Informatiebeveiliging en de rol van de overheid

K.J.M. Kool en Mr. E.G. Venekamp

THEMA

1 Inleiding

Binnen de overheid is de beveiliging van gegevens van oudsher een belangrijk aandachtspunt. Traditioneel ging het daarbij primair om de bescherming van gegevens die van belang zijn voor de staatsveiligheid of andere gewichtige belangen van de staat. Hierbij is te denken aan het beschermen van staatsgeheimen en andere gerubriceerde gegevens. Vanaf de jaren '70 is er sprake van een geleidelijke ontwikkeling naar informatiebeveiliging in bredere zin. Dit is allereerst ingegeven door het toenemend belang van geautomatiseerde gegevensverwerking. In samenhang daarmee en mede onder invloed van maatschappelijke ontwikkelingen is de bescherming van de privacy van burgers en daarmee de beveiliging van persoonsgegevens van groter belang geworden.

De laatste jaren zijn er enkele belangrijke impulsen voor de informatiebeveiliging bij de rijksoverheid tot stand gekomen. Het belangrijkste zijn het totstandkomen van het Besluit Voorschrift Informatiebeveiliging Rijksdienst 1994 (VIR), het instellen van het Informatiebeveiligingsberaad en de oprichting van het Advies- en Coördinatiecentrum Informatiebeveiliging (ACIB).

Dit geheel aan activiteiten is vooral totstandgekomen naar aanleiding van onderzoeksrapporten van de Algemene Rekenkamer over computerbeveiliging bij de rijksoverheid en een door het

ministerie van Binnenlandse Zaken uitgevoerd onderzoek naar de kwetsbaarheid van bestuurlijke informatiesystemen (SIBAS, 1989).

Ook bij andere onderdelen van de overheid, zoals gemeenten en de politieorganisatie, is er een toenemende aandacht voor informatiebeveiliging waar te nemen. Belangrijk in dit kader is onder meer het totstandkomen van het Handboek Beveiliging, dat een methodiek beschrijft voor het opstellen van beveiligingsplannen voor gemeenten (VIAG, 1992).

Naast de zorg voor de eigen informatievoorziening (interne taak) heeft de overheid op het gebied van informatiebeveiliging een taak in het stellen van regels voor de maatschappij als geheel (externe taak). De snelle ontwikkeling van informatie- en communicatietechnologie vraagt om kaders ten aanzien van bijvoorbeeld de privacybescherming, auteursrechten en intellectuele eigendom. Daarbij kan de overheid - naast haar taak als wetgever - ook een rol spelen in het stimuleren van ontwikkelingen, zowel op beleidsmatig als op technologisch terrein. Zij doet dat bijvoorbeeld via het Nationaal Actieprogramma Elektronische Snelwegen. Overigens zijn daar voor zover ons bekend geen specifieke projecten in voorzien met het oog op de beveiliging. Dit terwijl beveiliging en authenticatie (bijvoorbeeld door middel van een elektronische handtekening) juist in het kader van de elektronische snelweg zeer belangrijke randvoorwaarden zijn voor verdere ontwikkeling.

K.J.M. Kool RA en Mr. E.G. Venekamp zijn werkzaam bij de directie Planning, Financiën en Control van de Belastingdienst als hoofd van de afdeling Planning en Control, respectievelijk hoofd van de afdeling Informatiemanagement. Dit artikel is op persoonlijke titel geschreven.

In dit artikel wordt ingegaan op eerstgenoemde aandachtspunt: de rol van de overheid inzake het beveiligen van de 'eigen' informatievoorziening. Het accent ligt daarbij op de ontwikkelingen bij de rijksoverheid.

2 Informatiebeveiliging bij de rijksoverheid

Er is een aantal redenen waarom informatiebeveiliging voor de rijksoverheid belangrijk is. Allereerst is het goed functioneren van de overheid als bedrijf in toenemende mate afhankelijk van het betrouwbaar en ongestoord functioneren van informatie- en communicatiesystemen. De ontwikkeling bij de overheid is hierbij geen andere dan die bij andere organisaties en het bedrijfsleven. De laatste 10 jaar is het gebruik van informatietechnologie doorgedrongen tot elke werkplek. Waar er voorheen sprake was van concentratie in een centraal rekencentrum is er nu sprake van deconcentratie van gegevens, programmatuur en infrastructuur. Gekoppeld daaraan is er veelal sprake van een decentralisatie van verantwoordelijkheden inzake het beheer. Tegelijkertijd is er sprake van het integreren c.q. koppelen van informatiesystemen. Deze ontwikkelingen leiden, zoals gesteld wordt in de toelichting bij het VIR, tot 'complexe situaties met diffuse verantwoordelijkheden. Gegevens komen steeds gemakkelijker beschikbaar, maar gegevensstromen zijn steeds moeilijker beheersbaar'.

Een tweede reden waarom informatiebeveiliging voor de overheid van belang is hangt samen met de publieke taak die de overheid vervult.

Ten behoeve van het uitvoeren van die taak is het noodzakelijk dat de overheid beschikt over een groot aantal persoonlijke gegevens van burgers. Te denken valt aan gegevens ten behoeve van huursubsidie, studiefinanciering, sociale uitkeringen, belastingen en dergelijke. Burgers (en bedrijven) zijn doorgaans verplicht deze gegevens te verstrekken. Een adequate beveiliging van deze gegevens is dan ook een eerste eis die aan het overheidshandelen gesteld moet worden. Dit vloeit voort uit het grondwettelijk recht van eerbiediging van de persoonlijke levenssfeer. De regels hieromtrent zijn onder meer vastgelegd in de Wet Persoonsregistraties. Uiteraard gelden deze regels niet alleen de overheid, maar gezien de aard van de gegevens en de titel waarop ze worden verkregen (wettelijke verplichting) heeft de overheid hier wel een bijzondere verantwoordelijkheid.

Directeur-Generaal Van Lunteren van de Belastingdienst merkte in dit verband in 1994 op: '...door de aard van de gegevens ontstaat macht. De Belastingdienst verzamelt niet alleen maar

gegevens. Hij verzamelt in feite macht.Macht, en zeker overheidsmacht, moet begrensd zijn en gecontroleerd worden.' (Van Lunteren, 1994). Waar de toegankelijkheid van gegevens toeneemt, mede onder invloed van het koppelen van systemen en bestanden, zijn maatregelen nodig om te kunnen waarborgen dat gegevens slechts gebruikt worden binnen het kader van het doel waarvoor ze verstrekt zijn. Het kunnen beheersen van de toegang tot gegevens is een belangrijke eis.

Een derde reden waarom informatiebeveiliging bij de rijksoverheid in het bijzonder aandacht verdient is in de inleiding aan de orde gekomen. Met het oog op de staatsveiligheid en andere gewichtige belangen van de staat is het van belang dat bepaalde gegevens nadrukkelijk geheim zijn en geheim blijven. Ook is het van belang dat de beschikbaarheid van bepaalde vitale voorzieningen en systemen gewaarborgd is. De regels hieromtrent binnen de rijksoverheid liggen vast in de Wet op de inlichtingen- en veiligheidsdiensten, het Beveiligingsvoorschrift I-1949, de voorschriften inzake verbodingsbeveiliging en de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst (Beveiligingsvoorschrift 1989).

Opvallend is dat het per 1 januari 1995 in werking getreden VIR met name lijkt ingegeven door de eerstgenoemde reden: het belang van informatiebeveiliging voor het effectief en doelmatig opereren van de overheid zelf, anders geformuleerd 'het bedrijfsbelang'. Dit is te meer opmerkelijk, omdat het VIR in de plaats is gekomen van een tweetal andere voorschriften binnen de rijksdienst, waaronder de Aanwijzingen inzake de beveiliging van persoonsgegevens (1982). In de inleiding van deze Aanwijzingen werd gesteld dat het eerste doel was te verzekeren dat onbevoegd kennis nemen van persoonsgegevens door derden en door eigen personeel wordt voorkomen. Daarnaast werd aangegeven dat de gegeven aanwijzingen indirect ook het waarborgen van een ongestoorde en correcte computerverwerking beogen en bedrijfszekerheid. De lijn van het VIR is een andere.

Het doel van het VIR is te komen tot betrouwbare informatiesystemen: betrouwbaarheid heeft bij het VIR betrekking op drie aspecten, te weten beschikbaarheid, integriteit en exclusiviteit. In het VIR valt het beschermen van de persoonlijke levenssfeer onder het begrip exclusiviteit: de mate

waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden.

De te stellen betrouwbaarheidseisen worden bepaald op basis van risico-analyse of, in termen van het VIR, een afhankelijkheidsanalyse. Kernvraag daarbij is: in welke mate zijn bestuurs-/bedrijfsprocessen afhankelijk van de betrouwbaarheid (waaronder de exclusiviteit) van een informatiesysteem en welke potentiële schades kunnen optreden als gevolg van verstoringen in de informatievoorziening.

In deze benaderingswijze lijkt de bescherming van de persoonlijke levenssfeer de resultante van een risico-afweging door een pragmatisch redenerende overheid: wat is het afbreukrisico? Gelukkig wordt in de artikelsgewijze toelichting bij het VIR wel opgemerkt dat in sommige situaties betrouwbaarheidseisen rechtstreeks kunnen worden afgeleid uit de relevante wet- en regelgeving. Voor persoonsgegevens kan in dit verband aan de Wet Persoonsregistraties worden gedacht.'

Samenvattend is het beschermen van de persoonlijke levenssfeer, als eis van zorgvuldigheid die inherent is aan het optreden van de overheid, in het VIR als 'leitmotiv' van ondergeschikte betekenis.

In de lijn van de Aanwijzingen inzake de beveiliging van persoonsgegevens zou het meer prominent aandacht geven aan dit aspect passend zijn geweest. Zeker waar geconstateerd kan worden dat er weer een toenemende aandacht is voor het ethisch aspect in het overheidsoptreden. In dit verband kan onder meer worden gewezen op de aandacht die de laatste jaren bestaat voor het aspect integriteit in het overheidshandelen c.q. in het handelen van overheidsdienaren.

Een tweede punt dat opvalt in de aanpak van informatiebeveiliging bij de rijksoverheid is dat er in zekere zin sprake lijkt te zijn van twee werelden. Allereerst is daar de wereld van de 'algemene' informatiebeveiliging. Deze betreft de zorg voor betrouwbare werkprocessen en de privacybescherming bij de overheid. De zorg hiervoor ligt primair bij de leiding van de onderscheiden departementen. De kaders voor de algemene beveiliging worden gegeven in het VIR.

Daarnaast wordt onderscheiden de 'bijzondere' informatiebeveiliging. Deze omvat de bescherming van de informatie die van belang is voor het

voortbestaan van de democratische rechtsorde en voor de veiligheid of andere gewichtige belangen van de staat. Op dit gebied spelen de inlichtingen- en veiligheidsdiensten een belangrijke rol. Zij beschikken over actueel inzicht in mogelijke dreigingen en over hoogwaardige technologische kennis. De relevante regelgeving op dit terrein is hiervoor al genoemd. In de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst (1989) is er sprake van een zekere overlap met het VIR. Voorbeelden hiervan zijn de eis een beveiligingsplan op te stellen, het aanwijzen van de secretaris-generaal als eerstverantwoordelijke voor het beleid en het aanwijzen van een beveiligingsambtenaar (BVA).

Het is onduidelijk hoe bijvoorbeeld deze aanwijzing inzake de BVA zich verhoudt tot de informatiebeveiligingsfunctie, waarvan in artikel 3 van het VIR wordt gesproken. Hierdoor is het niet denkbeeldig dat op departementen een dubbele lijn ontstaat: allereerst de lijn van het VIR, waarbij in de praktijk waarschijnlijk een groot accent zal liggen op de beveiliging van de geautomatiseerde gegevensverwerking. Daarnaast de lijn van de genoemde Aanwijzingen, waarbij het accent meer ligt op procedures rondom rubricering van documenten of bestanden, screening van personeel (vertrouwensfuncties) en procedures met betrekking tot opslag en transport van geclassificeerde gegevens (waaronder toegangsbeveiliging van gebouwen en ruimten).

Duidelijk is dat de secretarissen-generaal (of directeuren-generaal bij grote diensten of dienstonderdelen) een belangrijke rol hebben in het coördineren van de activiteiten op de onderscheiden gebieden. Bij hen komen de onderscheiden 'werelden' immers bij elkaar. Toch is het te betreuren dat in het VIR niet nader is ingegaan op de verhouding tussen het VIR en de genoemde Aanwijzingen. Juist waar het VIR is opgesteld vanuit de erkenning dat informatiebeveiliging een geïntegreerd onderdeel van de bedrijfsvoering op alle niveaus moet zijn, doet het niet ingaan op de relatie met de bijzondere informatiebeveiliging afbreuk aan het integrale karakter van het VIR.

3 Aanpak binnen de rijksoverheid

In 1989 is door de Stichting Samenwerkende Instellingen ten behoeve van Beleidsanalytische Studies (SIBAS) een studierapport uitgebracht ten behoeve van de minister van Binnenlandse Zaken,

de coördinerend bewindspersoon voor de openbare informatievoorziening (SIBAS, 1989). In dit rapport wordt informatiebeveiliging gezien als een onderdeel van de kwaliteitszorg rondom de informatievoorziening. Veel aandacht wordt daarbij gegeven aan bewustwording van de toenemende afhankelijkheid van geautomatiseerde informatiesystemen. Beleid en sturing worden nadrukkelijk als taken voor de top van de organisatie gezien. Daarnaast wordt beklemtoond dat beveiligingsmaatregelen het resultaat moeten zijn van een afweging, waarbij niet kan worden uitgegaan van standaardmaatregellijsten.

In 1988 was door de Algemene Rekenkamer het rapport 'Computerbeveiliging; Beveiliging van gegevens in geautomatiseerde systemen bij de ministeries' uitgebracht. Hieruit bleek dat ministeries nog weinig gestructureerd met informatiebeveiliging omgingen. Inzicht in risico's ontbrak en de Aanwijzingen met betrekking tot persoonsgegevens en gerubriceerde gegevens werden onvoldoende opgevolgd.

Het SIBAS-rapport is richtinggevend geweest voor de verbeteringsacties die binnen de rijksoverheid sedertdien geëntameerd zijn. Sinds 1990 is informatiebeveiliging een beleidsprioriteit van de minister van Binnenlandse Zaken. Daarna zijn een aantal belangrijke stappen gezet:

- het instellen van een Interdepartementale Commissie Informatiebeveiliging in 1991. Inmiddels heeft na evaluatie een herschikking van taken plaatsgevonden en is het ICIB voor wat betreft de algemene informatiebeveiliging opgevolgd door het informatiebeveiligingsberaad (IB-beraad). Hierin hebben de verantwoordelijke topambtenaren van departementen zitting. Zij fungeren tevens als portefeuillehouder op strategisch niveau binnen de departementen. Op deze wijze worden de voorwaarden geschapen voor een goede sturing op de departementen (Need to Know 1996);
- het instellen van het Advies- en Coördinatiepunt Informatiebeveiliging (ACIB). Het ACIB ondersteunt het IB-beraad, maar heeft daarnaast een faciliterende rol ten behoeve van de departementen. Geconstateerd kan worden dat het ACIB binnen de rijksoverheid een belangrijke functie vervult als 'aanjager' op het terrein van informatiebeveiliging;
- het totstandkomen van het VIR, zoals hiervoor al aan de orde is gekomen.

In 1995 is door de Algemene Rekenkamer

opnieuw gerapporteerd over de stand van zaken op het terrein van informatiebeveiliging bij de rijksoverheid (Tweede Kamer 1994-1995, kamerstuk 24.175).

Hoewel er ten opzichte van 1988 sprake is van verbeteringen, is de Rekenkamer van mening dat de beheersing van de informatiebeveiliging nog tekortkomingen vertoont. Zo stelt zij onder meer dat de ambtelijke top van de ministeries in het algemeen onvoldoende sturing geeft aan de informatiebeveiliging. Slechts op een viertal ministeries en bij de Belastingdienst acht de Rekenkamer de situatie toereikend. Voor de centrale regelgeving en de overige coördinatie door de minister van Binnenlandse Zaken komt de Rekenkamer tot de conclusie dat de minister in belangrijke mate invulling heeft gegeven aan zijn coördinerende rol. Wel drong de Rekenkamer aan op adequaat regelen van de bovende departementale coördinatie van het toezicht op de naleving van het VIR.

Een dergelijk toezicht werd evenwel door de minister in zijn reactie van de hand gewezen. Naar zijn mening ligt dit toezicht uiteindelijk bij de Tweede Kamer. Wel wilde de minister op termijn bezien of het wenselijk is om de ministeries de plicht op te leggen hem periodiek te informeren omtrent de stand van de informatiebeveiliging op de ministeries. Bij de bespreking van het rapport in de kamercommissies voor Binnenlandse Zaken en voor de Rijksuitgaven is overigens van diverse zijden aangedrongen op een meer concrete toezegging door de staatssecretaris van Binnenlandse Zaken op het punt van het periodiek informeren van de Kamer omtrent de stand van zaken van de informatiebeveiliging.

Inmiddels is het zo dat de Tweede Kamer begin 1997 in ieder geval zal worden geïnformeerd over de stand van zaken per eind 1996 van de invoering van de VIR op de verschillende departementen.

Het IB-beraad heeft zich met de voorbereiding van deze rapportage belast.

4 Het VIR nader beschouwd

Eén van de meest opvallende kenmerken van het Voorschrift Informatiebeveiliging Rijksdienst is zijn beknoptheid. Waar de Aanwijzingen inzake de beveiliging van persoonsgegevens ongeveer 65 (sub)artikelen bevatte, telt het VIR slechts 6 artikelen. In aanmerking nemend dat artikel 1

slechts begripsbepalingen bevat en artikel 6 enkele slotbepalingen inzake het intrekken van eerdere regelgeving, gaat het in feite om 4 artikelen:

- belangrijk in artikel 2 (plaatsbepaling en reikwijdte) is de bepaling dat informatiebeveiliging een lijnverantwoordelijkheid is en een onderdeel vormt van de kwaliteitszorg voor de bedrijfs- en bestuursprocessen;
- artikel 3 bepaalt dat de secretaris-generaal van een departement het informatiebeveiligingsbeleid vaststelt in een beleidsdocument en dit beleid uitdraagt. Het artikel noemt een aantal elementen die ten minste in dit document moeten voorkomen. Eén van die elementen is de wijze waarop periodiek het beleid geëvalueerd wordt en tevens de toereikendheid van het beleid; de implementatie en de uitvoering worden beoordeeld door een onafhankelijk deskundige;
- artikel 4 bepaalt dat het lijnmanagement moet zorgen dat voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied op systematische wijze bepaald wordt welke beveiligingsmaatregelen moeten worden getroffen. Concreet gaat het om het uitvoeren van afhankelijkheids- en kwetsbaarheidsanalyses. Hierop zal hierna nog worden ingegaan;
- artikel 5 bepaalt dat het lijnmanagement moet zorgen dat de in informatiesystemen te treffen maatregelen worden vastgelegd en geïmplementeerd en/of uitgedragen en dat de werking ervan systematisch wordt gecontroleerd.

Nu moet op het punt van de beknoptheid wel worden toegevoegd dat in de algemene en de artikelsgewijze toelichting vervolgens 47 pagina's worden besteed aan het uitleggen wat met de artikelen wordt beoogd en bedoeld. Bovendien is er in samenhang met het VIR het Handboek Informatiebeveiliging Rijksdienst ontwikkeld. Dit lijvige boekwerk is bedoeld als handreiking voor de ministeries bij het uitvoeren van het VIR.

Dit neemt echter niet weg dat het VIR in zijn essentie beknopt is en slechts een zeer beperkt aantal regels geeft. Hiermee onderscheidt het zich niet alleen van de Aanwijzingen inzake de beveiliging van persoonsgegevens, maar ook van meer recente publicaties, zoals de Code voor Informatiebeveiliging (uitgebracht door het ministerie van EZ en het NNI) en de brochure 'Beveiliging van persoonsregistraties' van de Registratiekamer.

Deze laatste brochure is bedoeld als advies met het oog op de beveiligingsplicht, zoals neergelegd in artikel 8 van de Wet Persoonsregistraties.

De aanbevelingen uit het advies vormen tegelijkertijd het uitgangspunt voor de Registratiekamer bij het uitvoeren van haar toezichthoudende taak (Registratiekamer 1994).

Hieruit blijkt dat het VIR een fundamenteel andere benaderingswijze heeft dan de andere genoemde stukken. Het VIR ziet informatiebeveiliging als een belangrijk kwaliteitsaspect van de informatievoorziening. Het primaire oogmerk is om de aandacht van het management op dit aspect te richten. Het bevat geen opsomming van te nemen maatregelen. Die keuze kan slechts het verantwoordelijke management maken. Wat het VIR in essentie van het management eist, is dat het informatiebeveiliging als een integraal onderdeel van de managementtaak opvat en er op een planmatige wijze mee omgaat. Hiermee is een andere weg ingeslagen dan indertijd met de Aanwijzingen uit 1982 het geval was. Daarbij lag het accent op gedetailleerde regelgeving van bovenaf. In die zin sluit het VIR ook aan op de wijze waarop het denken inzake overheidsmanagement zich sedertdien heeft ontwikkeld. Decentralisatie, integraal management en sturen op resultaten zijn daarbij belangrijke begrippen.

Het VIR volgt ook een andere aanpak dan de Code voor Informatiebeveiliging. Daarbij moet worden aangetekend dat de Code bedoeld is als een verzameling van 'best business practices'. Hij stelt organisaties in staat om op een pragmatische en snelle wijze de belangrijkste beveiligingsmaatregelen te inventariseren en in te voeren. De Code is in aanvulling op het VIR uitstekend bruikbaar bij het vaststellen van concrete beveiligingsplannen voor specifieke (onderdelen van) departementen respectievelijk specifieke informatiesystemen. Dit geldt met name in situaties waar de beveiligingssituatie nog onvoldoende is. Implementatie van de aanbevelingen uit de Code kan dan een eerste stap zijn, voorafgaand aan het uitvoeren van uitgebreide afhankelijkheids- en kwetsbaarheidsanalyses.

Het verschil in benadering tussen het VIR en de aanpak die wordt voorgestaan door de Registratiekamer wekt geen verwondering. De Registratiekamer heeft immers een specifiek belang op het oog: de bescherming van de persoonlijke levens-

sfeer. De Registratiekamer stelt dan ook specifieke eisen, waarbij onderscheid wordt gemaakt naar drie exclusiviteitsniveaus. Een voorbeeld van een dergelijke eis is: 'De gegevensdragers moeten op een zodanige wijze worden bewaard en behandeld dat alleen bevoegde personen erover kunnen beschikken' (Registratiekamer 1994, pag. 22). Als zwaarste eis inzake de beveiliging van datacommunicatie (exclusiviteitsniveau 3) formuleert de Registratiekamer echter: 'De gegevens dienen versleuteld, via erkende cryptografische methoden, te worden verzonden.' (Registratiekamer 1994, pag. 33). Het komt ons voor dat het hier geen eis betreft, maar veeleer een maatregel. In dit geval wel een maatregel met nogal verstrekkende consequenties. Meer voor de hand zou liggen een eis te formuleren in de zin van 'Waarborgen dienen te worden getroffen om onbevoegde ontsluiting van de gegevens tijdens het transport uit te sluiten.'. Afhankelijk van de concrete situatie kan het gebruik van cryptografie dan als maatregel al dan niet aan de orde zijn.

Het voert te ver om in het bestek van dit artikel meer uitgebreid in te gaan op het advies van de Registratiekamer. Nu het advies op onderdelen meer het karakter heeft van maatregelen dan van eisen, impliceert dit een risico voor de houders van persoonsregistraties. De Registratiekamer treedt hiermee namelijk in de afweging welke in beginsel is voorbehouden aan de houder van de persoonsregistratie.

5 De overheidsaccountant en het VIR

In de Comptabiliteitswet wordt niet expliciet ingegaan op beveiligingsaspecten. Wel wordt in artikel 25 gesteld, dat de administratie moet voldoen aan de eisen van doelmatig beheer en controle. Voorts is in de Comptabiliteitswet bepaald dat de departementale accountantsdienst (DAD) tot taak heeft controle uit te oefenen op het gevoerde financiële beheer en de financiële verantwoording en op de administraties die ten behoeve daarvan worden gevoerd. Op basis van de Comptabiliteitswet is voorts de Algemene Rekenkamer belast met het rechtmatigheidsonderzoek (resultierend in een rapport bij de financiële verantwoording van het Rijk). Daarbij gaat zij onder meer na of er sprake is van een ordelijk en controleerbaar financieel beheer.

In het Besluit taak departementale accountantsdienst is bepaald dat de DAD belast is met de

controle van systemen die van belang zijn voor de financiële verantwoording. Voorts is de beoordeling van de continuïteit, de beveiliging, de privacybescherming en de controleerbaarheid bij grotere en geautomatiseerde administraties mede een object van beoordeling.

Voor de accountants van gemeenten is er niets centraal voorgeschreven. Ook de verplichting die de openbaar accountant op basis van de Wet Computercriminaliteit heeft om in zijn verslag naar aanleiding van de controle van de jaarrekening tevens melding te maken van zijn bevindingen inzake de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking, is niet van toepassing op de overheid, in casu de gemeenten (Schönfeld, 1995).

Artikel 3 van het VIR bevat de verplichting om het beveiligingsbeleid en de implementatie en uitvoering daarvan periodiek te laten beoordelen door een onafhankelijk deskundige. Gelet op de vereiste deskundigheid ligt het in de rede een dergelijke beoordeling te doen uitvoeren door een EDP-auditor. Binnen de rijksoverheid beschikken de DAD's over deze deskundigheid (in de EDP Audit Pool en de EDP Audit afdelingen van specifieke DAD's respectievelijk de Interne Accountantsdienst Belastingen).

6 Conclusie

We hebben in dit artikel willen aantonen dat de (rijks)overheid de laatste jaren informatiebeveiliging steeds meer als een volwaardig, professioneel beleidsterrein is gaan zien.

De overheid kan ook niet anders. Gegevens en informatiesystemen vormen inmiddels immers de onmisbare brandstof waarop veel beleids- en operationele bedrijfsprocessen binnen de overheid draaien.

Het adequaat beveiligen van deze gegevens en systemen is noodzakelijk geworden omdat zonder dat:

- het functioneren van de interne organisatie van de overheid ernstig verstoord kan worden. Inbreuken op het efficiënt en effectief functioneren hebben invloed op de bedrijfsvoering van de onderscheiden departementen, maar kunnen ook veroorzaken dat boven de verschillende departementen uitstijgende doelstellingen als gemeenschappelijke fraudebestrijding niet gehaald worden;

- aan de kwaliteit van het overheidshandelen naar de burger ernstig afbreuk kan worden gedaan;
- de privacy van de burgers geschaad kan worden.

Binnen de departementen en vooral ook binnen grote diensten als bijvoorbeeld de Belastingdienst, waar gegevensverwerking veelal het hoofdproces vormt, is men steeds meer gaan inzien dat informatiebeveiliging onderdeel uit moet maken van integraal management en lijnsturing. Bij de Belastingdienst bijvoorbeeld maakt informatiebeveiliging onderdeel uit van een geïntegreerde risicobeheersingsaanpak als managementproces. Op deze wijze tegen informatiebeveiliging aankijken betekent dat beveiliging steeds minder de positie van 'sluitpost' inneemt en steeds meer wordt beschouwd als een terrein dat toegevoegde waarde kan leveren aan de kwaliteitsverbetering van de totale geautomatiseerde informatievoorziening.

Aan de toegenomen bewustwording van het belang van informatiebeveiliging, vooral ook op topmanagementniveau, heeft ook zeker bijgedragen de effectieve, gecoördineerde overheidsaanpak die Binnenlandse Zaken door de instelling van het ACIB heeft gerealiseerd. Dit is in het belang van de totale overheid en van de burgers. De bewustwordingscampagne van de Belastingdienst op dit terrein voerde

dan ook niet voor niets het motto: 'Informatiebeveiliging:zorg voor kwaliteit!'

L I T E R A T U U R

- Stichting Samenwerkende Instellingen t.b.v. Beleidsanalytische Studies (SIBAS), (1989), *Kwetsbaarheid en Beveiliging van bestuurlijke informatiesystemen*.
- Schönfeld, C., (1995), Informatiebeveiliging bij Rijk en Gemeenten, *Openbaar bestuur*, 1.
- Lunteren, J.N. van, (1994), Complexe belastingwetgeving maakt intensieve uitwisseling gegevens onvermijdelijk, *Staatscourant* 172, 8 september.
- Aanwijzingen voor de Beveiliging van Staatsgeheimen en vitale onderdelen bij de Rijksdienst, (1989), SDU, 's-Gravenhage.
- Aanwijzingen inzake de beveiliging van persoonsgegevens, verwerkt en opgeslagen in geautomatiseerde gegevensverwerkende systemen bij de Rijksoverheid, (1982), Staatsuitgeverij, 's-Gravenhage.
- Voorschrift Informatiebeveiliging Rijksdienst, (1994), ministerie van Binnenlandse Zaken, 's-Gravenhage.
- Algemene Rekenkamer, *Beheersing informatiebeveiliging* (Tweede Kamer 1994-1995, kamerstuk 24.175), SDU, 's-Gravenhage.
- Registratiekamer, *Beveiliging van persoonsregistraties*, (1994), SDU, 's-Gravenhage.
- Ministerie van Economische Zaken, *Code voor Informatiebeveiliging*, Nederlands Normalisatie-instituut, Delft.