Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1994–1995

24 175 Beheersing informatiebeveiliging

Nr. 3

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 29 augustus 1995

De vaste commissie voor Binnenlandse Zaken[1] en de algemene commissie voor de Rijksuitgaven[2] hebben op 22 juni 1995 overleg gevoerd met staatssecretaris Kohnstamm van Binnenlandse Zaken over het **ARK-rapport Beheersing informatiebeveiliging** (kamerstuk 24 175).

Bij dit veslag is een brief van staatssecretaris Kohnstamm d.d. 14 juli 1995 als bijlage gedrukt.

Van het gevoerde overleg brengt de commissie bijgaand beknopt verslag uit.

Vragen en opmerkingen uit de commissie

De heer **Kamp** (VVD) begon zijn betoog met de opmerking dat het op zich gedegen ARK-rapport toch niet helder maakt wat het probleem informatiebeveiliging precies inhoudt. Zijns inziens gaat het om vijf risico's.

– Als er op een verkeerde manier met geïnformatiseerde bestanden wordt omgesprongen, gaat veel ambtelijk werk verloren.

– In het geval dat bestanden niet beschikbaar zijn of niet op de juiste manier gebruikt kunnen worden, zullen allerlei uitbetalingen of bijvoorbeeld belastinginning niet naar behoren kunnen geschieden.

– Bestanden kunnen al dan niet opzettelijk gemuteerd worden met alle (financiële) schade van dien.

– Als bestanden toegankelijk zijn voor mensen die daartoe niet het recht hebben, kan de privacy worden aangetast.

– Er kunnen veiligheidsrisico's worden gelopen als gevolg van het «op straat» komen van bestanden, vooral als het gaat om bestanden van het openbaar ministerie.

Onlangs is gebleken dat men via Internet toegang heeft weten te krijgen tot politiedossiers. Voorts is gebleken dat informatie van het openbaar ministerie te Amsterdam en te Rotterdam door werknemers is verkocht aan buitenstaanders.

Een tweede manco van het ARK-rapport is, dat de Algemene Rekenkamer zich bij haar onderzoek heeft geconcentreerd op de kerndepartementen, terwijl juist bijvoorbeeld zelfstandige bestuursorganen (ZBO's) grote geautomatiseerde bestanden kennen met infor-

[1] Samenstelling:
Leden: Van Erp (VVD), V.A.M. van der Burg (CDA), Te Veldhuis (VVD), Van der Heijden (CDA), De Cloe (PvdA), voorzitter, Janmaat (CD), Van den Berg (SGP), Scheltema-de Nie (D66), ondervoorzitter, Apostolou (PvdA), Kalsbeek-Jasperse (PvdA), Zijlstra (PvdA), Van der Hoeven (CDA), Remkes (VVD), Gabor (CDA), Koekkoek (CDA), Nijpels-Hezemans (AOV), Oedayraj Singh Varma (GroenLinks), Essers (VVD), Dittrich (D66), Dijksman (PvdA), De Graaf (D66), Cornielje (VVD), Rouvoet (RPF), Van Boxtel (D66) en Rehwinkel (PvdA).
Plv. leden: Korthals (VVD), Dankers (CDA), Van Hoof (VVD), Bijleveld-Schouten (CDA), Liemburg (PvdA), Poppe (SP), Schutte (GPV), Van 't Riet (D66), Van Heemst (PvdA), Noorman-den Uyl (PvdA), Vreeman (PvdA), Verhagen (CDA), Van der Stoel (VVD), Mateman (CDA), Mulder-van Dam (CDA), Van Wingerden, Rabbae (GroenLinks), H.G.J. Kamp (VVD), Assen (CDA), M.M. van der Burg (PvdA), Bakker (D66), Klein Molekamp (VVD), Leerkes (Unie 55+), Hoekema (D66) en Van Oven (PvdA).

[2] Samenstelling:
Leden: Schutte (GPV), De Korte (VVD), Van Rey (VVD), voorzitter, Terpstra (CDA), Smits (CDA), ondervoorzitter, Reitsma (CDA), Ter Veer (D66), De Jong (CDA), Ybema (D66), Witteveen-Hevinga (PvdA), Hillen (CDA), Van Heemst (PvdA), Leerkes (Unie 55+), Van Wingerden, Rabbae (GroenLinks), Noorman-den Uyl (PvdA), Vreeman (PvdA), Liemburg (PvdA), H.G.J. Kamp (VVD), Zonneveld (CD), Hoogervorst (VVD), Van der Ploeg (PvdA), Bakker (D66), Van Walsem (D66) en Hofstra (VVD).
Plv. leden: Van der Vlies (SGP), Klein Molekamp (VVD), Hessing (VVD), Van de Camp (CDA), Van der Linden (CDA), Wolters (CDA), Schimmel (D66), Heerma (CDA), Roethof (D66), Van Zuijlen (PvdA), Boers-Wijnberg (CDA), Duivesteijn (PvdA), Van Dijke (RPF), Hendriks, Rosenmöller (GroenLinks), Vliegenthart (PvdA), Adelmund (PvdA), Van Zijl (PvdA), Remkes (VVD), Marijnissen (SP), B.M. de Vries (VVD), Van Gelder (PvdA), Giskes (D66), Van Rooy (CDA) en Verbugt (VVD).

5K2292
ISSN 0921 - 7371
Sdu Uitgeverij Plantijnstraat
's-Gravenhage 1995

matie die de burgers rechtstreeks aangaat. De VVD-fractie wenst de toezegging dat het Voorschrift informatiebeveiliging rijksdienst (VIR) van toepassing zal worden verklaard op alle ZBO's.

Bij informatiebeveiliging gaat het om de beveiliging van gegevens van kaartenbak, PC en grote computersystemen. De verspreiding van gegevens over de gehele rijksdienst maakt het voor ieder ministerie noodzakelijk een goed beleid ter beheersing van de informatiebeveiliging te formuleren, dat goed uit te werken in plannen en die plannen goed uit te voeren. Tussen dat «goed» en het «volstrekt onvoldoende» van de ARK voor het Ministerie van Sociale Zaken en Werkgelegenheid (Sociale Zaken en Werkgelegenheid) zit veel te veel ruimte. De fractie wil dat het kabinet voor het einde van 1995 schriftelijke informatie aan de Kamer doet toekomen, waaruit kan worden geconcludeerd dat de problemen bij Sociale Zaken en Werkgelegenheid zijn opgelost en dat de informatiebeveiliging er naar behoren is geregeld.

Zelfs bij de ministeries die een goede voldoende hebben gekregen van de ARK ontbreekt er nog wel het een en ander, wat ernstig is omdat het bij beveiliging gaat om een cirkel van maatregelen. Ontbreekt daar iets aan, dan is de cirkel niet compleet en de beveiliging dus niet goed. Eigenlijk is bij geen enkel ministerie de informatie naar behoren beveiligd.

Iedere minister blijft verantwoordelijk voor wat op zijn/haar ministerie gebeurt, maar moet ook de coördinerend Minister van Binnenlandse Zaken informeren over de implementatie van de VIR op het ministerie, inclusief agentschappen, directies op afstand en ZBO's. Al deze informatie wordt verzameld in het jaaroverzicht Informatiebeveiliging. Aan de hand daarvan kan de Kamer controleren of alle mooie voornemens uit de jaaroverzichten ook worden uitgevoerd. Om dat echt mogelijk te maken, zal het jaaroverzicht drastisch van karakter moeten veranderen. Is het kabinet bereid om de ministeries, conform de wens van de Rekenkamer, een informatieplicht op te leggen richting Minister van Binnenlandse Zaken? Is de staatssecretaris bereid het jaaroverzicht zodanig aan te passen, dat het bruikbaar wordt voor de Kamer als controleur van het kabinet? Waar er zeer veel nieuwe ontwikkelingen op het gebied van de communicatietechnieken op handen zijn, zal het beheersen van de beveiliging er niet gemakkelijker op worden. Daarom dient de uitgangspositie van de rijksoverheid in dezen snel op orde te worden gebracht. De heer Kamp spoorde de staatssecretaris aan de gevraagde toezeggingen te doen en snel uit te voeren.

Mevrouw **Van der Burg** (PvdA) stelde ook vast dat uit het ARK-onderzoek blijkt dat de informatiebeveiliging bij alle ministeries te kort schiet. Zij somde vervolgens een aantal tekortkomingen op. De ARK concludeert dat de beheersing van de beveiliging ontoereikend is en dat de rijksoverheid nog steeds risico's loopt van onbekende omvang, zoals verlies en het uitlekken van gegevens en ongeautoriseerd gebruik van gegevens. De laatste tijd is met name de onvoldoende beveiliging van politiedossiers gebleken, wat zeer schadelijke gevolgen kan hebben. Het is op zich wel positief dat de situatie beter is dan in 1988, behalve bij het Ministerie van Sociale Zaken en Werkgelegenheid. Van ministeriële zijde is op Sociale Zaken en Werkgelegenheid toegegeven dat de beveiliging nog niet op orde is. Er wordt gewerkt aan verbetering, waarbij de aanbevelingen van de ARK voor het merendeel worden overgenomen. De PvdA-fractie is van mening dat er veel meer aandacht moet worden besteed aan de beveiliging, zowel door de afzonderlijke ministeries als door de coördinerend bewindspersoon, of dat nu de Minister of de Staatssecretaris van Binnenlandse Zaken is.

Een adequaat beveiligingsbeleid is onmisbaar, met name gezien de nieuwe technologische ontwikkelingen waardoor de datacommunicatie sterk toeneemt. De beveiliging moet daarmee gelijke tred houden. Dat vergt meer prioriteit voor de ontwikkeling van de beveiligingsplannen

binnen de ministeries en vooral binnen het management, want die beveiliging moet worden geïmplementeerd in de normale werkprocessen.

Het realiseren van een adequate beveiliging op de ministeries is nogal lastig. Afgesproken is dat de ministeries zelf verantwoordelijk zijn voor de beveiliging en dat de coördinerend bewindspersoon verantwoordelijk is voor het stimuleren van die beveiliging en voor het geven van richtlijnen. De Interdepartementale commissie informatiebeveiliging (ICIB) en het Advies- en coördinatiepunt informatiebeveiliging (ACIB) hebben goed werk gedaan voor de bewustwording van de ministeries. Per 1 januari jl. is het VIR in werking getreden. Er is dus wel wat gebeurd, maar te weinig. De staatssecretaris deelt die mening kennelijk en heeft aangekondigd dat de ICIB een opvolger op hoog strategisch niveau krijgt en dat hij er zelf zitting in zal nemen. Maar dat is nog onvoldoende.

Gelet op de geconstateerde tekortkomingen wenst de ARK terecht een sterkere rol van de coördinerend minister en een jaarlijkse rapportage over de beveiligingssituatie. Pas in 1997 zal de coördinerend minister bezien of de ministeries een periodieke informatieplicht moet worden opgelegd. De PvdA-fractie wenste de toezegging dat die plicht er komt en dat jaarlijks in het jaaroverzicht Informatiebeveiliging op soortgelijke wijze als in bijlage 3 van het ARK-rapport inzicht zal worden gegeven in de beveiligingssituatie van de verschillende ministeries.

Op bijna de helft van de ministeries ontbreekt een adequaat calamiteitenplan, terwijl het in noodsituaties mogelijk moet zijn gegevens te vernietigen. Wat is de actuele stand van zaken wat de noodvernietiging betreft? Wanneer zullen alle plannen gereed zijn? Welke extra druk wordt daarop vanuit het Ministerie van Binnenlandse Zaken uitgeoefend?

Hoewel de Wet persoonsregistratie (WPR) al enkele jaren van kracht is, is er nog steeds sprake van een forse achterstand bij het opstellen van privacyreglementen bij bedrijven en overheden. De Registratiekamer heeft hierop al vaak gewezen en heeft eind 1994 beveiligingsvoorschriften verspreid. De Ministeries van Financiën, Onderwijs, Cultuur en Wetenschappen en Volksgezondheid, Welzijn en Sport voldoen wel aan de norm. Hoe is de situatie bij de andere ministeries en op welke termijn zal de achterstand worden ingehaald? Welke druk oefent het Ministerie van Binnenlandse Zaken daarop uit?

Het is opvallend dat er veel te weinig risicoanalyses worden gemaakt, terwijl op basis daarvan juist kan worden beoordeeld welke maatregelen absoluut noodzakelijk zijn en wat die gaan kosten. Worden er te weinig risicoanalyses gemaakt door gebrek aan deskundigheid? Zo ja, hoe kan hierin dan verbetering worden gebracht?

Het Ministerie van Sociale Zaken en Werkgelegenheid beschikt over veel privacy-gevoelige gegevens, wat de slechte informatiebeveiliging nog ernstiger maakt. Ook mevrouw Van der Burg wilde nog in 1995 vernemen op welke wijze dit ministerie gaat voldoen aan de beveiligingseisen.

Ook zij wilde weten hoe een adequate beheersing van de informatiebeveiliging is geregeld bij ZBO's, agentschappen en dergelijke. Zij memoreerde in dit verband de problemen die zich enkele jaren geleden op dit stuk hebben voorgedaan met een verzelfstandigd orgaan van een Noordhollandse sociale dienst waarvoor de interne gemeentelijke beveiligingsregelingen niet bleken te gelden. Hoe gaat een ministerie, dat eigenaar is van de gegevens die bij een ZBO berusten, om met de daarmee overeengekomen beveiligingsprocedure? Gelden overeengekomen calamiteitenprocedures ook voor ZBO's?

Alle bestaande ZBO's worden momenteel op diverse aspecten doorgelicht. Mevrouw Van der Burg verzocht de staatssecretaris om de ZBO's ook door te lichten op het punt van de beveiliging en de Kamer daarover in 1996 te informeren. Ook zij was van mening dat de informatiebeveiligingsvoorschriften voor de ministeries ook moeten gelden voor de ZBO's.

Mevrouw **Assen** (CDA) onderschreef dat het belang van beveiliging van informatie steeds groter wordt als gevolg van de voortschrijdende automatisering en gegevensuitwisseling. Koppeling van bestanden wordt steeds belangrijker, maar levert wel een aantal risico's op. Bij de bespreking van de elektronische snelweg heeft de CDA-fractie grote nadruk gelegd op de inspanningen op het punt van de informatiebeveiliging, met name in verband met de privacybewaking. De criminaliteit heeft deze «markt» ontdekt. Regering en topdepartementen lijken dat belang steeds meer te beseffen. Ondanks de vooruitgang sinds 1988 bij vrijwel alle ministeries, is er nog een groot aantal onvolkomenheden en achterstanden bij de onderscheiden ministeries. De beheersing, besturing en beveiliging van de gegevens is onvoldoende. Het is van belang dat het proces van beveiliging voortgaat. Nieuwe ontwikkelingen, zowel op het terrein van de informatica en telecommunicatie als op het terrein van de beveiliging (nieuwe en grotere risico's) zouden de ministeries moeten dwingen tot voortvarend handelen. De achtergebleven ministeries moeten hun achterstand zo snel mogelijk inhalen. De CDA-fractie deelt de mening van de ARK dat een sterke coördinatie door de Minister van Binnenlandse Zaken (of namens hem door de staatssecretaris) belangrijk is, maar dan niet pas na de rapportage in 1997. Een tussenstandrapportage is gewenst.

Zeker nu ministeries steeds meer informatie uitwisselen en steeds meer informatiebestanden koppelen, neemt het belang van de coördinatie toe, niet in de laatste plaats met het oog op een adequate privacybescherming. Die coördinatie is ook noodzakelijk bij het begeleiden van het wegwerken van de achterstanden.

Beveiliging en informatie worden in de managementwereld gezien als een lijnmanagementkwestie. Dat is ook zichtbaar bij bedrijfsleven en overheid, die beide bezig zijn codes en voorschriften te ontwikkelen op het gebied van de informatiebeveiliging. De overheid doet dat via aanwijzingen en de Raad van de centrale ondernemingsorganisaties via leidraden. Deze codes en voorschriften dienen op elkaar afgestemd te worden om zo mogelijk een nationale standaard te bereiken. Informatiebeveiliging zou een vanzelfsprekend onderdeel van beleid moeten zijn. Het verdient aanbeveling dat Binnenlandse Zaken in zijn coördinerende rol relaties legt met andere overheden die met dezelfde problematiek kampen. Binnenlandse Zaken zal ook zelf het goede voorbeeld moeten geven.

Bij de beheersing van informatiebeveiliging moet niet alleen worden gekeken naar de organisatorische kanten, maar ook naar praktische zaken, zoals lekkage, diefstal en verlies van informatie, het onbedoeld wissen van brieven en bestanden en archivering. De toegang tot de elektronische informatie zal beveiligd moeten worden om een «bezetting», zoals onlangs bij Internet voorkwam, te voorkomen.

Er moeten centrale normen komen voor de screening van automatiseringspersoneel.

Mevrouw Assen herinnerde aan de toezegging van de minister van 15 juni jl. om de informatiebeveiliging op te nemen in de Kaderwet ZBO's.

Beschikken de departementale accountantsdiensten, die geautomatiseerde systemen moeten controleren op veiligheidsaspecten, wel over voldoende expertise op dat stuk?

Mevrouw **Roethof** (D66) merkte op dat in de titel van het ARK-rapport vooral de angst voor ontsnapping van informatie tot uitdrukking wordt gebracht. Er spreekt nogal wat onmacht uit het rapport over een fenomeen dat zich niet gemakkelijk laat beteugelen.

De elektronische informatie-uitwisseling tussen overheid en burger neemt toe. In vrij korte tijd is de informatisering van hele beleidsterreinen gerealiseerd. De informatiebeveiliging heeft geen gelijke tred gehouden met die ontwikkeling. Dat betekent ook dat de overheid in gebreke is gebleven.

Het is de vraag of dit probleem kan worden opgelost door een bewindspersoon – is dat nu de Minister of de Staatssecretaris van Binnenlandse Zaken? – coördinerende bevoegdheden te geven en de leiding van ministeries te belasten met het sturen van en het toezicht houden op de informatiebeveiliging. De D66-fractie vraagt zich af of dit probleem wel op hiërarchische wijze kan worden opgelost. De minister koesterde kennelijk dezelfde twijfel, want hij is van oordeel dat de verantwoordelijkheid voor afdoende beveiliging het meest effectief gerealiseerd kan worden door een decentrale aanpak. De Rekenkamer vindt evenwel dat bovendepartementale toezicht belangrijk, mede omdat de Tweede Kamer aan de hand daarvan kan oordelen. Mevrouw Roethof geloofde evenwel niet in de fictie van de Rekenkamer dat het probleem te beteugelen is via strakke leiding.

Bevat het rapport een reële beschrijving van de werkelijkheid of antwoorden van de ambtelijke top op gestelde vragen? In het laatste geval is het de vraag of het rapport spoort met de werkelijkheid. Misschien was het management onvoldoende geïnformeerd of is er een vraagstelling gehanteerd die voorbijging aan de echte problemen op dit gebied. Zij vreesde het laatste.

Immers, het gaat om databanken, adressenbestanden, elektronische betaal- en inningssystemen die buitengewoon kwetsbaar zijn. Er zijn meestal geen alternatieve mogelijkheden om bij uitval te voldoen aan de overheidsverplichtingen. Is de staatssecretaris het ermee eens dat veel te weinig ministeries zijn voorbereid op zo'n situatie? De moderne overheid kan niet meer zonder informatietechnologie en wordt er steeds afhankelijker van. De automatisering heeft ook directe invloed gehad op de organisatie van de verzorgingsstaat. Informatiebeveiliging kan derhalve geen randverschijnsel zijn. Die beveiliging heeft alleen een kans van slagen als deze tegelijk met het informatiesysteem wordt opgezet. Het moet daarbij gaan om: confidentiality, availability en integrity (CAI). De Rekenkamer kiest als uitgangspunt wat de deskundigen noemen het Fort Knox-concept, waarbij ervan wordt uitgegaan dat de informatie zich in een kluis bevindt die zwaar wordt bewaakt. Die benadering is evenwel strijdig met het streven naar een elektronische snelweg.

In reactie op de bij interruptie gemaakte opmerking dat de Rekenkamer juist procedures wenst waardoor de beveiliging als het ware vanzelf verloopt, zei mevrouw Roethof dat de Rekenkamer meent dat de informatiebeveiliging het best is gediend met een benadering langs hiërarchische lijnen. Haars inziens moet juist meer worden gewerkt met richtlijnen en gedragsnormen en moet meer worden vertrouwd op de decentrale aanpak, omdat het elektronische verkeer tussen burger en overheid op korte termijn zeer sterk zal toenemen. Er moet een oplossing voor het beveiligingsprobleem worden gevonden zonder dat de ontwikkelingen in de informatieverschaffing worden afgeremd. Zou de staatssecretaris uit de voeten kunnen met die CAI-voorwaarden? Of wil hij andere criteria introduceren? Er moeten in ieder geval heldere normen worden gecreëerd om bij het toezicht te hanteren, zonder dat dit al te strak gebeurt. Wat gaat de opvolger van de ICIB doen?

Het is belangrijk het beveiligingsbeleid op peil te brengen, niet in de laatste plaats omdat de overheid ook het mikpunt kan zijn van computerkraak. De overheidsnetwerken bevatten veel vertrouwelijke gegevens, die voor een groot deel commerciële waarde hebben. Het is teleurstellend dat uitgerekend het Ministerie van Justitie slecht scoorde op punten als toegang tot gegevens, systeemontwikkeling, personele maatregelen en toetsbaarheid van fysieke beveiliging. Is al duidelijk wanneer de Kamer de door de Minister van Justitie toegezegde informatie zal ontvangen over een gestructureerde aanpak van de informatiebeveiliging?

Welke ervaringen heeft de overheid met computerkraak? Is de Wet op de computercriminaliteit een effectief instrument? Kan de Kamer, zo nodig

vertrouwelijk, worden geïnformeerd over aantal en aard van computerdelicten tegen de overheid?

Het is hoogst merkwaardig dat vijf van de dertien ministeries te kort schieten in het naleven van de WPR, die uit 1988 dateert. Zijn de reglementsverplichtingen te bewerkelijk of is men te laks geweest? In het laatste geval zou bovendepartementale leiding op dit punt wèl nodig zijn. De gemeenten hebben, daartoe aangespoord door een handhavingscampagne, inmiddels aan de eisen voldaan. Op welke termijn zullen de ministeries en de ZBO's daar ook aan kunnen voldoen?

Inderdaad moet meer aandacht worden besteed aan de beveiliging van informatie die bij de ZBO's ligt opgeslagen. De Rekenkamer voegt daar de Hoge Colleges van Staat aan toe. Immers, ook op die terreinen is cruciale informatie in gebruik. Het bestand van de studiefinanciering bijvoorbeeld is privacygevoelig en ook kwetsbaar omdat het uniek is en aantrekkelijk is om te kraken.

Is het waar dat er vanuit de werkgeversorganisaties wordt aangedrongen op privacybescherming van bedrijfsgegevens? Zo ja, wat vindt het kabinet daar dan van? Hoe denkt de staatssecretaris te laveren tussen de informatiebeveiliging en de wens tot meer openbaarheid? Uit de BIOS-nota blijkt dat hij bij het informatiebeleid juist wil uitgaan van een loketfunctie van de overheid en van een intensiever contact tussen burger en overheid. Zou dat gevolgen hebben voor de CAI-normen, bijvoorbeeld doordat het niet-beschikbare, dus vertrouwelijke deel van overheidsinformatie extra moet worden beveiligd? Blijft het uitgangspunt dat bestanden nimmer mogen worden gekoppeld volledig overeind? Of wordt de verleiding groot om enkele databanken te koppelen en gegevens te gebruiken voor andere doeleinden dan die waarvoor zij zijn ingezameld? Dat laatste zou mevrouw Roethof met het oog op de rechtszekerheid zeer betreuren.

Antwoord van de regering

De **staatssecretaris** was ervan overtuigd dat ook in de huidige situatie informatiebeveiliging zowel politiek als managerial een onvoldoende erkend belang is bij het doen en laten van het openbaar bestuur. Informatiebeveiliging zal inderdaad in de naaste toekomst een nog grotere rol gaan spelen naarmate er meer met netwerken wordt gewerkt en er meer uitvoering wordt gegeven aan de plannen die zijn gepresenteerd in het Nationaal actieplan en de nota Terug naar de toekomst. Bij uitvoering van de één-loketgedachte zal veel informatie samenkomen. Op de langere termijn zal elektronische communicatie tussen burgers, bedrijven en overheid veel gewoner zijn dan nu. Informatiebeveiliging wordt dan nog belangrijker dan nu al het geval is. Als die beveiliging nu niet goed wordt aangepakt, zullen er straks grote problemen kunnen ontstaan.

Het ARK-rapport zou inderdaad door velen als (informatie)technisch ter zijde kunnen worden geschoven, omdat de politieke en maatschappelijke dilemma's die erachter schuilen niet zo duidelijk zijn verwoord.

Informatiebeveiliging is een weerbarstige materie waarvoor in Nederland noch in andere landen waarin erover wordt nagedacht, een soort standaardoplossing is gevonden. De staatssecretaris zei een aantal aanzetten te zullen geven tot een oplossing, overigens enigszins in de richting van wat vanuit de Kamer is verwoord. Er is alle reden om alert te zijn en te blijven om ervoor te zorgen dat informatie niet in handen komt van mensen die er niet aan mogen komen en om te voorkomen dat iemand die informatie mag ontvangen, informatie krijgt die door derden is vervormd, met alle risico's van dien bij gebruik van die informatie. Er zijn meer situaties die het van het grootste belang maken om dit punt zo hoog mogelijk op de politieke agenda te plaatsen en zo min mogelijk te (doen) ervaren als een zaak voor technici. Politieke sturing in dezen is niet alleen

nuttig, maar ook noodzakelijk voordat men de elektronische snelweg opgaat.

Inderdaad moet informatiebeveiliging eigenlijk worden geregeld op het moment waarop de informatietechnologie wordt geïmplementeerd. In de nota Terug naar de toekomst is voor een aantal initiatieven, zoals het Overheidsnetwerk 2000, vastgelegd dat er direct afspraken worden gemaakt over de beveiliging. Waar bij dat netwerk ook de belastingdienst is betrokken, mag worden verwacht dat dit een belangrijke spin-off zal hebben wat de alertheid op beveiliging betreft.

De staatssecretaris ging vervolgens in op de bijna onoplosbare knoop van de coördinerende bevoegdheid van Binnenlandse Zaken en de mate waarin dit een meestal hiërarchisch supertoezicht moet uitoefenen. Overigens is de staatssecretaris en niet de minister in dezen de verantwoordelijke bewindspersoon, enige misverstanden ten spijt.

Wil men succesvol het bewustzijn kweken dat beheersing van informatiebeveiliging noodzakelijk is, dan zal vanaf het begin volstrekt helder moeten zijn waar de politieke verantwoordelijkheid daarvoor ligt. Volgens de staatssecretaris schiet de Kamer naast haar doel als zij die verantwoordelijkheid te veel bij hem legt. Hij gaf aan dat primair de eigen verantwoordelijkheid bij het ministerie zelf moet liggen. Hij voelde er weinig voor om binnen het kabinet als een soort politiefunctionaris te moeten optreden in het kader van de decentrale bevoegdheden in de sfeer van informatiebeveiliging. Een andere vraag is hoe de informatie over de informatiebeveiliging zodanig ter tafel kan worden gebracht, dat de direct verantwoordelijken daarop voor een deel door de staatssecretaris en voor een ander deel door de Kamer kunnen worden aangesproken.

Desgevraagd verklaarde de staatssecretaris dat het volgens hem in staatsrechtelijke zin heel ongebruikelijk is dat een bewindspersoon controleert of de door een collega-bewindspersoon verschafte gegevens correct zijn. Hij was van mening dat hij ervan moest uitgaan, dat wat bijvoorbeeld de Minister van Sociale Zaken en Werkgelegenheid in reactie op het ARK-rapport heeft gezegd, juist is en dat deze zal doen wat hij heeft gezegd. De controle daarop moet niet door de coördinerend staatssecretaris worden uitgevoerd, maar door de Kamer. Hij zal conform het heden gedane verzoek van de Kamer de Minister van Sociale Zaken en Werkgelegenheid met klem vragen om in de memorie van toelichting op de begroting of in een afzonderlijk stuk te rapporteren over de vorderingen met de toegezegde verbeteringen op het stuk van de informatiebeveiliging.

De staatssecretaris ontkende dat hij in dezen een brievenbusfunctie vervult, zoals bij interruptie werd verondersteld. Hij had bijvoorbeeld het VIR in het kabinet gebracht en probeerde ook collega-bewindspersonen op dit terrein aan te spreken, maar het door hem verrichten van de pure controle op de juistheid van op zijn verzoek verstrekte gegevens is volgens hem staatsrechtelijk gezien een brug te ver. De coördinatie is erop gericht te bewerkstelligen dat iedereen optimaal de eigen verantwoordelijkheid ter hand neemt en ervoor zorgt dat het volgende rapport van de Rekenkamer een aanzienlijke verbetering te zien zal geven in vergelijking met dit rapport. Daartoe wordt andere ministeries gevraagd hoe het gaat met de informatiebeveiliging en of zij hulp nodig hebben. Daarbij is ook het Informatiebeveiligingsberaad (IBB) actief.

De staatssecretaris was het in essentie eens met de bij interruptie geschilderde weergave van de gang van zaken waarbij hij als coördinerend bewindspersoon de Kamer een jaaroverzicht moet geven, waarin hij de VIR-informatie van de ministeries verzamelt en verwoordt op welke wijze het VIR volgens hem door de ministeries wordt uitgevoerd en wat zijn algemene conclusies zijn, waarna de Kamer hem kan aanspreken op het beeld van dat geheel.

De staatssecretaris wees erop dat hij zijn eerste jaaroverzicht Informatie-

voorziening in de ministerraad aan de orde had gesteld en het vervolgens eind 1994/begin 1995 aan de Kamer had toegestuurd. Volgens hem is het evenwel een bureaucratisch stuk waaraan Kamer noch ministerraad veel heeft bij de beoordeling van de feitelijke gang van zaken. In het kabinet is afgesproken dat men zich opnieuw zal beraden op frequentie en inhoud van de jaaroverzichten. Graag vernam de staatssecretaris van de Kamer welke functie het jaaroverzicht zou kunnen hebben in het kader van het zodanig verzamelen van informatie, dat hierdoor een volledig beeld van de rijksdienst als geheel wordt geboden. Waar het beveiligingsvraagstuk bij uitstek relevant is, is het zeer wel denkbaar dat het jaaroverzicht wordt omgevormd tot een overzicht dat meer in het bijzonder daarop betrekking heeft. Informatiebeveiliging zou wel eens de relevantste achilleshiel kunnen zijn van de hele operatie tot verdere implementatie van de informatie- en communicatietechnologie.

Gevraagd of hij het ermee eens is dat hij wel degelijk een coördinerende taak heeft inzake de WPR en het voldoen aan de daarin opgenomen reglementsverplichtingen, zei de staatssecretaris dat deze zaak net iets anders ligt, omdat hierbij sprake is van een wet die moet worden nageleefd en niet van onderling gemaakte afspraken.

In het kabinet is afgesproken dat de direct verantwoordelijken decentraal de acties ondernemen die staan omschreven in het VIR en dat er begin 1997 een eerste rapportage over komt. De staatssecretaris wilde wel nagaan of in 1996 een tussenrapportage mogelijk is, maar vreesde dat er dan nog niet zoveel nieuws te melden zal zijn. In ieder geval zou hij begin 1997 met een rapportage komen over het geheel, mede tegen de achtergrond van de evaluatie van het VIR. Hij hoopte dan goed nieuws te kunnen melden en met de Kamer over die rapportage te kunnen spreken.

In reactie op het bij interruptie gedane verzoek om toch eerder op enigerlei wijze informatie te verstrekken over de informatiebeveiliging herinnerde de staatssecretaris eraan dat de diverse ministers hebben toegezegd in de memorie van toelichting op hun begroting te zullen rapporteren over datgene wat er in die ministeries gebeurt op het stuk van de informatie- en communicatietechnologie. De individuele bewindslieden zullen dan door de Kamer direct op hun verantwoordelijkheid kunnen worden aangesproken. De staatssecretaris zegde toe, te zullen proberen de evaluatie van het VIR iets te bespoedigen, maar veronderstelde dat pas in de tweede helft van 1996 met enig resultaat een evaluatie zal kunnen worden uitgevoerd, omdat het VIR pas op 1 januari 1995 van kracht is geworden. Hoe dan ook zullen Kamer en kabinet op dit punt veel sneller met elkaar komen te spreken dan tot op heden het geval is geweest.

Desgevraagd beloofde de staatssecretaris zijn uiterste best te zullen doen om de Kamer, zodra dat beleidsinhoudelijk zinvol is, te rapporteren over de voortgang van de implementatie van het VIR bij de rijksdienst.

Inderdaad moet de informatiebeveiliging bij de ZBO's goed worden geregeld. Zoals in het ARK-rapport staat, zal de ministerraad een voorstel worden voorgelegd om de toepassing van het VIR bij deze organisaties strakker te regelen. Dan zal ook kunnen worden bekeken wat de toepasbaarheid van het VIR is bij de Hoge Colleges van Staat. In het voorstel zal uiteraard rekening worden gehouden met de wijze waarop het kabinet met de ZBO's in het algemeen omgaat. Omdat de verschillen tussen de ZBO's nogal nauw luisteren, moest nader uitgezocht worden hoe in het VIR kan worden opgenomen dat de informatiebeveiligingsvoorschriften ook op de ZBO's van toepassing zijn. Het rechtstreeks van toepassing verklaren van het VIR zou bovendien een zwaardere regelgeving vereisen dan een intern voorschrift van de rijksdienst. Dat laat onverlet dat het VIR rechtstreeks toepasbaar zou kunnen zijn op ZBO's, zoals de Informatiebeheergroep en het Kadaster. Om een goede regeling te kunnen creëren, worden in hoog tempo acties uitgevoerd zoals het inventariseren van de juridische mogelijkheden om het VIR van toepassing te verklaren op die ZBO's waarbij dat zinvol is. Dat gebeurt in samenhang met de

ZBO-activiteiten naar aanleiding van het ZBO-rapport van de ARK. Bij de inventarisatie van de groep ZBO's waarvoor het VIR inhoudelijk rechtstreeks van toepassing kan worden verklaard en de groep waarvoor dat niet het geval is, zal vooral naar de kleine ZBO's worden gekeken. Er zal een specifieke regeling worden ontworpen waaraan die tweede groep inhoudelijk dient te voldoen. Tot slot wordt nagegaan of er een nadere regeling nodig is om te garanderen dat de ministeries voldoende geïnformeerd zijn over de toestand van de informatiebeveiliging bij «hun» ZBO('s). Al deze acties zijn bedoeld om het door de ARK geconstateerde gat te dichten. De minister zal de Kamer te zijner tijd informeren over het resultaat van een en ander.

Of in de doorlichting van de ZBO's ook de huidige regeling van de informatiebeveiliging bij de ZBO's wordt meegenomen, was de staatssecretaris niet bekend. Die vraag zal schriftelijk worden beantwoord.

Toetsing en controle in het kader van de WPR liggen in eerste instantie op het werkterrein van de Registratiekamer. Het werkingsgebied is een complexe materie. Onlangs is er een richtlijn tot stand gekomen over de exclusiviteitsklassen van persoonsgegevens. Het is dan ook niet geheel verwonderlijk dat de privacyreglementen langzamer tot stand komen dan gewenst. Er is nu per ministerie een privacy-officer aangesteld die de totstandkoming van de reglementen moet regelen. De Registratiekamer begint thans met de directe controle hierop.

Noodvernietiging wordt in eerste instantie gezien als onderdeel van de calamiteitenparagraaf. Het ACIB zal dit najaar een brochure uitbrengen over die paragraaf om het mogelijk te maken dat de ministeries handen en voeten geven aan dit onderdeel van de informatiebeveiliging. Er wordt ook een aantal informatieve bijeenkomsten georganiseerd voor de ministeriële ambtenaren die belast zijn met de uitvoering van de calamiteitenparagraaf.

De staatssecretaris beaamde dat de toenemende mogelijkheden op het terrein van de informatieverschaffing grote alertheid vergen op het punt van beveiliging.

Het Ministerie van Economische Zaken en het VNO hebben de Engelse code voor informatiebeveiliging overgenomen. Het verband tussen de beveiligingsstelsels van overheid en bedrijfsleven is in kaart gebracht. Inhoudelijk zijn er nauwelijks of geen verschillen, wat logisch is omdat men daarover al eerder informatie heeft gewisseld. In een soort PR-operatie wil men binnen overheid en bedrijfsleven grotere bekendheid geven aan de samenhang en overeenstemming. De Registratiekamer heeft in het kader van artikel 8 van de WPR een beveiligingsadvies uitgebracht. Dat wordt inhoudelijk vergeleken en in relatie gebracht met het VIR.

De CAI-normen zijn de essentialia voor beveiliging. Inderdaad moet men zich daar constant van bewust zijn. Dit moet ook op het decentrale niveau worden gedragen, want het is nu eenmaal mensenwerk.

Het IBB is samengesteld uit de plaatsvervangende SG's van alle ministeries. Dat is een uitbreiding van de rol van het voormalige ICIB. Het IBB is gericht op de normale beveiliging van de bedrijfsprocessen en heeft onder meer tot taak interdepartementale afstemming inzake informatiebeveiliging. Het moet de ontwikkelingen op dit gebied volgen, niet alleen op technisch, maar vooral ook op maatschappelijk gebied. Het moet prioriteiten in de aanpak stellen om te komen tot een verantwoord beveiligingsniveau. Voorts moet het IBB instrumenten ontwikkelen om informatiebeveiliging te beheersen en nagaan of een systeem van intercollegiale toetsing kan worden opgezet. Volgens de staatssecretaris is dat een van de beste methodes voor de controle op de naleving van afspraken.

Hij beaamde dat ook van werkgeverszijde wordt aangedrongen op privacybescherming van bedrijfsgegevens. Het VNO heeft duidelijk gemaakt dat het voor het bedrijfsleven naarmate er meer elektronisch

wordt gecommuniceerd tussen overheid en bedrijfsleven, van steeds groter belang wordt dat overduidelijk is dat de gegevens die op verzoek van de overheid worden verstrekt, alléén worden gebruikt voor het doel waarvoor ze gevraagd zijn en dat deze gegevens niet verder worden verspreid. Elke gedachte aan elektronische communicatie op grote schaal tussen overheid en bedrijfsleven, ook als het gaat om wettelijk opgelegde verplichtingen, is illusoir als er geen goed reglement is ter bescherming van de gegevens. Het stond de staatssecretaris nog niet concreet voor ogen hoe hieraan vorm moet worden gegeven.

Er is een aantal positieve ontwikkelingen te onderkennen wat computerkraken bij de overheid betreft. Het instellen van een incidentenrapportage is volgens het VIR verplicht. De Minister van Justitie heeft recentelijk het meldpunt voor gevallen van computercrimaliteit nieuw leven ingeblazen. leder ontdekt incident is aanleiding om reactief maatregelen bij te stellen. Proactief is het opstellen van een risicoanalyse, ook overeenkomstig de richtlijnen in het VIR.

Voor zover de departementale accountantsdiensten onvoldoende kennis hebben van de beveiliging van informatiesystemen, kunnen zij gebruik maken van de EDP-audit pool. De meeste accountantsdiensten hebben de afgelopen jaren zelf meer ervaring opgebouwd.

Nadere gedachtenwisseling

De heer **Kamp** (VVD) noemde de toezeggingen over het Ministerie van Sociale Zaken en Werkgelegenheid en de ZBO's voldoende.

Hij was het ermee eens dat er gelegenheid moet zijn om het nieuwe VIR goed te implementeren en dat er niet tussentijds energie moet worden verspild aan evaluatie-onderzoek. Hij wilde de evaluatie verschuiven naar eind 1996/begin 1997, maar zou het resultaat graag met ingang van dat moment verwerkt willen zien in een aangepast jaaroverzicht. Derhalve verzocht de heer Kamp de staatssecretaris te bevorderen dat de ministers wordt voorgeschreven dat zij jaarlijks over de implementatie van de VIR moeten rapporteren aan het Ministerie van Binnenlandse Zaken. Hij verzocht hem er zelf voor te zorgen dat de informatie in de goede vorm en volledig wordt gegeven en het geheel te beoordelen en van een conclusie te voorzien, om het vervolgens in de vorm van een opgewaardeerd jaaroverzicht aan de Kamer te doen toekomen, opdat die inhoud kan geven aan haar controlerende taak op het stuk van de beheersing van informatiebeveiliging.

Mevrouw **Van der Burg** (PvdA) meende zich te herinneren dat het kamerlid Kohnstamm bij motie heeft bewerkstelligd dat de Kamer het jaaroverzicht krijgt.

Het blijft een weerbarstige materie met als eerstverantwoordelijken de ministeries, maar er zijn middelen nodig om alert te kunnen blijven. Dat geldt ook voor de Kamer. Vandaar de wens om zo vroeg mogelijk een evaluatierapport te ontvangen. Mevrouw Van der Burg wenste jaarlijkse informatie op dit stuk. Het kwam haar gewenst voor om te overleggen over de beste opzet van het jaaroverzicht, uitgaande van die noodzakelijke alertheid.

Mevrouw **Assen** (CDA) was blij dat uit de discussie duidelijker naar voren is gekomen wat de coördinerende rol van de Staatssecretaris van Binnenlandse Zaken in dit opzicht moet zijn.

Mevrouw **Roethof** beaamde dat het belangrijk is om het risico van misleiding door misvorming van informatie te voorkomen. Dat zou kunnen door in de contacten met de burger zo snel mogelijk te komen tot een elektronische handtekening of iets van dien aard.

Zij was bang dat in het geval dat de jaaroverzichten als toetssteen worden gebruikt, andere ministeries dat als excuus kunnen gebruiken om niet zelf te letten op en verantwoordelijkheid te nemen voor hun eigen informatiebeveiliging. De Kamer zal daar bij de afzonderlijke begrotingen op moeten letten.

De **staatssecretaris** was zich er niet van bewust dat hij mogelijk zelf de jaaroverzichten heeft veroorzaakt.

Volgens de opsteller van een soort Amerikaanse BIOS-3-nota staat het risico van misleiding ook in de VS te weinig op de agenda. In de VS wordt ook naar een 100% sluitende aanpak gezocht. Internet wordt een van de slechtst beveiligde grote netwerken genoemd, terwijl het eigenlijk voortvloeit uit een initiatief van het Amerikaanse ministerie van Defensie. Het is duidelijk dat er nog veel kan worden gedaan aan veiligheids-bewustzijn.

De staatssecretaris was bereid op enigerlei wijze te komen tot een gedachtenwisseling over de vraag, welke vorm en inhoud het jaarover-zicht moet krijgen, wil een vervolg daarop zinvol zijn. Dat staat in eerste aanleg los van zijn toezeggingen over de beveiligingsfollow-up. Of de beveiligingsrapportage eind 1996/begin 1997 in het jaaroverzicht zal worden gegeven, liet hij in verband met het voorgaande open. Mocht bij de eerste evaluatie van het VIR blijken, dat het nuttig en nodig is, dan was hij bereid om te bezien of een niet in het VIR opgenomen verplichting tot jaarlijkse rapportage noodzakelijk is.

De voorzitter van de vaste commissie voor Binnenlandse Zaken,
De Cloe

De voorzitter van de algemene commissie voor de Rijksuitgaven,
Van Rey

De griffier van de algemene commissie voor de Rijksuitgaven,
Hubert

BIJLAGE

Aan de voorzitters van de
– vaste commissie voor Binnenlandse Zaken
– algemene commissie voor de Rijksuitgaven

's-Gravenhage, 14 juli 1995

Tijdens het algemeen overleg op 22 juni jl. heb ik toegezegd u nader te informeren over de wijze waarop het onderwerp informatiebeveiliging aan de orde komt bij de doorlichting van de bestaande ZBO's.

Recent heeft het kabinet het advies van de Raad van State ontvangen over de nieuwe Aanwijzingen inzake zelfstandige bestuursorganen. Van die nieuwe Aanwijzingen zijn in dit verband de nummers 124s en 124t van belang. In artikel 124s wordt de verplichting vastgelegd om jaarlijks door een ZBO een verslag uit te laten brengen aan de minister. In artikel 124t wordt de verstrekking van inlichtingen door een ZBO aan de minister voorgeschreven. Daarmee is voor de nabije toekomst in ieder geval verzekerd dat een minister zich volledig op de hoogte kan stellen van de beheersing van de informatiebeveiliging bij ZBO's en daarover desgewenst verantwoording af kan leggen.

Op dit moment bereidt de Ministerraad een plan van aanpak voor dat voorziet in doorlichting van ZBO's en waar nodig een reparatie van het aansturingsinstrumentarium. Dit plan van aanpak zal in het voorjaar van 1996 tot tastbare resultaten leiden. Vooruitlopend daarop ben ik van plan om voor het onderwerp informatiebeveiliging, nu eerst de stappen te zetten die ik u al in het algemeen overleg kon melden. Het gaat immers slechts om een betrekkelijk gering onderdeel van het geheel van de ZBO-problematiek. Ik verwacht daarom nog dit jaar een voorstel aan de Ministerraad te kunnen doen waarin de expliciete vastlegging van de vereisten ten aanzien van informatiebeveiliging bij ZBO's is vastgelegd.

De Staatssecretaris van Binnenlandse Zaken,
J. Kohnstamm