovendien bleek dat er geen uniforme invulling wordt gegeven aan het toezien op de naleving hiervan.

4.2.2 Nevenwerkzaamheden

In 1997 heeft de IAB in opdracht van de directeur Personeel en Organisatie (POB) een audit uitgevoerd naar de wijze waarop het (toenmalig) beleid omtrent nevenactiviteiten werd toegepast binnen de Belastingdienst. Eén van de conclusies van de IAB hield in dat het aantal geregistreerde

meldingen van nevenwerkzaamheden lager was dan het aantal feitelijk uitgevoerde nevenwerkzaamheden.
Uit een recent uitgevoerde analyse van de directie POB op aangemelde nevenactiviteiten en daarop al dan niet verleende toestemming bleek dat de huidige registratie van nevenwerkzaamheden niet uniform en consistent is. Aanleiding voor deze analyse was het feit dat de DG der Belastingen meer dan incidenteel signalen had gekregen op grond waarvan hij concludeerde dat ten aanzien van niet-verboden nevenwerkzaamheden sprake kon zijn van belangenverstrengeling. De analyse van POB wees verder uit dat voor 1012 meldingen van nevenwerkzaamheden van de directies Particulieren en Ondernemingen die nader zijn onderzocht er bij 105 toegestane nevenwerkzaamheden op het eerste gezicht risico van belangenverstrengeling aanwezig zou kunnen zijn. Het gaat dan bijvoorbeeld om het voeren van een administratie voor het bedrijf van de partner, of het drijven op kleine schaal van een handel/nering. Daarnaast bleek in 68 gevallen de omschrijving van de aard of de omgeving waarin de nevenwerkzaamheid wordt uitgevoerd vragen op te roepen. Een voorbeeld hiervan is de omschrijving «werkzaamheden voor een onderneming».

Het Rekenkameronderzoek bij de vier eenheden wees uit dat bij twee van de vier eenheden geen volledig overzicht bestond van de feitelijk uitgevoerde nevenwerkzaamheden. Daarnaast bleek dat een aantal nevenwerkzaamheden, voor zover deze in verband staan met de functievervulling, de belangen van de dienst zouden kunnen raken.

De mogelijkheid bestaat om aan de toestemming de nevenwerkzaamheden te verrichten voorwaarden te verbinden, zowel ten aanzien van de inhoud als de tijdsduur.
In geval van de aanleiding voor dit onderzoek waren nevenwerkzaamheden onder voorwaarden toegestaan. Toen de aard hiervan veranderde is dit echter niet gemeld.
De Belastingdienst hanteert inmiddels – ten gevolge van de aanleiding tot het onderzoek – als beleid dat geen nevenwerkzaamheden meer mogen worden verricht bij incassobureaus. Het Reglement Personeelsvoorschriften Belastingdienst zal dienovereenkomstig worden aangepast.

Bij het verlenen van toestemming voor nevenwerkzaamheden onder voorwaarden (in werkzaamheden en/of in tijdsduur) speelt ook de ontwikkeling van de organisatie een rol. Enkele jaren geleden was dit bijvoorbeeld het geval toen de gemeenten zelf de heffing en inning van de gemeentelijke Onroerende Zaakbelasting gingen uitvoeren. Voor de deurwaarders van de Belastingdienst betekende dit een vermindering van werkzaamheden. Medewerkers met onvoldoende toekomstperspectief worden daarom in bepaalde gevallen gestimuleerd om nevenwerkzaamheden te verrichten waardoor de kansen op de arbeidsmarkt worden vergroot en men op termijn kan uitstromen. Hierdoor kan een spanningsveld ontstaan tussen het belang van de organisatie en het toestaan van nevenwerkzaamheden die de belangen van de dienst kunnen raken. Een beoordeling of toestemming voor de nevenwerkzaamheden kan worden gegeven wordt dan bemoeilijkt.

4.2.3 Verklaring omtrent gedrag en geheimhoudingsverklaring

Vaste medewerkers beschikken over een verklaring omtrent gedrag en tekenen bij aanstelling een geheimhoudingsverklaring. Recent is opnieuw ingesteld dat eed of belofte wordt afgelegd. Voor uitzendkrachten is met twee uitzendorganisaties een mantelcontract gesloten, waarin is opgenomen dat de uitzendorganisatie er voor zorg draagt dat de medewerkers die bij de Belastingdienst worden ingezet een verklaring

omtrent gedrag bezitten. Hetzelfde geldt voor de geheimhoudingsverklaring. De IAB heeft in juli 1998 geconcludeerd dat de eenheden er geen zicht op hebben wie de afspraken met de uitzendorganisaties bewaakt; men gaat er vanuit dat uitzendbureaus hun afspraken in het contract nakomen.

Daarnaast constateerde de IAB dat de normen die door de gemeenten gehanteerd worden bij de afgifte van de verklaring niet altijd voldoen aan de verwachtingen die leven bij de Belastingdienst. Voorgesteld werd om voor de verklaring omtrent gedrag een aantal basisnormen vast te stellen die aan de behoefte van de Belastingdienst voldoen en om in overleg met de Vereniging van Nederlandse Gemeenten (VNG) zorg te dragen voor een landelijke toepassing van deze basisnormen. Onlangs is het overleg hierover gestart.

Uit het Rekenkameronderzoek op betrokken eenheden bleek dat de maatregelen voor tijdelijk personeel in de praktijk onvoldoende worden nageleefd.

> *Zo bleek op een eenheid dat bij 71% van de 163 uitzendkrachten geen geheimhoudingsverklaring was aangetroffen. Naar de mening van een andere eenheid, waarbij 33 tijdelijke medewerkers werden ingezet, werd met zowel de geheimhoudingsverklaring als de verklaring omtrent gedrag te vrijblijvend omgegaan. Een teamleider van een derde eenheid (42 tijdelijke medewerkers) gaf aan dat hij – bij het ontbreken van geheimhoudingsverklaringen – zelf verklaringen heeft opgesteld en heeft laten ondertekenen.*

4.3 Communicatie over integriteit

4.3.1 Integriteitsprogramma

Het proces van bewustwording, verantwoordelijkheid, onderlinge verantwoording en vaardigheidsontwikkeling had eind 1997 zijn beslag moeten krijgen. Inmiddels is gebleken dat dit niet is gelukt. Als mogelijke oorzaak wordt aangegeven dat de eerste fase (dilemmatraining voor het management) een verplichtend karakter had en centraal gefinancierd was. De vervolgactiviteiten zijn daarentegen niet voorgeschreven en moeten uit reguliere budgetten bekostigd worden. Bij de onderzochte eenheden werden capaciteits-beslag en/of afstemmingsproblemen met het Belastingdienst/Centrum voor Kennis en Communicatie als oorzaken genoemd.

4.3.2 Dilemmatrainingen

Op basis van een landelijk overzicht van de periode 1996–1999 waarin is aangegeven welke activiteiten in het kader van het integriteitsprogramma hebben plaatsgevonden kan worden geconstateerd dat:

- nog niet bij alle eenheden van directies Particulieren en Ondernemingen het management dilemmatraining had gevolgd. Voor de 15 eenheden Particulieren bleek dat bij 9 het management nog geen training had gevolgd;
- bij de directie Ondernemingen in 1999 80 van de ongeveer 400 deurwaarders dilemmatraining hebben gevolgd en dat enkele teams een verkorte training of een introductiedag hebben gehad. Ook is er voor deze directie een video ontwikkeld waarin aan de hand van praktijkvoorbeelden dilemma's kunnen worden besproken;
- volgens het overzicht bij de directie particulieren alle deurwaarders, hun direct leidinggevenden en vrijwel alle klantendiensten in 1997 op dilemmatraining zijn geweest.

Bij de vier in het Rekenkameronderzoek betrokken eenheden bleek dat in de periode 1996–1997 bij drie van de vier eenheden het management dan wel het hoofd van de eenheid dilemmatraining heeft gevolgd. Bij de vierde eenheid zou het management eind september van dit jaar op dilemmatraining gaan. Van één in het onderzoek betrokken eenheid van directie Particulieren waren medewerkers van de klantendienst en deurwaarders op dilemmatraining geweest.

4.3.3 Basiswaarden Belastingdienst

Een brochure waarin de Basiswaarden worden toegelicht is medio 1998 aan de hoofden van eenheden verzonden. Communicatie over basiswaarden wordt gezien als een instrument waardoor leidinggevenden en medewerkers dilemma's en de uitvoering van maatregelen die betrekking hebben op het waarborgen van integriteit bespreekbaar kunnen maken.

De basiswaarden zijn echter lastig te communiceren. De voorzitter van de «Reflectiegroep Integriteit Belastingdienst» heeft in juli 1999 door middel van een notitie zijn zorgen geuit over de implementatie van de brochure Basiswaarden – met name ten aanzien van het thema «geloofwaardigheid – en het onderwerp op de agenda van de Directieraad gezet. Aanleiding hiervoor waren signalen dat de situatie dreigde te ontstaan of wellicht al ontstaan was dat deze basiswaarde in de communicatie gaan aandacht zou krijgen.

Bij het onderzoek op de eenheden is gebleken dat op een enkele uitzondering na de medewerkers niet of nauwelijks met de brochure of de inhoud bekend waren. Slechts één medewerker kon desgevraagd de drie basiswaarden, geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid, noemen.

4.3.4 Vertrouwenspersoon integriteit Belastingdienst

Aanleiding voor het aanstellen van een vertrouwenspersoon integriteit was dat er situaties denkbaar zijn waarbij medewerkers die geconfronteerd worden met integriteitsinbreuken, zich niet of minder eenvoudig met hun leidinggevenden kunnen verstaan.

> *Dit bleek bijvoorbeeld het geval te zijn bij de integriteitsinbreuk die de aanleiding vormde voor het onderzoek. De collega-deurwaarders en een aantal medewerkers uit hetzelfde team bleken al langere tijd op de hoogte te zijn van de gang van zaken. Om daar niet meer mee geconfronteerd te hoeven worden wijzigde een aantal medewerkers hun werktijden.*

De vertrouwenspersoon integriteit gaf desgevraagd aan dat hij sinds zijn aanstelling in februari dit jaar één maal door een medewerker is benaderd. Dit heeft niet geleid tot een melding. Navraag op de eenheden leerde dat een groot aantal van de medewerkers niet op de hoogte is van het feit dat er een vertrouwenspersoon integriteit Belastingdienst is aangesteld. De medewerkers die hiervan op de hoogte waren gaven aan dat de drempel om deze vertrouwenspersoon te benaderen – mede vanwege zijn voormalige functie – erg hoog was. De vertrouwenspersoon Integriteit deelde deze mening overigens niet. Na een jaar zal de functie worden geëvalueerd.

4.3.5 Bewustzijn/cultuur

De onderzochte eenheden hebben zonder uitzondering aangegeven dat communicatie over integriteit de belangrijkste invulling vormt van het integriteitsbeleid. Bij de onderzochte eenheden bleek dat:

- waar integriteit als onderdeel van het werkoverleg aan de orde zou worden gesteld, dat niet in alle gevallen gebeurde. Bovendien bleek niet in alle gevallen regelmatig werkoverleg te hebben plaatsgevonden of bleek dat niet alle medewerkers structureel in het werkoverleg te participeren;
- bij drie van de vier eenheden integriteit niet tijdens het functionerings- of beoordelingsgesprek aan de orde kwam;
- bij twee eenheden integriteit aan de hand van een video met praktijkvoorbeelden in de behandelteams besproken zal gaan worden; dit is echter ter discretie van de teamleider. Voor één eenheid wordt dit de eerste kennismaking met integriteit, de andere eenheid heeft in 1997 een communicatieronde gehouden.

De uitvoering van het integriteitsprogamma is bij de onderzochte eenheden nog niet goed van de grond is gekomen. Wel is gebleken dat er concrete voornemens bestaan om hier nadere invulling aan te geven of dat hiertoe ontwikkelingen in gang zijn gezet.

Bij communicatie over integriteit hoort naar de mening van de Rekenkamer ook het communiceren over integriteitsinbreuken die zich binnen de Belastingdienst hebben voorgedaan. Hierin is niet voorzien, hoewel zeer ernstige integriteitsinbreuken gemeld worden aan de directies en/of DG der Belastingen. De casus die de aanleiding vormde voor het onderzoek is op één van de andere eenheden gebruikt als kapstok om integriteit als onderwerp onder de aandacht van de medewerkers te brengen. Duidelijk was wel bij de overige eenheden dat medewerkers behoefte hadden aan informatie over feiten en omstandigheden, vooral omdat in de media naast juiste ook onjuiste berichtgeving had plaatsgevonden.

Als laatste onderdeel van het omgaan met integriteit en het bewustzijn van medewerkers is gevraagd naar de cultuur en manier waarop medewerkers elkaar aanspreken op gedrag. Uit gesprekken met medewerkers, teamleiders en bedrijfsmaatschappelijk werkers kwam naar voren dat binnen grote delen van de Belastingdienst een cultuur heerst waarin medewerkers elkaar niet aanspreken op onprofessioneel of niet-integer gedrag en verantwoordelijkheid hiervoor uit de weg gaan. Uitkomsten van de Beveiligingsmonitor bevestigen dit beeld als het gaat om aanspreken van collega's op het overtreden van beveiligingsregels. Verdergaand zijn de signalen die er op wijzen dat als zich integriteitsinbreuken voordoen die niet gemeld worden bij de (direct) leidinggevende.

4.4 Maatregelen op personeelsgebied

De maatregelen die de Belastingdienst heeft getroffen om integriteit te bevorderen of onder de aandacht van nieuwe en/of tijdelijke medewerkers te brengen werden als volgt ingevuld:

- Functieroulatie
  Bij de vier onderzochte eenheden was meestal sprake van de gewenste mobiliteit.
- Opleidingen
  Bij de vier onderzochte eenheden werd aangegeven dat integriteit als apart aspect in de startopleiding van nieuwe medewerkers is opgenomen.
- Aandacht voor integriteit nieuwe/tijdelijke medewerkers
  De voorlichting over integriteit aan nieuwe en tijdelijke medewerkers bleek bij de vier eenheden verschillend te worden ingevuld. Dit varieerde van een introductiepakket en/of aandacht voor het onderwerp tijdens een introductiedag tot aandacht die in het reguliere werkoverleg aan integriteit wordt gegeven.

Overigens dient bij de laatste twee maatregelen opgemerkt te worden dat bij de Belastingdienst de afgelopen jaren weinig nieuwe medewerkers zijn aangenomen.

4.5 Conclusie

De intensivering van de aandacht voor integriteit heeft geleid tot een integraal integriteitsbeleid in 1995 waarin naast regelgeving, communicatie over integriteit een belangrijke rol vervult. Deze combinatie ziet de Rekenkamer als een positieve bijdrage aan het verhogen van de weerbaarheid van medewerkers tegen integriteitsinbreuken. De werking van het beleid heeft echter in de praktijk nog onvoldoende effect gesorteerd. Dit blijkt ondermeer uit de onbekendheid van medewerkers met de (brochure) basiswaarden en de vertrouwenspersoon integriteit. Ook laat de voortgang van de uitvoering van het integriteitsprogramma in de vorm van dilemmatrainingen te wensen over. De meldingsplicht voor nevenwerkzaamheden blijkt bij medewerkers goed bekend te zijn. Uit het onderzoek en uit eigen informatie van de Belastingdienst blijkt evenwel dat de registratie niet compleet is en dat in bepaalde gevallen risico's van belangenverstrengeling aanwezig zijn. Preventieve maatregelen en instrumenten op personeelsgebied worden in bepaalde gevallen niet nageleefd respectievelijk nauwelijks benut en incidenten worden niet aangegrepen om «integriteit» onder de aandacht van medewerkers te brengen. Nu bovendien naar voren is gekomen dat er binnen grote delen van de Belastingdienst een cultuur heerst waarin medewerkers elkaar niet aanspreken op gedrag en de verantwoordelijkheid daarvoor uit de weg gaan, of belangrijker nog, integriteitsinbreuken in bepaalde gevallen niet melden, betekent dit dat het voorgestane proces van bewustwording en verantwoordelijkheid in de praktijk nog nauwelijks zijn beslag heeft gekregen. De hiermee gepaard gaande risico's worden naar de mening van de Rekenkamer onvoldoende beheerst.

5 CONCLUSIE

De taken en de verantwoordelijkheden van de Belastingdienst brengen met zich mee dat de risico's ten aanzien van het omgaan met vertrouwelijke gegevens beheersbaar dienen te zijn. Het onvoldoende beheersen van deze risico's kan bovendien afbreuk doen aan de bereidheid van belastingplichtigen om vrijwillig aan hun verplichtingen te voldoen. Inzicht in risico's is daarvoor noodzakelijk. Hoewel eigen onderzoeken van de Belastingdienst op het gebied van informatiebeveiliging aangeven hoe medewerkers met beveiligingsregels omgaan, zijn de tekortkomingen op centraal niveau onvoldoende bekend. Mede hierdoor ontbreekt het integrale inzicht in de risico's en de daaruit voortvloeiende tekortkomingen bij de Belastingdienst.

De Belastingdienst heeft de laatste jaren veel inspanningen gepleegd om de informatiebeveiliging en de waarborgen tegen inbreuken op de ambtelijke integriteit te versterken. Aanscherping van beveiligingsregels en intensivering van het integriteitsbeleid, dat waarborgen kan bieden tegen integriteitsinbreuken, nieuwe instrumenten als speerpunt-onderzoeken en de Beveiligingsmonitor, zijn hier voorbeelden van. Deze inspanningen hebben echter nog niet het gewenste resultaat gehad. De aandacht op de werkvloer voor het productieproces heeft tot gevolg dat informatiebeveiliging en integriteit minder of in bepaalde gevallen lage prioriteit hebben gekregen. Er is een spanningsveld ontstaan tussen enerzijds het voldoen aan de productie-eisen en klantgerichtheid richting belastingplichtigen en anderzijds de beheersing van risico's op het gebied van informatiebeveiliging en integriteit. Naar de mening van de Reken-

kamer zou een integrale benadering waarin controle op en verantwoording over informatiebeveiliging en integriteit als volwaardig elementen in de bedrijfsvoering worden meegenomen, dit spanningsveld kunnen verkleinen. De integrale verantwoordelijkheid hiervoor is organisatorisch bij de eenheid gelegd, maar wordt nu onvoldoende ingevuld. Aan de achtergronden daarvan dient de Belastingdienst meer aandacht te besteden opdat er meer inzicht in en een betere beheersing van risico's voor het omgaan met vertrouwelijke gegevens komt. Dit is naar de mening van de Rekenkamer nu nog onvoldoende het geval.

6 AANBEVELINGEN

6.1 Toegang tot de gegevens

Teneinde een betere invulling te geven aan het «need to know»-beginsel zou de Belastingdienst in kaart moeten brengen welke gegevens de individuele medewerker nodig heeft voor het uitvoeren van zijn taak. Ondersteunende toegangsbeperkende maatregelen hierbij kunnen zijn:

- bij centrale systemen een horizontale inperking aan te brengen tot het ambtsgebied van de eenheid of tot doelgroepen belastingplichtigen voor de behandelteams. Eén medewerker zou dan geautoriseerd kunnen worden voor de overige landelijke gegevens;
- een horizontale inperking aan te brengen tot het werkpakket van de medewerker;
- verticale inperking aan te brengen door uitsluitend toegang tot een deel van de gegevens van belastingplichtigen toe te staan: wel naam-adres-woonplaats (NAW)-gegevens maar niet de daarbij opgeslagen fiscale gegevens.

Teneinde de problemen rond het omgaan met wachtwoorden weg te nemen zou gebruik moeten worden gemaakt van:

- principe van single log on: één individuele gebruikersnaam en één wachtwoord voor toegang tot een eigen beveiligd bestand waarin de wachtwoorden en eventueel gebruikersnamen worden bijgehouden voor de informatiesystemen.

De problemen rond het autorisatieregime kunnen op de volgende wijze worden weggenomen:

- de autorisatieprocedure moet versneld worden en (nieuwe) medewerkers moeten tijdig te worden aangemeld;
- controle moet (blijven) plaatsvinden op het verband tussen functie en autorisatie, ook in geval van nieuwe autorisaties (zijn deze in overeenstemming met de huidige autorisaties);
- controle moet (blijven) plaatsvinden in geval van ander takenpakket of andere functie: zijn de huidige autorisaties nog nodig en hoe verhouden deze zich tot de nieuw toe te kennen autorisaties;
- controle moet (blijven) plaatsvinden op het intrekken van bestaande autorisaties in geval van verandering van werkplek (ander team of zelfs andere eenheid) en/of ontslag;
- de mogelijkheid tot minder ruime autorisaties voor toepassingsbeheer en faciliteitenbeheer moet worden onderzocht.

De authenticiteit van de gebruiker dient gewaarborgd te worden:

- het gebruik van groeps- en fictieve wachtwoorden moet voorkomen worden;
- het gebruik van wachtwoorden van andere medewerkers moet voorkomen worden; in geval van langdurige ziekte of afwezigheid dient een andere medewerker opnieuw voor de behandeling van dat takenpakket geautoriseerd te worden.

- er dient vastlegging plaats te vinden van de gebruikersnaam bij elke toegang tot gegevens van een belastingplichtige. Een eenvoudig bestand is hiervoor noodzakelijk waarin wordt vastgelegd: sofinummer, gebruikersnaam en datum/tijd.
- bij alle medewerkers moet bekend zijn dat indien een medewerker zijn gebruikersnaam door een collega laat gebruiken, de verantwoordelijkheid hiervoor bij degene blijft die zijn identificatie laat gebruiken.

Teneinde de controle mogelijkheden op het onbevoegd raadplegen te vergroten zou er

- voor uitzonderlijke situaties een ondersteunend programma moeten zijn, met gebruikmaking van laatstgenoemd bestand. Indien het systeem detecteert dat de gebruiker vertrouwelijke gegevens benadert kan dat automatisch worden vastgesteld.

De volgende situaties zouden hier aanleiding toe kunnen geven:

* het opvragen van reeds afgehandelde bestandsgegevens;
* het opvragen van informatie over een belastingplichtige uit een ander ambtsgebied/regio;
* het opvragen van vertrouwelijke gegevens op een ongebruikelijk tijdstip

In extreme situaties zou in aanvulling hierop automatisch een e-mail naar de leidinggevende kunnen worden gestuurd (als de ernst van de situatie daar aanleiding toe geeft) om de gebruiker te betrappen.

- voldoende bekendheid gegeven moeten worden aan deze methoden van loggen: iedereen weet waar die aan toe is (eigen verantwoordelijkheid) en de preventieve werking kan een remmend effect hebben op onbevoegd raadplegen, dan wel het uit nieuwsgierigheid bekijken van gegevens.

6.2 Organisatie en personeel

Teneinde het spanningsveld tussen de primaire processen en de onvoldoende aandacht voor informatiebeveiliging en integriteit te verminderen dient er

- bij de beleidsvorming geïnventariseerd te worden welke consequenties nieuwe maatregelen hebben voor de primaire processen. Daarbij dient in aanmerking te worden genomen dat er voldoende ruimte beschikbaar blijft om aandacht aan informatiebeveiliging en integriteit te besteden;
- terugkoppeling plaats te vinden vanuit de eenheden naar het kerndepartement indien het spanningsveld in deze mate blijft bestaan. Duidelijke en concrete informatie over de (on)mogelijkheden ten aanzien van het implementeren van beleid draagt bij aan de effectiviteit van dergelijke maatregelen.

Teneinde de integrale verantwoordelijkheid op eenheidsniveau betere invulling te geven dient:

- een betere afstemming tussen de verantwoordelijke dienstonderdelen te zijn en dienen er duidelijke afspraken te zijn over verantwoordelijkheden. Hierop dient gemonitord te worden. Het gaat om afspraken over interne controle tussen eenheid en Belastingdienst Automatiseringscentrum, tussen eenheid en Belastingdienst/Centrum voor Facilitaire Dienstverlening over de beveiliging van de gebouwen en tussen eenheid en Belastingdienst/Centrum voor Kennis en Communicatie over afstemming voor wat betreft de dilemmatrainingen;
- het beleid op het gebied van informatiebeveiliging en integriteit vertaald te zijn in een lokaal integraal veiligheidsplan.

Teneinde de onduidelijkheid die bij medewerkers bestaat over voorschriften/richtlijnen weg te nemen dient:
- geïnventariseerd te worden over welke voorschriften en/of richtlijnen bij medewerkers onduidelijkheid bestaat;
- de onduidelijkheden besproken te worden en de richtlijnen vertaald te worden in «huisregels»;
- bij het inhoud geven van een dergelijk plan en eventuele huisregels nadrukkelijk alle medewerkers te worden betrokken om voldoende inzicht in de werkbaarheid te krijgen en een breed draagvlak voor naleving te creëren.

Teneinde op eenheidsniveau (en hoger) meer inzicht te krijgen in risico's en daaruit mogelijk voortvloeiende tekortkomingen dient:
- gestructureerd overleg tussen de beveiligingsfunctionarissen op eenheidsniveau (FIB-3) onderling en met de FIB-2 te worden ingesteld;
- het afleggen van verantwoording over uitvoering van het beleid voor informatiebeveiliging en integriteit op vaste momenten (bijvoorbeeld in beheersverslag) plaats te vinden;
- het uitvoeren van controles op aanwezigheid geheimhoudings-verklaring en verklaring omtrent gedrag bij tijdelijke personeel plaats te vinden op vaste momenten;
- er een eenduidige registratie van beveiligingsincidenten en van integriteitsinbreuken te zijn. Deze registratie dient op eenheidsniveau, doelgroepniveau en centraal niveau te worden onderhouden.

Teneinde de medewerkers meer ondersteuning en weerstand mee te geven zou gedacht kunnen worden aan de volgende maatregelen:
- Inventariseer op basis van de bekend geworden integriteitsinbreuken en beveiligingsincidenten welke signalen eerder tot actie hadden kunnen leiden. Neem deze mee in een training voor teamleiders bij aspect «integriteit» (alertheidstraining);
- benut objectieve momenten als functioneringsgesprekken en werkoverleggen om beveiliging en integriteit aan de orde te stellen door middel van een checklist aan de hand waarvan aspecten op dit gebied doorgenomen moeten worden;
- breng relevante informatie ook ter kennis van betrokkenen, zoals informatie over nevenwerkzaamheden in het personeelsdossier opnemen en het doorgeven aan toepassingsbeheer dat medewerkers niet meer op de eenheid werkzaam zijn.

6.3 Bewustzijn en cultuur

Teneinde het bewustzijn van de medewerkers inzake informatiebeveiliging en integriteit te verhogen dient
- bij de introductie van nieuwe maatregelen of instrumenten die bedoeld zijn om het bewustzijn te verhogen meer voorlichting te worden gegeven zodat de bekendheid wordt vergroot;
- rekening te worden gehouden met en afgestemd te worden op de doelgroep; een (voorlichtings)brochure dient in begrijpelijker taal te worden gesteld en voorzien te worden van concrete voorbeelden;
- meer duidelijkheid inzake het overtreden van voorschriften en /of richtlijnen en welke consequenties hier aan verbonden kunnen zijn, te worden verschaft;
- plichtsverzuim en de sanctie daarop geanonimiseerd bekend te worden gemaakt bij de eenheid en binnen de Belastingdienst en zouden dergelijke incidenten aangegrepen moeten worden om aandacht te vragen voor het onderwerp;
- de uitkomsten van de Beveiligingsmonitor te worden gebruikt als input voor de bespreking van het omgaan met beveiligingsregels. De

uitkomsten dienen per eenheid bekend te worden en te worden ingebracht in werkoverleg.

Mogelijkheden om de cultuur – waarin medewerkers verantwoordelijkheid voor gedrag of het aanspreken van anderen daarop uit de weg gaan – om te buigen, zijn:

- verwerk integriteitsaspecten in de Beveiligingsmonitor zodat meer inzicht komt in de werking van het integriteitsbeleid en de effecten van dilemmatraining;
- maak de uitkomsten van deze monitor bespreekbaar als een probleem waar medewerkers zelf een oplossing voor dienen aan te dragen en de verantwoordelijkheid voor nemen;
- een uniforme uitvoering op de eenheden van voorschriften en/of richtlijnen. In het managementoverleg dienen hier afspraken over te worden gemaakt.
- het belang van de verdere uitvoering van het integriteitsprogramma dient nogmaals onderstreept te worden. Dit kan door bijvoorbeeld een eenheidsdag te faciliteren of centraal Belastingdienst/per doelgroep dit via een themadag te organiseren. Verschaf indien nodig de noodzakelijke voorwaarden daartoe;
- het aanstellen van een laagdrempelig aanspreekpunt op eenheidsniveau als het gaat om een vertrouwenspersoon Integriteit. Zorg bij het instellen van deze functie voor onafhankelijkheid en voor informatie richting medewerkers in welke gevallen en onder welke voorwaarden de vertrouwenspersoon een rol kan spelen.

7 REACTIE STAATSSECRETARIS EN COMMENTAAR REKENKAMER

De staatssecretaris van Financiën sprak in zijn reactie op het rapport waardering uit voor het bereikte resultaat en hij gaf aan de eindconclusie te onderschrijven. De aanbevelingen bieden naar zijn mening een goede basis om het ingezette beleid binnen de Belastingdienst op het gebied van informatiebeveiliging en integriteit verder uit te bouwen en te verbeteren. De gedifferentieerde aanpak door verschillende maatregelen aan te reiken die elkaar kunnen versterken en soms vervangen, sprak hem aan. Op zijn voorgenomen aanpak van enkele aanbevelingen gaf hij een toelichting. Voor de aanbevelingen om de problemen rond het omgaan met wachtwoorden weg te nemen kiest de staatssecretaris voor een tweesporenaanpak. Op korte termijn zal het aantal gebruikersnamen en wachtwoorden worden beperkt, waarmee eveneens de autorisatieprocedure versneld kan worden. Hierdoor wordt het gebruik van groeps- en fictieve wachtwoorden overbodig. Tevens zullen de ontwikkelingen rond het «single log on»-principe, hetgeen door de staatssecretaris wordt onderschreven maar dat op korte termijn niet toepasbaar is, scherp worden gevolgd en mogelijk door eigen verkenning worden versneld.

Om de onduidelijkheden over voorschriften en richtlijnen weg te nemen kiest de staatssecretaris eveneens voor een tweesporenaanpak. Deze houdt in dat voor de huidige voorschriften de voorgestelde aanbevelingen zullen worden gerealiseerd. De staatssecretaris vindt het evenwel ook van belang de eigen verantwoordelijkheid van medewerkers te benadrukken. Daartoe gaan zijn gedachten uit om een «digitale vraagbaak» op het intranet van de Belastingdienst te creëren waar alle medewerkers met hun specifieke vragen terecht kunnen. Communicatie hierover levert dan een gemeenschappelijk referentiekader voor gedrag en handelen.
Om de onafhankelijke positie van een laagdrempelige vertrouwenspersoon te waarborgen zou hij ervoor willen kiezen deze functie op

directieniveau in te stellen en in een enkel geval op eenheidsniveau. Voor de overige aanbevelingen gaf hij aan zich hierin te kunnen vinden.
Ten aanzien van de registratie van beveiligingsincidenten gaf de staatssecretaris aan dat deze inmiddels op orde is gebracht. Tenslotte merkte de staatssecretaris op dat hij ervan overtuigd is dat de medewerkers van de dienst in het algemeen gesproken op uiterst prudente wijze omgaan met vertrouwelijke gegevens.

De Rekenkamer heeft met genoegen kennis genomen van het voornemen van de staatssecretaris haar aanbevelingen over te nemen. Alleen ten aanzien van het instellen van een vertrouwenspersoon pleit de Rekenkamer, in afwijking van wat de staatssecretaris voorstaat, voor het aanwijzen van een functionaris voor deze rol op eenheidsniveau. Naar haar mening hoeft dit de onafhankelijkheid van de functie niet aan te tasten, terwijl er toch een laagdrempelige toegang is.

BIJLAGE 1 **OVERZICHT VAN DE BELANGRIJKSTE INFORMATIESYSTEMEN**

1. Centrale systemen

Directies P en O

BVR = Beheer van Relaties
Dit systeem bevat de landelijke gegevens van de belastingplichtigen (en eventuele relaties) als naam-adres-woonplaats en sofinummer.

COA = Centrale ontvangersadministratie
Landelijke verwerking van
- de (terug)betalingen op aanslagen
- vervolgingsacties

van alle belastingplichtigen.

HSB = Houderschapsbelasting
Verwerking (heffing en inning) van de motorrijtuigenbelasting.

Directie O
OB = Omzetbelasting
Landelijke verwerking van de aangiften/aanslagen omzetbelasting.

LB = Loonbelasting
Landelijke verwerking van de aangiften/aanslagen loonbelasting.

KaVPB = Vennootschapsbelasting
Centraal systeem voor de lokale verwerking van de aangiften/aanslagen vennootschapsbelasting.

2. Lokale systemen

Directies P en O

IBS = Inkomstenbelastingsysteem
Verwerking van de gegevens van de aangiften tot aanslagen inkomstenbelasting, vermogensbelasting en premies volksverzekeringen.

GOA = Geautomatiseerde ontvangersadministratie
Lokale verwerking van
- de (terug)betalingen op aanslagen
- vervolgingsacties

van de belastingplichtigen van het ambtsgebied van de eenheid.

Directie O

IKB = Integrale klantbehandeling
Registratie en beheer van gegevens van belastingplichtige ondernemingen, zoals organisatie, relaties, historie.