AZ

Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie

maart 2004

Inleiding

1. Het Voorschrift informatiebeveiliging rijksdienst - bijzondere informatie (hierna te noemen: Vir-bi) geeft regels voor de beveiliging van bijzondere informatie bij de rijksdienst. Deze regels strekken er toe het aantal personen dat met bijzondere informatie in aanraking komt zo beperkt mogelijk te houden. Daarnaast is het van belang dat zo spoedig mogelijk actie wordt ondernomen bij kennisname door niet gerechtigden (compromittering).

2. Informatie' wordt in dit voorschrift ruim opgevat: namelijk als kennis die in welke vorm dan ook gecommuniceerd kan worden. Ook 'materiaal' waarin deze kennis is opgeslagen, zoals bijvoorbeeld een document of communicatieapparatuur wordt aangemerkt als informatie.
Bijzondere informatie wordt onderscheiden in staatsgeheimen en in niet-staatsgeheime bijzondere informatie. Er is sprake van een staatsgeheim als het belang van de Staat of zijn bondgenoten in het geding is en indien kennisname door niet gerechtigden kan leiden tot schade aan deze belangen. Er is sprake van niet-staatsgeheime bijzondere informatie indien kennisname door niet gerechtigden kan leiden tot nadeel aan het belang van één of meer ministeries.

3. Het Vir-bi vervangt de uit 1989 daterende Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst, 'de AAR-9'.
De AAR-9 richtte zich met name op de fysieke en organisatorische beveiliging van gerubriceerde niet-elektronische documenten.
In 1995 werd het Besluit voorschrift informatiebeveiliging rijksdienst (Vir) ingevoerd. Dit voorschrift is in beginsel ook van toepassing op de beveiliging van staatsgeheimen. Omdat bij de inwerkingtreding van het Vir het Voorschrift inzake de beveiliging van gerubriceerde gegevens verwerkt en opgeslagen in geautomatiseerde systemen bij de Rijksoverheid van 25 maart 1980 is komen te vervallen, is een leemte ontstaan als het gaat om de eisen die gesteld moeten worden aan de beveiliging van moderne informatie- en communicatievoorzieningen waarop gerubriceerde informatie wordt verwerkt. Enerzijds komt dit omdat de AAR-9 geen voorziening kon bieden voor de risico's die het gebruik van ICT-voorzieningen bij de behandeling van staatsgeheimen met zich meebrengt. Anderzijds biedt het Vir weliswaar een uniforme methodiek om te komen tot beveiligingsmaatregelen, maar laat het de keuze van de uiteindelijk te treffen beveiligingsmaatregelen over aan het lijnmanagement zonder hieraan expliciet eisen te stellen.
Dit laatste is in het geval van staatsgeheimen ongewenst.
Ook is de bevoegdheidsverdeling in de beide voorschriften enigszins verschillend.
Los van deze ontwikkeling werd gaandeweg duidelijk dat het verschil tussen de beveiliging van informatie waarop uitsluitend de regels van het Vir van toepassing zijn en de beveiliging van staatsgeheimen te groot was. Binnen de rijksdienst bleek behoefte te bestaan aan een rijksbrede beveiligingsregeling voor een niveau dat daar tussenin ligt; dit speelt vooral bij informatie die op basis van een departementale regeling wordt gemerkt (bijvoorbeeld 'BZ-vertrouwelijk'). Telkens wanneer dit soort informatie interdepartementaal wordt uitgewisseld blijkt dat de informatiebeveiliging op basis van het Vir onvoldoende garanties biedt, terwijl beveiliging volgens de systematiek van staatsgeheimen als veel te zwaar wordt beschouwd, zoals bijvoorbeeld de verplichte uitvoering van het veiligheidsonderzoek.

4. Bij het opstellen van het Vir-bi zijn de volgende uitgangspunten gehanteerd.
In de eerste plaats is tegemoet gekomen aan de wens van een aantal ministeries om een niveau van beveiliging te creëren voor informatie, die weliswaar geen staatsgeheim is, maar toch meer bescherming behoeft dan informatie waarop het Vir slechts van toepassing is. Toevoeging van dit niveau voorkomt dat er bij interdepartementale uitwisseling van kwetsbare informatie bilaterale afspraken gemaakt moeten worden over het gemeenschappelijk te hanteren beveiligingsniveau. In het verleden werd vaak nagelaten dergelijke afspraken te maken, hetgeen soms ongewenste gevolgen had voor de exclusiviteit van de informatie, dat wil zeggen de mate waarin de toegang is beperkt tot een gedefinieerde groep van gerechtigden. Voor staatsgeheimen en deze overige kwetsbare informatie tezamen wordt de term 'bijzondere informatie' gehanteerd. Door het creëren van dit nieuwe beveiligingsniveau wordt bovendien aangesloten bij de regelgeving van de NAVO, de EU en de meeste West-Europese landen, die een dergelijk beveiligingsniveau kennen. Dit heeft als voordeel dat gerubriceerde informatie die van deze landen of organisaties wordt ontvangen niet onnodig zwaar wordt beveiligd bij gebrek aan een overeenkomstig beveiligingsniveau.
Het tweede uitgangspunt is dat het Vir-bi aansluit op het VIR, dat algemene regels geeft voor de beveiliging van informatie binnen de rijksoverheid. Bijzondere informatie maakt immers deel uit van de totale bij de overheid aanwezige informatie. In verband met de aansluiting bij het VIR wordt in dit voorschrift een met het Vir vergelijkbaar systeem voor de bepaling van risico's en maatregelen (afhankelijkheids- en kwetsbaarheidsanalyse, risicomanagement) opgenomen.
Tevens kent het voorschrift een vergelijkbare regeling van taken en verantwoordelijkheden als het VIR waarbij de verantwoordelijkheid van het lijnmanagement voorop staat.
Een belangrijk gevolg van dit uitgangspunt is dat het nieuwe voorschrift uitsluitend betrekking heeft op de beveiliging van bijzondere infor-

matie en geen regels meer geeft voor de beveiliging van vitale onderdelen bij de rijksdienst zoals in de AAR-9 wél het geval was. Er wordt naar gestreefd binnen afzienbare termijn een regeling in te voeren die niet alleen is gericht op de vitale onderdelen bij de rijksdienst, maar op vitale onderdelen en processen in de samenleving in het algemeen.
In de derde plaats houdt het Vir-bi rekening met de eisen op basis van internationale en nationale wetgeving, zoals de voorschriften van de NAVO en de EU voor de beveiliging van gerubriceerde informatie, de Wet veiligheidsonderzoeken en de Archiefwet. Tenslotte is er, in verband met de steeds voortschrijdende techniek, voor gekozen om in het VIR - BI geen concrete beveiligingsmaatregelen voor te schrijven, maar beveiligingseisen. Maatregelen zijn immers dikwijls techniekafhankelijk en daarmee tijdsgebonden. De eisen zijn op hun beurt weer uitgewerkt in meer concrete beveiligingseisen per deelaspect, die zijn opgenomen in een aparte bijlage (bijlage 3), die bij het Vir-bi hoort. De minister van Binnenlandse Zaken en Koninkrijksrelaties kan, op basis van een daartoe door het Bijzondere Informatie Beveiligingsberaad of zijn rechtsopvolger verstrekt advies, deze bijlage wijzigen. Op deze wijze kan in de toekomst snel worden ingespeeld op nieuwe ontwikkelingen zonder dat het voorschrift zelf behoeft te worden gewijzigd.

5. Het Vir-bi bevat regels, gericht op de bescherming van de exclusiviteit. Het is een aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 1994 (Vir) waarin beveiliging van informatie in het algemeen binnen de rijksdienst is geregeld. Dit betekent dat bij de beveiliging van bijzondere informatie zowel de regels van het Vir als die van het Vir-bi gevolgd moeten worden.
Informatiebeveiliging volgens het Vir richt zich op de bescherming van integriteit, exclusiviteit en beschikbaarheid van de informatie. Het Vir schrijft voor dat door het lijnmanagement op basis van een afhankelijkheids- en kwetsbaarheidsanalyse de betrouwbaarheidseisen en de bijbehorende beveiligingsmaatregelen voor een informatiesysteem worden bepaald.
Bijzondere informatie heeft als kenmerk dat de gevolgen die voor de Staat, zijn bondgenoten of de diverse ministeries uit onbevoegde kennisname kunnen voortvloeien, in ieder geval veel ernstiger zijn dan bij onbevoegde kennisname van overige informatie het geval is. Daarom moet deze bijzondere informatie zwaarder tegen onbevoegde kennisname worden beschermd dan de overige informatie bij de rijksdienst. Het Vir-bi bevat daarom, afhankelijk van de kwetsbaarheid van de informatie, eisen ten aanzien van de exclusiviteit die voor de gehele rijksdienst gelden.
Voorzover dat noodzakelijk is om de exclusiviteit te waarborgen zijn eisen met betrekking tot integriteit meegenomen. Aangezien overigens geen nadere eisen worden gesteld aan de integriteit en beschikbaarheid van bijzondere informatie, kan met de afhankelijkheids- en kwetsbaarheidsanalyse conform het Vir worden volstaan.

6. Beveiligen brengt meestal extra werkzaamheden en daardoor extra kosten met zich mee. Ook kan het leiden tot inbreuk op de persoonlijke levenssfeer omdat een veiligheidsonderzoek verricht moet worden ter beoordeling van de vraag of een persoon in aanmerking kan komen voor de vervulling van een vertrouwensfunctie. Vandaar dat bij het beveiligen altijd twee uitgangspunten moeten worden gehanteerd. In de eerste plaats moet onnodig beveiligen worden vermeden. Dit betekent dat er pas beveiligingsmaatregelen worden getroffen indien er risico's aanwezig zijn die dat rechtvaardigen. In de tweede plaats moet, indien beveiligen noodzakelijk is, het samenhangend pakket van beveiligingsmaatregelen zodanig zijn ingericht dat zo min mogelijk inbreuk hoeft te worden gemaakt op de privacy.

7. Voor wat betreft de financiële gevolgen het navolgende: de voor het vierde beveiligingsniveau (niet-staatsgeheime bijzondere informatie) in de Matrix Exclusiviteitseisen (bijlage 3 van dit voorschrift) vastgelegde eisen zijn voornamelijk organisatorisch van aard ('clean desk' en 'need to know'). Deze maatregelen brengen nauwelijks extra kosten met zich mee. Verder geldt voor deze informatie dat deze in een bergmiddel met deugdelijk hang- en sluitwerk moet worden opgeborgen bij het verlaten van de werkplek; omdat geen extra eisen worden gesteld aan het hang- en sluitwerk zal ook dit vereiste weinig extra kosten met zich meebrengen. Tenslotte geldt als eis dat deze informatie slechts versleuteld over externe netwerken mag worden verzonden. Door het hanteren van een invoeringstermijn van vier jaar (de normale afschrijvingstermijn voor ICT-voorzieningen) wordt voorkomen dat beveiligingsvoorzieningen voortijdig moeten worden vervangen.
Voor het eerste, tweede en derde beveiligingsniveau (de staatsgeheimen) zullen de meerkosten van de gestelde eisen gering zijn, omdat het Vir-bi grotendeels de thans bestaande praktijk met betrekking tot de opslag en verwerking van staatsgeheimen in geautomatiseerde systemen vastlegt.

8. Met het voorschrift wordt ervoor zorggedragen dat informatie met een gelijke rubricering binnen de gehele rijksdienst op een gelijk niveau wordt beveiligd. Vooral bij de uitwisseling van informatie tussen ministeries is dit van groot belang. Het is met name gewenst dat informatie die wordt uitgewisseld bij het ontvangende ministerie op hetzelfde niveau wordt beveiligd als bij het ministerie waarvan de informatie afkomstig is.