Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1998–1999

20 644 Informatievoorziening Openbare Sector

Nr. 36

BRIEF VAN DE MINISTER VOOR GROTE STEDEN- EN INTEGRATIEBELEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

's-Gravenhage, 27 april 1999

In zijn schriftelijke beantwoording van vragen uit het Algemeen Overleg met de Tweede Kamer van 19 maart 1998 (brief d.d. 23 april 1998, kenmerk BIO98/U559) geeft de Staatssecretaris van Binnenlandse Zaken aan dat hij voornemens is om in het voorjaar van 1999 een nadere rapportage uit te brengen inzake de invoering van het Voorschrift Informatiebeveiliging Rijksdienst 1994 (VIR). Deze brief geeft invulling aan dit voornemen.

Bij het opstellen van deze rapportage is aan de departementen gevraagd om op beknopte wijze en in kwalitatieve zin aan te geven hoe de stand van zaken ten aanzien van de invoering van het VIR is. Een weerslag van deze stand van zaken is hieronder opgenomen. De volledige rapportages van de ministeries zijn als bijlage toegevoegd[1].

Stand van zaken invoering VIR

De invoering van het VIR binnen de rijksoverheid gaat gestaag door. De doelstelling van het VIR is het op adequate wijze regelen van een goed stelsel van informatiebeveiliging binnen de departementen. Dit stelsel kenmerkt zich door de zorg voor de integriteit van systemen en informatie, vertrouwelijkheid van informatie en continuïteit van informatie en informatiesystemen.

Ten aanzien van integriteit en continuïteit moet gesteld worden dat veel aandacht en inzet op het gebied van informatiebeveiliging gericht is op het oplossen van het millennium-probleem. Het oplossen van het millennium-probleem is van cruciaal belang voor een kwalitatief goede informatievoorziening binnen de departementen en de daaronder ressorterende diensten. Bij het schrijven van deze rapportage wordt voorzien dat ook in de nog resterende tijd tot in het eerste kwartaal van 2000 hiervoor veel aandacht nodig zal zijn. De analyses die in het kader van het oplossen van het millennium-probleem nodig zijn hebben echter

[1] Ter inzage gelegd bij de afdeling Parlementaire Documentatie.

KST35082
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 1999

ook een functie en voordeel voor de invoering van het VIR. Door de analyses wordt een goed beeld verkregen van het totale aantal systemen binnen de departementen en het onderscheid tussen essentiële en ondersteunende systemen. Daarbij is de aanpak van het VIR, dat redeneert vanuit de belangrijke en essentiële bedrijfssystemen, bij een groot aantal departementen gevolgd om de analyses in het kader van het millennium-probleem vorm te geven.

Bij het opstellen en implementeren van informatiebeveiligingsplannen wordt gebruik gemaakt van de in het VIR opgevoerde methode van afhankelijkheidsen kwetsbaarheidsanalyses (A&K-analyses). Deze methode, waarbij uitgegaan wordt van de bedrijfsprocessen en het belang van de informatiesystemen voor de juiste uitvoering van deze bedrijfsprocessen, wordt steeds meer gezien als essentieel voor een goede informatiebeveiliging. Omdat een handmatige methode voor de uitvoering van de A&K-analyses te veel werk met zich meebracht, is een software-pakket door en voor de departementen ontwikkeld, dat bekend staat onder de naam ESAKa (ExpertSysteem Afhankelijkheids- en Kwetsbaarheidsanalyse). Met behulp van dit pakket kunnen door departementen beveiligings- en implementatie- plannen worden opgesteld.
Hierbij wordt wel opgemerkt dat in de praktijk blijkt dat de volledige invoering van het VIR ook met ondersteuning van een geautomatiseerd instrument een complexe zaak blijft, zoals ook in de rapportage van 1997 reeds is aangegeven. De ingewikkeldheid van de digitale wereld is door de millennium-problematiek nog eens extra bevestigd. Om informatiebeveiliging adequaat aan te pakken is in het VIR een methode gekozen die nieuw was en waarvoor de instrumenten nog volledig ontwikkeld moesten worden. Wel kan gesteld worden dat deze methode met de focus op de bedrijfsprocessen en de rol van de verantwoordelijke manager daarbij en het inzetten van afhankelijkheids- en kwetsbaarheidsanalyses, alsmede het stimuleren van bewustwordingsprocessen op alle niveaus veel weerklank vindt, en in toenemende mate ook in het bedrijfsleven. De invoering van het VIR heeft derhalve een proces losgemaakt, waardoor er continue aandacht is voor informatiebeveiliging binnen de departementen. In dit proces worden nieuwe ontwikkelingen meegenomen (denk bijvoorbeeld aan het gebruik van internet). In die zin worden ook op dit terrein goede vorderingen gemaakt. Zo is een Internetgedragscode in ontwikkeling en zal voor de zomer een architectuur voor beveiligd e-mail besproken kunnen worden.

Op het terrein van de interdepartementale afstemming heeft het Informatiebeveiligingsberaad (IB-beraad) in de afgelopen 3 jaar veel werk verricht. In het IB-beraad is voorgesteld om het werkterrein van een dergelijk gremium uit te breiden naar het hele terrein van ICT-ontwikkelingen binnen de rijksoverheid. Daartoe is nu een omzetting in de maak waarbij gekomen zal worden tot een zogenaamd ICT-beraad. De wijze waarop de ondersteuning van het IB-beraad werd uitgevoerd zal worden gecontinueerd. In dit ICT-beraad zal het onderwerp van de algemene[1] Informatiebeveiliging de nodige aandacht blijven krijgen.

Samenvatting van de departementale rapportages

Door een groot aantal departementen wordt aangegeven dat op het gebied van de informatiebeveiliging prioriteit wordt gegeven aan het continuïteit- en integriteitsvraagstuk dat voortkomt uit het millennium-probleem. De kennis die noodzakelijk is voor de oplossing van dit probleem ligt voor een groot gedeelte bij de functionarissen die zich bezighouden met de informatiebeveiliging binnen het departement. Daardoor kan het lijken dat de aandacht voor informatiebeveiliging te

[1] Voor de bijzondere informatiebeveiliging waar met name de aandacht voor staatsgeheimen en zeer sensitieve informatie centraal staat is een Bijzonder Informatiebeveiligingsberaad (BIB-beraad) in het leven geroepen. In dit BIB-beraad zijn de meest betrokken ministeries vertegenwoordigd.

eenzijdig gericht is. De departementen geven echter aan dat de aandacht voor informatiebeveiliging en het integrale karakter van het VIR blijft bestaan. Dit komt ondermeer tot uiting door de binnen veel departementen opgerichte beveiligingsoverleg-organen in de vorm van stuurgroepen, platforms en taskforces voor informatiebeveiliging.
Alle departementen beschikken nu over een beleidsdocument informatiebeveiliging, dat vastgesteld is door de SG of door de bestuursraad van het betreffende departement. Daarmee wordt invulling gegeven aan het gestelde in artikel 3 van het VIR. Tevens zijn reeds een aantal departementen bezig met het bijstellen van het beleidsdocument naar aanleiding van interne of externe ontwikkelingen.
Ten aanzien van de afhankelijkheids- en kwetsbaarheidsanalyses wordt door een groot aantal departementen aangegeven dat in 1997 en 1998 reeds handmatig analyses zijn uitgevoerd. Daarnaast geven sommige departementen aan dat in 1999 ook nog analyses uitgevoerd worden. De inzet bij veel departementen, die nog niet volledig klaar zijn, is om in het jaar 2000 de eerste ronde van A&K-analyses af te sluiten, waarbij nu gebruik kan worden gemaakt van de beschikbaarheid van het geautomatiseerde instrument ESAKa. Medewerkers worden daartoe opgeleid in het gebruik van ESAKa. Tevens zullen de ervaringen van de diverse trajecten door middel van interdepartementaal overleg voor alle departementen beschikbaar komen, zodat van en met elkaar geleerd kan worden.

Ten aanzien van de beveiligings- en implementatieplannen wordt een breed beeld geschetst. Er zijn departementen die reeds volledig klaar zijn, een aantal departementen heeft voor een groot deel van de organisatie beveiligingsplannen klaar, maar er zijn ook departementen die nog bezig zijn, en een intensivering van de activiteiten voorzien in 1999. Daarnaast is ook door sommige departementen gekozen voor een zogenaamde baseline-benadering (een adequate set van beveiligingsmaatregelen die voor de hele organisatie geldt).

Voor wat betreft het opstellen van calamiteitenplannen wordt slechts af en toe gemeld dat deze calamiteitenplannen aanwezig zijn. Het feit dat calamiteitenplannen het sluitstuk zijn van een goed stelsel van informatiebeveiliging en daardoor op het eind van de rit komen draagt hieraan bij. Dit laat natuurlijk onverlet dat in het kader van het millennium-probleem veel aandacht is en wordt besteed aan de overgangsplannen voor de kritische systemen.

Ten aanzien van de evaluatie van beveiligingsplannen en beleidsdocumenten is eind 1998 door het IB-beraad en door het Interdepartementaal Overlegorgaan Departementale AccountantsDiensten (IODAD) het Raamwerk Kwaliteitstoetsen VIR (RKVIR) vastgesteld. Daarnaast worden in het kader van het RKVIR zogenaamde «Green Papers» opgesteld, die door betrokkenen gebruikt kunnen worden om bepaalde onderdelen van informatiebeveiliging te controleren, c.q. op te zetten.

Conclusie

Al met al kan geconstateerd worden, dat het proces informatiebeveiliging nog steeds kan rekenen op grote ondersteuning vanuit de departementen. Dat het volledig invoeren van het VIR nog steeds niet bij alle departementen heeft plaatsgevonden, hangt samen met de gekozen prioriteit gericht op het hanteerbaar maken en oplossen van het millennium-probleem. Overigens past dit in de door het VIR gehanteerde probleemanalyse; waarbij informatiebeveiliging wordt gezien als een onderdeel van kwaliteitszorg en «het geheel van zaken (betreft) die geregeld dienen te worden om ervoor te zorgen dat een informatiesysteem niet alleen

functioneel in orde is, dat wil zeggen dat de juiste dingen worden gedaan, maar dat deze dingen ook op de juiste wijze worden gedaan».
Kortom, ook in het kader van het oplossen van het millennium-probleem zijn veel activiteiten ontplooid die misschien op korte termijn de volledige invoering van het VIR hebben vertraagd, maar die in de komende periode een belangrijke versnelling van het verbeteren van de informatie-beveiliging kunnen betekenen. Gerealiseerd wordt dat dit voor verschillende departementen een «doorstart» kan inhouden die gemaakt moet worden op een of meerdere deelterreinen van het VIR.

De Minister voor Grote Steden- en Integratiebeleid,
R. H. L. M. van Boxtel