Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2006–2007

29 876 Evaluatie AIVD

Nr. 20

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 december 2006

Aanleiding

Ultimo januari 2006 verschenen in De Telegraaf publicaties uit staatsgeheime documenten van een eind jaren negentig afgesloten BVD-onderzoek naar georganiseerde criminaliteit (het zogeheten MIKADO-onderzoek). In de krantenartikelen werd gesteld dat de geheime informatie van de BVD al langere tijd in Amsterdamse criminele kringen zou circuleren. Tevens werd door De Telegraaf gesuggereerd dat de documenten door een ex-medewerker van de BVD aan criminelen zouden zijn doorgespeeld. Er bleek sprake van compromittering van staatsgeheimen, waarover ik u bij brief van 24 januari jl., 29 876 nr. 11, heb geïnformeerd. Tevens informeerde ik diezelfde datum per brief de Commissie voor de inlichtingen- en veiligheidsdiensten (CIVD) van uw Kamer.

De AIVD heeft zowel vanuit art. 6, lid 2 a van de Wet op de inlichtingen- en veiligheidsdiensten (WIV 2002) als vanuit art. 18 van het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (Vir-bi) onderzoek verricht naar de vraag hoe de compromittering van staatsgeheime informatie heeft kunnen plaatsvinden, naar de aard en omvang van de schade en naar de vraag welke maatregelen nodig zijn om de schade te beperken en herhaling te voorkomen. Met deze brief informeer ik u, zoals toegezegd, over de uitkomsten van de onderzoeken.

Het operationele AIVD onderzoek

Zoals bekend gaf ik de AIVD opdracht een eigenstandig en diepgaand onderzoek in te stellen naar de schade voor de nationale veiligheid. Dit betrof een operationeel onderzoek (op basis van art. 6, lid 2 a van de WIV 2002) en richtte zich op de hoeveelheid en aard van de uitgelekte gegevens, op welke wijze deze gegevens bij onbevoegde derden (kunnen) zijn geraakt, en de eventuele gevolgen voor lopende onderzoeken en de veiligheid van personen (bronnen, medewerkers – inclusief medewerkers van

KST104198
0607tkkst29876-20
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2006

buitenlandse collega-diensten – en derden). In het kader van dit onderzoek werden ook bijzondere bevoegdheden aangewend. Ik heb hierover de CIVD geïnformeerd bij brief van 22 mei jl.

De Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft op mijn verzoek, naar aanleiding van het door De Telegraaf aangespannen kort geding, de rechtmatigheid van het operationele onderzoek onderzocht. Het rapport van de CTIVD met mijn reactie daarop heb ik u en de voorzitter van de Eerste Kamer op 6 december jl. toegestuurd (2006–2007, 29 876, nr. 19). en eveneens, met nadere vertrouwelijke informatie, aan de CIVD. De belangrijkste conclusie van de CTIVD is dat het operationele AIVD-onderzoek en de inzet van bijzondere bevoegdheden in dat kader rechtmatig is geweest. Wel is door de CTIVD een aantal onvolkomenheden gesignaleerd, die evenwel geen invloed hebben gehad op de rechtmatigheid van de ambtsberichten die op basis van het AIVD-onderzoek zijn uitgebracht.

Tevens heeft de CTIVD, conform artikel 83, derde lid van de WIV 2002, mij geadviseerd inzake de klacht die De Telegraaf bij mij had ingediend over de handelwijze van de AIVD jegens de twee Telegraaf-journalisten. Dit advies overnemend heb ik klagers inmiddels laten weten de klacht op de drie hoofdpunten ongegrond te verklaren en op een afgeleid onderdeel van de klacht ten dele gegrond (de wijze van toepassing van de bijzondere bevoegdheden). Of klagers hiermee genoegen nemen of zich tot de Nationale ombudsman zullen richten met hun klacht, is mij tot op heden niet bekend.

Het gerechtshof in Den Haag heeft op 31 augustus jl. arrest gewezen in de kort-gedingprocedure, die door De Telegraaf c.s. was aangespannen tegen de Staat. Naar aanleiding van deze uitspraak heeft De Telegraaf c.s. inmiddels cassatie ingesteld.

Het Vir-bi onderzoek

Gelet op het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (Vir-bi) heeft het hoofd van de AIVD, in opdracht van de secretaris-generaal van mijn ministerie, tegelijkertijd een onderzoek laten uitvoeren conform art. 18 van het Vir-bi. Dit bedrijfsmatige onderzoek kende een brede opzet en was met name gericht op de te nemen organisatorische en beveiligingsmaatregelen om de schade te beperken en herhaling te voorkomen, ofwel het trekken van lessen uit dit incident voor de interne beveiliging.

De opzet en inrichting van dit laatste onderzoek is vooraf besproken met de CTIVD. Over de wijze waarop de adviezen van de CTIVD ten aanzien van het onderzoek zijn verwerkt, heb ik de CIVD per brief van 11 mei jl. ingelicht. Het Vir-bi onderzoek heeft waar nodig gebruik gemaakt van de informatie afkomstig uit het operationele onderzoek, met name daar waar het vragen betrof naar de wijze waarop de compromittering heeft plaatsgevonden en de aard en omvang van de operationele schade.

Het strafrechtelijk onderzoek tegen een verdachte ex-medewerker van de BVD

In het kader van het strafrechtelijk onderzoek dat het Openbaar Ministerie is opgestart naar aanleiding van de aangifte van de AIVD, heeft de Rijksrecherche op 4 mei jl. onder meer een ex-medewerker van de BVD aangehouden op verdenking van het schenden van staatsgeheimen. Verwacht wordt dat de strafzaak tegen deze verdachte ex-medewerker eind januari

2007 ter zitting zal komen voor inhoudelijke behandeling. Thans worden in deze zaak nog enkele getuigen bij de rechter-commissaris gehoord.

Genoemde persoon werd per 1 augustus 2001 ontslag verleend met een eenmalige uitkering ter afkoop van het wachtgeld. Dit ontslag vloeide voort uit een vertrouwensbreuk tussen betrokkene en de BVD ten gevolge van een incident, waarover de CIVD in detail is geïnformeerd.

Hoe heeft de compromittering van staatsgeheimen plaatsgevonden?

Zoals hiervoor aangegeven beschikte De Telegraaf over een aanzienlijke verzameling gekopieerde bladzijden uit een afgesloten, operationeel, grotendeels gerubriceerd dossier van de BVD. Het oudste gecompromitteerde document uit de Telegraaf-verzameling dateert van 1996, het meest recente document dateert van februari 2000. Het dossier had betrekking op het MIKADO-onderzoek, dat eind jaren negentig door de BVD werd uitgevoerd en dat zich onder meer richtte op vermeende integriteitsaantastingen van het openbaar bestuur vanuit de criminele organisatie van Robert Mink K.

Het onderzoek heeft niet met zekerheid kunnen vaststellen hoeveel documenten in die periode gecompromitteerd zijn en hoeveel daarvan uiteindelijk bij De Telegraaf zijn beland, c.q. bij andere daartoe niet-gerechtigden. Mogelijk geeft het strafrechtelijk onderzoek hier nog meer opheldering over.
Uit de uiterlijke kenmerken van de documenten valt af te leiden dat de documenten waarschijnlijk in papieren vorm buiten het BVD-gebouw zijn gebracht. Niet met zekerheid is vast te stellen of die kopieën die in omloop zijn geraakt, binnen of buiten de BVD vervaardigd zijn. Het merendeel van de bij De Telegraaf belande documenten bestaat uit kopieën van het werkdossier van toenmalig team Mikado.

Het door de rijksrecherche ingestelde onderzoek leverde voldoende feiten en omstandigheden op om een ex-medewerker van de BVD aan te houden op verdenking van schending van staatsgeheimen. Zoals hierboven aangegeven worden thans in deze zaak nog enkele getuigen bij de rechter-commissaris gehoord.

Aard en omvang van de schade en getroffen operationele maatregelen

In mijn brief van 24 januari heb ik u een globale inventarisatie gegeven van de inhoud van de gecompromitteerde documenten en een eerste inschatting van de schade. De gecompromitteerde documenten geven inzicht in het toenmalige operationele kennisniveau van de BVD op het taakveld integriteit van de openbare sector en in de werkwijze van de BVD op dat taakveld. Uit de verzameling documenten valt een beeld te destilleren dat zou kunnen worden vertaald naar het huidige kennisniveau en de huidige werkwijze van de AIVD. Door het uitlekken van deze informatie zijn staatsgeheimen geschonden.

Schade voor lopende onderzoeken en modus operandi
Het onderzoek wijst uit dat de schade aan lopende onderzoeken en de gevolgen van het bekend raken van de toen gehanteerde werkwijzen (modus operandi) gering zijn.

Blijkens de ervaringen direct na de geconstateerde compromittering, is tijdelijk schade toegebracht aan de bereidheid tot medewerking van bestaande en potentiële menselijke bronnen. De garantie van bron-

bescherming is één van de meest essentiële voorwaarden voor die bereidheid, die onontbeerlijk is voor het inlichtingenproces.

Schade aan de veiligheid van personen
De veiligheidsrisico's als gevolg van de schending van staatsgeheimen voor AIVD-medewerkers en medewerkers van andere diensten en overheidsorganisaties genoemd in de documenten of betrokken bij het toenmalige BVD-onderzoek, zijn direct onderzocht. Daaruit is gebleken dat de risico's voor hen niet groot worden ingeschat. Risico's voor agenten en/of informanten kunnen echter niet worden uitgesloten. Waar nodig zijn operationele maatregelen getroffen om deze risico's te reduceren.

Schade aan belangen van bondgenoten
De schade voor buitenlandse collega-diensten is niet goed in te schatten, maar lijkt beperkt. Tot dusverre zijn geen nadelige gevolgen gebleken voor de samenwerking.

Imagoschade
Het spreekt voor zich dat de compromittering van staatsgeheimen en inbreuken op de eigen beveiliging een negatieve invloed heeft op het imago van de AIVD.

Interne beveiliging van de AIVD: toetsing van beleid en uitvoering

Het onderzoek heeft vastgesteld dat de wet- en regelgeving ten tijde van de compromittering voldoende voorschreef om de kans op het ongeautoriseerd en ongemerkt naar buiten brengen van grote hoeveelheden documenten te minimaliseren. Ook de huidige wetgeving voldoet volgens het onderzoek en hoeft niet aangescherpt te worden als gevolg van de compromittering. Het interne beleidskader schreef eveneens voldoende maatregelen voor om de mogelijkheden te minimaliseren om grote hoeveelheden documenten ongeautoriseerd en ongemerkt buiten de werkomgeving te brengen. Het onderzoek concludeert dat noch de wettelijke kaders, noch het interne beleidskader van de AIVD behoeft te worden aangescherpt als gevolg van de compromittering.

Wel heeft het onderzoek vastgesteld dat de uitvoeringsrichtlijnen en de naleving van die richtlijnen in de praktijk (controle, handhaving) verbeterd moeten worden. Het onderzoek oordeelt dat het risico op een compromittering in de geconstateerde omvang gereduceerd had kunnen worden als er meer ondersteunende faciliteiten voorhanden waren geweest, bijvoorbeeld op het gebied van personeelsbegeleiding bij dreigende probleemsituaties. Ook een betere bekendstelling van de vastgestelde beveiligingsregels in combinatie met een zichtbaarder sanctionering, een betere registratie van beveiligingsrelevante activiteiten en een beter geborgd toezicht en onafhankelijke toetsing op de implementatie hadden het risico kunnen verminderen.

Optimale versus maximale beveiliging: een permanente afweging

De AIVD is een organisatie waar vanuit vijf wettelijke taken staatsgeheime informatie snel, doeltreffend en sluitend onderling gecommuniceerd moeten worden om die taken effectief te kunnen uitvoeren. De grondslag voor een optimale beveiliging wordt gevormd door een afwegingsproces waarbij alle belangen met betrekking tot de bedrijfsvoering rondom het inlichtingenproces (inclusief de belangen voor geheimhouding van vertrouwelijke informatie) worden betrokken. Er dient een balans gevonden te worden waarbij zowel belangen van het operationele inlichtingenproces als de veiligheidsbelangen voortdurend tegen elkaar worden afgewogen (immers, bij een in theorie realiseerbare, maximale

beveiliging komen de effectiviteit en de efficiency van de AIVD als organisatie in het gedrang). Het onderzoek heeft vastgesteld dat de wet- en regelgeving een dergelijk afwegingsproces niet in de weg staat.

In het onderzoek wordt geconcludeerd dat ook met een optimale beveiliging het voorkomen van opzettelijke compromittering een illusie is. Immers, nooit zal onder werkbare omstandigheden kunnen worden voorkomen dat medewerkers die geautoriseerd kunnen kennis nemen van staatsgeheimen en die kwaad willen, in staat zijn om staatsgeheimen langs enige weg opzettelijk ongeautoriseerd buiten de gebouwen van de AIVD te brengen. Het screenen van (nieuwe) medewerkers door middel van veiligheidsonderzoeken en herhaalonderzoeken kan de risico's op opzettelijke compromittering beperken, maar niet uitsluiten.

De consequentie hiervan is dat er, onafhankelijk van de wijze waarop beveiliging is ingericht, altijd vertrouwen in medewerkers zal moeten worden gesteld. Naast het onderlinge vertrouwen dat noodzakelijk is voor praktische samenwerking, zijn anderzijds sociale controle, alertheid op signalen die zouden kunnen wijzen op veiligheidsrisico's en het elkaar aanspreken op niet-veiligheidsbewust gedrag dan ook noodzakelijke onderdelen in de beveiliging.

Maatregelen om beveiliging verder te verbeteren en de kans op herhaling te reduceren

Intern beleid
Mede teneinde voldoende aansluiting te kunnen verzekeren met recente wet- en regelgeving is al geruime tijd geleden binnen de AIVD een modernisering van het beveiligingsplan en de uitvoeringsrichtlijnen in gang gezet. Deze modernisering van het interne beleid was niet alleen noodzakelijk om aan te sluiten bij het nieuwe Beveiligingsvoorschrift Rijksdienst 2005, maar ook om aan te sluiten bij actuele ontwikkelingen (nieuwe dreigingscenario's, voortschrijden van de informatietechnologie, etc.).

Het nieuwe beveiligingsplan is in september 2006 vastgesteld. Daarin zijn op basis van dreigingscenario's allereerst de dreigingen richting de AIVD betrekking hebbend op (on)bewust menselijk handelen in kaart gebracht, geordend op waarschijnlijkheid. Vervolgens worden de beveiligingsmaatregelen beschreven welke de AIVD moet nemen om het ongestoord en vertrouwelijk functioneren van de dienst optimaal te waarborgen. De beveiligingsmaatregelen hebben betrekking op de fysieke, personele, organisatorische en ICT-beveiliging. In het derde deel van dit beveiligingsplan worden de dreigingen afgezet tegen de beveiligingsmaatregelen (risicoanalyse). Dit geeft een beeld van de restrisico's.

Een aantal van de beschreven beveiligingsmaatregelen wordt nader beschreven en uitgewerkt in procedures en uitvoeringsrichtlijnen. Het totaal vormt dan een vernieuwd Handboek beveiliging AIVD. Om de werking van dit geactualiseerde beveiligingsregime in de praktijd te effectueren wordt een intensieve communicatiecampagne onder het AIVD-personeel gevoerd, zodat de geactualiseerde richtlijnen bekendgesteld en nageleefd kunnen worden.

Personele aspecten van beveiligingsbeleid

De personele aspecten van beveiliging (beveiligbewustzijn, persoonlijke integriteit, (sociale) controle) vormen een belangrijke pijler van de beveiliging. Sinds de personele groei van de AIVD, ingezet na de aanslagen van 11 september 2001, is hier zowel beleidsmatig als praktisch al veel in gang gezet.

Het reeds lopende project «Intelligent en veilig groeien», voortvloeiend uit het rapport van de Commissie Havermans, is overkoepelend voor de diverse initiatieven binnen de AIVD gericht op het handhaven van een veiligheidsbewuste organisatiecultuur in een periode van ongekende groei. Bij de werving van nieuwe medewerkers is het bevorderen van het veiligheidsbewustzijn een prioriteit. In het introductieprogramma worden de nieuwe medewerkers intens doordrongen van de wettelijke, technische en personele aspecten van beveiliging.

Sturing op het handhaven van een constant hoog niveau van beveiligingsbewustzijn op de werkvloer door het lijnmanagement dient een permanent punt van aandacht te zijn. Daarbij dienen signalen met betrekking tot de motivatie en persoonlijke omstandigheden (risicogedrag) van personeelsleden met extra zorg en aandacht behandeld te worden. Het onderzoek beveelt aan verdergaand beleid te ontwikkelen voor de begeleiding van medewerkers die voortijdig en/of onder ongebruikelijke omstandigheden de dienst verlaten (nazorg) of dreigen te verlaten, en de personele aspecten van de interne beveiliging gestructureerd onderdeel te laten uitmaken van de bedrijfsprocessen, zodat signalen omtrent risicogedrag van (voormalige) personeelsleden tijdig herkend worden en opvolging krijgen. Maatregelen op dit punt zullen versneld worden uitgevoerd (zoals scherpere werkafspraken over begeleiding van nieuwe medewerkers op de werkvloer).

Maatregelen op het gebied van fysieke en ICT-beveiliging

Mede in het kader van de nieuwe huisvesting van de AIVD in 2007 wordt een aantal fysieke en technische maatregelen getroffen om de informatiebeveiliging te verbeteren.

Tot slot

Er is sprake van een ernstig incident geweest: een aanzienlijke verzameling gekopieerde documenten uit een afgesloten werkdossier van de BVD is, in strijd met de regels, buiten het gebouw gebracht. Operationeel onderzoek van de AIVD en onderzoek van de rijksrecherche wijst erop dat dit waarschijnlijk is gebeurd door een ex-medewerker van de BVD, die hiertoe tot augustus 2000 in de gelegenheid is geweest. Vervolgens zijn de documenten, mogelijk via derden, uiteindelijk in het bezit van de Telegraaf gekomen, die hierover in januari van dit jaar publiceerde. Ik wijs erop dat definitieve conclusies over de wijze waarop de compromittering heeft plaatsgevonden formeel pas getrokken kunnen worden als de rechtsgang tegen de verdachte ex-medewerker is afgerond.
De gecompromitteerde documenten geven inzicht in het toenmalige operationele kennisniveau van de BVD op het taakveld integriteit van de openbare sector in en in de werkwijze van de BVD op dat taakveld. De schade aan lopende onderzoeken en de gevolgen van het bekend raken van de toen gehanteerde werkwijzen (modus operandi) zijn betrekkelijk gering. Risico's voor agenten en/of informanten kunnen echter niet worden uitgesloten. Waar nodig zijn operationele maatregelen getroffen om deze risico's te reduceren.

Toetsing aan de toen en thans geldende beveiligingsvoorschriften levert het inzicht op dat meer regelgeving niet of nauwelijks winst oplevert. De naleving van en toezicht op regels en voorschriften dient wel te worden versterkt. Het vernieuwde beveiligingsplan en de interne communicatie daarover zullen daarin voorzien. Het treffen van technische maatregelen, zoals de invoering van nieuwe beveiligingstechnologie bij geautoriseerde systemen, en maatregelen op het gebied van personeelsbeleid, zoals voortzetting van gedegen veiligheids- en herhaalonderzoeken van nieuw

en zittend personeel, zullen eveneens bijdragen aan het verder reduceren van veiligheidsrisico's. Uiterste alertheid op signalen die zouden kunnen wijzen op veiligheidsrisico's en betere (sociale) controle op niet-veiligheidsbewust gedrag zijn daarbij noodzakelijk.

Ik concludeer uit de onderzoeken ook dat een beveiliging die opzettelijk compromitteren volledig voorkomt niet haalbaar is. Nooit zal kunnen worden uitgesloten dat medewerkers die geautoriseerd kennis kunnen nemen van staatsgeheimen en die bewust kwaad willen, in staat zijn om staatsgeheimen langs enige weg, opzettelijk en ongeautoriseerd, buiten de gebouwen van de AIVD te brengen.

Er dient sprake te zijn van een balans tussen een maximale beveiliging en een effectief werkproces. Mede op basis van de regelgeving en door toezicht en sturing op de naleving van de regelgeving kunnen risico's voor het compromitteren van vertrouwelijke informatie worden geminimaliseerd. Dit heeft de volle aandacht van de AIVD. Een restrisico met betrekking tot de menselijke factor zal echter altijd blijven bestaan.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. W. Remkes