36600 VI Vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2025

Nr. 123 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 december 2024

Op 1 november 2023 heeft mijn voorganger uw Kamer geïnformeerd over de verontrustende berichtgeving dat op donderdag 26 oktober 2023 twee personen zijn aangehouden op verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie (Kamerstuk 36410-VI, nr. 10). Dit is aanleiding geweest voor het instellen van verschillende onderzoeken, waaronder een onafhankelijk onderzoek naar de omgang met bijzondere informatie[1] bij de NCTV en de politie door de Auditdienst Rijk (ADR). Het rapport dat door de ADR is opgesteld als resultaat van dit onderzoek is op 29 november jl. aangeboden aan mijn ministerie en stuur ik uw Kamer als bijlage[2] bij deze kabinetsreactie toe. Peildatum van het onderzoek van de ADR is 1 oktober 2023. De situatie na 1 oktober 2023 en de sindsdien genomen maatregelen maken daarom in beginsel geen onderdeel uit van het rapport en de bevindingen van de ADR. Dat betekent dat de ADR in beginsel heeft gekeken naar de situatie zoals die was direct voor de aanhoudingen.

Ik acht het van belang uw Kamer zo volledig en transparant mogelijk te informeren. Dat neemt niet weg dat, zoals ook gemeld in de Kamerbrief van 8 december 2023[3], juist over deze aangelegenheid goed moet worden bezien welke informatie - met het oog op de zorgvuldigheid en de veiligheid die moet worden

---

[1] Met bijzondere informatie wordt in deze brief gedoeld op gerubriceerde informatie, waaronder staatsgeheime informatie, en vertrouwelijke politie-informatie. Staatsgeheime informatie is anders van aard dan vertrouwelijke politie-informatie; bij staatsgeheime informatie is er altijd sprake van een belang voor de nationale veiligheid. Gerubriceerde politie-informatie kent een spectrum aan rubriceringen met uiteenlopende belangen.

[2] Op en in het rapport staat nog de rubricering departementaal-vertrouwelijk. Deze rubricering is er formeel afgehaald voor verzending aan uw Kamer maar blijft erop staan vanwege het format van het rapport.

[3] Kamerstukken 2023-24, 36 410-V, nr. 16

betracht - niet openbaar gemaakt kan worden. Dat heeft ertoe geleid te besluiten om enkele passages uit het rapport niet openbaar te maken, omdat deze ofwel 1) de belangen van de Staat kunnen schaden dan wel 2) veiligheidsrisico's opleveren omdat concreet inzicht wordt gegeven in de operationele werkwijze van de politie.

Ik ben de ADR erkentelijk voor het verrichte onderzoek en het rapport. De ADR concludeert dat de informatiebeveiliging, op peildatum 1 oktober 2023, onvoldoende was. Procedures en maatregelen werden onvoldoende nageleefd, er was onvoldoende alertheid op mogelijk misbruik en de samenwerking tussen verantwoordelijke onderdelen was onvoldoende. De ADR concludeert dat de NCTV en de politie daarmee hun eigen kwetsbaarheden hebben gecreëerd.

Uit het rapport spreekt een heldere boodschap: de informatiebeveiliging ten aanzien van bijzondere informatie kan en moet beter en moet beter voorbereid worden op misbruik van gerechtvaardigde toegang tot bijzondere informatie. Ik onderschrijf die boodschap volledig. Het is niet goed dat destijds niet is voldaan aan de geldende procedures en voorschriften voor informatiebeveiliging. Het is van groot belang dat deze worden nageleefd. Daar zet ik vol op in.

De geldende voorschriften moeten altijd omgezet worden in concrete maatregelen in de praktijk. Die concrete maatregelen moeten vervolgens constant getoetst en aangescherpt worden. Dat is nooit af. Het ADR rapport doet ten aanzien van die concrete maatregelen waardevolle aanbevelingen die ik omarm. Zoals ook uit de bijlage zal blijken, is een deel van de aanbevelingen reeds opgevolgd door de al sinds de aanhoudingen van de verdachten getroffen maatregelen.

De opvolging van de aanbevelingen van de ADR is niet met een enkele toegespitste maatregel te bereiken. Een andere aanpak en bewustzijn over de hele breedte van de omgang met bijzondere informatie bij de NCTV en de politie is nodig. De omvangrijke stappen die reeds sinds de aanhoudingen en naar aanleiding van het ADR rapport zijn gezet illustreren dat de aanbevelingen met de nodige urgentie en zorgvuldigheid zijn opgepakt en zullen blijven worden opgepakt. Er zal in het verdere proces continu getoetst worden waar nog verdere verbeteringen doorgevoerd kunnen worden. Ik heb daarbij ervaren dat de onderzochte organisaties de urgentie voelen en de aanbevelingen van de ADR adequaat hebben

opgepakt. Hieronder zal ik in algemene zin ingaan op de hoofdpunten waarop die aanpak gericht is en tot welke maatregelen dat leidt en geleid heeft. Een gedetailleerde reactie op de aanbevelingen en de uitwerking daarvan is in de bijlage weergegeven.

Kabinetsreactie

De NCTV en de politie spelen een belangrijke rol bij het veilig houden van ons land en beschikken daartoe over een specifieke informatiepositie. De NCTV, als onderdeel van het ministerie van Justitie en Veiligheid, doet dat vanuit een coördinerende rol. De politie, een *sui generis* organisatie, doet dat vanuit een operationele rol. De organisaties vervullen hun rollen onder bijzondere omstandigheden waarbij alertheid en veiligheidsbewustzijn hoog in het vaandel staan. Vanwege de verschillende positionering van de NCTV en de politie is er sprake van verschillende wettelijke verankerde regimes voor informatiebeveiliging.

Voor het vervullen van de rol in de bescherming van onze (nationale) veiligheid verwerken verschillende partijen binnen de overheid, waaronder de NCTV en de politie, bijzondere informatie. Dit maakt deze organisaties een interessant doelwit voor statelijke en niet-statelijke actoren. Het is bekend dat Nederland doelwit is van inlichtingenactiviteiten van landen met een offensief inlichtingenprogramma die daarmee de nationale veiligheid van Nederland bedreigen.[4] Digitale en fysieke spionage vormen een specifiek probleem waar het kabinet en de samenleving alert op moeten blijven.[5] Het is daarom van groot belang dat veiligheidsorganisaties, en daarmee onze samenleving, daartegen zo weerbaar mogelijk zijn en blijven. Tegelijkertijd zullen kwaadwillende actoren altijd op zoek blijven naar gevoelige informatie en daar met offensieve inlichtingencampagnes maximaal op inzetten.

1. Maatregelen naar aanleiding van de aanhouding

Zodra bekend werd dat er sprake was van een mogelijk lek van bijzondere informatie door een medewerker van de NCTV, zijn er binnen de NCTV noodmaatregelen getroffen. Het gaat dan om zowel noodmaatregelen als gelijktijdig ingezette maatregelen gericht op de lange(re) termijn. De noodmaatregelen beoogden een direct effect, waarbij de maatregelen gericht op de lange(re) termijn onderdeel uitmaken van een continu proces van verbetering. De aanbevelingen die de ADR in haar rapport heeft gedaan zijn, voor zover dat nog niet het geval was, weer integraal

[4] Dreigingsbeeld Statelijke Actoren, November 2022, p. 17
[5] Dreigingsbeeld Statelijke Actoren, November 2022, p. 4, 13-14, 17

meegenomen. Dit proces kent ook geen einde, nu informatiebeveiliging een constante cyclus van verbetering kent.

Doel van de (nood)maatregelen was zekerstellen dat alleen die mensen kennis kunnen nemen van informatie waarvoor dat voor de uitoefening van hun taak noodzakelijk is. Verschillende werkprocessen, waaronder informatiedeling, zijn daartoe onmiddellijk gestopt en de toegang tot bijzondere informatie is zeer sterk ingeperkt. Vervolgens is de toegang tot bijzondere informatie via het digitale systeem stap voor stap weer opgestart, waar nodig met aanvullende waarborgen en tussenstappen en met een sterk ingeperkt toegangsregime. De geldende wet- en regelgeving, waaronder het Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI) is daarbij de basis. Er is en wordt strikter gekeken naar wie welke informatie echt nodig heeft om zijn of haar werk te kunnen doen.

Daarnaast is de NCTV direct gestart met het nemen van maatregelen gericht op de lange(re) termijn. Er zijn zowel ten aanzien van de digitale als fysieke verwerking van bijzondere informatie belangrijke stappen gezet. Dit heeft er onder meer toe geleid dat de NCTV sinds 8 april jl. een accreditatie heeft ontvangen voor de duur van 1 jaar die ziet op het digitale systeem waarmee bijzondere informatie wordt verwerkt. Daarnaast zijn maatregelen getroffen ten aanzien van de fysieke context waarin bijzondere informatie wordt verwerkt. De uitkomsten van de eerste schouw op deze maatregelen is dat de NCTV momenteel voldoet aan de vereisten voor het verwerken van staatsgeheime informatie. Ook zijn de personele beveiligingsmaatregelen verder aangescherpt, om het risico op *insider threat* zo klein mogelijk te maken. Over de volle breedte zijn verdere verbetermaatregelen geïdentificeerd, die ook deels hun weerslag vinden in het ADR rapport. Deze elementen zullen ook nader aan bod komen in deze brief en de bijlage bij deze brief.

Na de aanhouding van de verdachten heeft ook de politie direct maatregelen getroffen. De gevolgen van de aanhouding van de verdachte die ingehuurd werd door de politie zijn in kaart gebracht, waaronder veiligheidsrisico’s voor individuele medewerkers en lopende onderzoeken. Waar nodig zijn maatregelen in de operatie getroffen om mogelijke schadelijke gevolgen te beheersen. De politie heeft in de periode na de aanhouding van de verdachten ook maatregelen getroffen bij het cluster Contraterrorisme, Extremisme en Radicalisering (CTER), onder meer naar aanleiding van eigen onderzoek. De politie heeft in de periode na de aanhoudingen ook structurele maatregelen getroffen. De voorlichting over het

geldende beleid is verbeterd en het eerstelijns toezicht hierop is verscherpt. Het gaat hierbij om het naleven van het beleid voor veilige communicatie en voor het veilig werken met tolken. Verder is de politie naar aanleiding van de aanhouding gestart met het treffen van lange(re) termijn maatregelen, zoals het (verder treffen van voorbereidingen voor) de invoering van *protective monitoring* voor de gehele politieorganisatie en het in gang zetten van een proces om tolken op een hoger niveau dan voorheen te screenen. Deze elementen zullen ook nader aan bod komen in deze brief en de bijlage bij deze brief.

2. Hoofdpunten ADR Rapport

De belangrijkste punten uit het ADR rapport zijn dat op de peildatum van 1 oktober 2023:

a) procedures en regels ingericht ten aanzien van informatiebeveiliging in de praktijk onvoldoende werden nageleefd;
b) er onvoldoende alertheid was ten aanzien van mogelijk misbruik van toegang tot informatie; en
c) de samenwerking tussen de verschillende onderdelen die een rol hebben in informatiebeveiliging onvoldoende was.

De NCTV en de politie hebben maatregelen getroffen om deze aandachtspunten structureel op orde te brengen. Deze komen hieronder één voor één aan bod, eerst algemeen en daarna per organisatie. Ik merk daarbij op dat de ADR ten aanzien van de NCTV en politie verschillende aanbevelingen heeft gedaan die zien op verschillende onderdelen van het proces van informatiebeveiliging.

a) <u>Het naleven van de procedures en voorschriften</u>

Het eerste aspect ziet op het voldoen aan de geldende procedures en voorschriften langs de lijnen van het veelgebruikte Plan-Do-Check-Act (PDCA) cyclus zoals ook gehanteerd door de ADR. Enerzijds omdat anders risico’s kunnen ontstaan in de beveiliging. Anderzijds omdat de (informatie)beveiliging anders niet toetsbaar is en kwetsbaarheden onvoldoende naar boven komen. Er was bij de NCTV en politie geen volledig cyclisch proces van informatiebeveiliging ingeregeld. Terwijl het juist nodig is voor goede informatiebeveiliging om deze stappen continu te doorlopen. Het ADR rapport laat zien dat de NCTV en politie op dit punt (verschillende) verbeteringen moeten doorvoeren. Zo heeft de ADR ten aanzien van de politie geconstateerd dat er al veel bruikbaars

op papier staat en beveelt aan om aanvullende aandacht te besteden aan de Do-Check-Act onderdelen van de cyclus. Bij de NCTV zal met een sluitende PDCA-cyclus worden voldaan aan het normenkader voor informatiebeveiliging, zoals die wordt vereist op basis van de Baseline Informatiebeveiliging Overheid (BIO) en het VIR-BI. Zowel de korpschef als de NCTV hebben reeds maatregelen getroffen die ertoe moeten leiden dat deze cyclus sluitend wordt gemaakt. Als onderdeel daarvan worden de verantwoordelijkheden voor informatiebeveiliging op alle niveaus versterkt.

NCTV

Hoewel de PDCA-cyclus nog niet sluitend is – waarbij ook de ADR constateert dat doorgaans een jaar nodig is om een volledige PCDA-cyclus te doorlopen -, heeft de NCTV inmiddels een proces uitgewerkt waarbij risico's in het kader van de bescherming van bijzondere informatie en de toegang daartoe in beeld worden gebracht en mitigerende maatregelen zijn en worden ontwikkeld en ingezet. Het Voorschrift Informatiebeveiliging Rijksdienst (VIR), uitgewerkt in het BIO, en het VIR-BI gelden daarbij als uitgangspunt. Hierbij was tevens 'need to know' altijd het uitgangspunt. Voorbeelden van verbeteringen die reeds zijn getroffen, zijn bijvoorbeeld het beperken van toegang tot systemen en informatie die alleen noodzakelijk is voor de goede uitoefening van een taak (een steviger inrichting van het '*need to know*'-principe), het aanscherpen van toezicht op en controleren van rechten en het vereisen van toezicht op atypische gedragingen, zoals bijvoorbeeld het vereisen van toestemming van een leidinggevende om voor een ander te printen.

Daarnaast acht ik het van belang om stil te staan bij het beleid ten aanzien van de veiligheidsonderzoeken en vertrouwensfuncties binnen de NCTV. Bevindingen uit het ADR onderzoek hebben aanleiding gegeven om ten aanzien van een beperkt aantal medewerkers nader te bezien in hoeverre de 'verklaringen van geen bezwaar toereikend waren voor de functie. Ten aanzien van een aantal medewerkers zijn vervolgens mitigerende maatregelen getroffen in afwachting van een hernieuwd veiligheidsonderzoek van de AIVD. Ook is de NCTV, met advies van de Beveiligingsautoriteit van het ministerie van Justitie en Veiligheid (hierna: BVA), gestart met de 5-jaarlijkse actualisatie van de lijst vertrouwensfuncties, zodat deze aansluit bij de laatste inzichten. Tot slot heeft de NCTV maatregelen genomen om het beleid t.a.v. het tijdig aanvragen van herhaalonderzoeken en het melden van gewijzigde omstandigheden bij vertrouwensfunctionarissen aan de BVA aangescherpt na te leven.

Politie
De ADR geeft aan dat er bij de politie veel bruikbaars op papier staat maar onvoldoende in de praktijk wordt nageleefd. Er worden verschillende stappen gezet om de implementatie daarvan in de praktijk te verbeteren. Er wordt bijvoorbeeld reeds een pilot gedraaid met *protective monitoring* waarmee gebruikershandelingen proactief en geautomatiseerd worden geanalyseerd op atypische signalen om onrechtmatig gebruik van systemen te detecteren. Per 1 januari 2025 wordt *protective monitoring* ingevoerd in de gehele politieorganisatie. Ook is het beleid ten aanzien van de screening voor tolken binnen de politie aangescherpt.

Het ADR rapport toont aan dat bij de leidinggevenden van het CTER-cluster het eerstelijns toezicht niet op orde was. Dit sluit aan bij het beeld uit eerdere rapporten[6] dat leidinggevenden te veel gericht waren op het bereiken van operationele resultaten wat ten koste gaat van het concretiseren en naleven van voorschriften en procedures rondom informatiebeveiliging. Daarom wordt als deel van de transitie van de landelijke eenheden binnen het CTER-cluster reeds ingezet op het versterken van het leiderschap en de verkleining van de *span of control* van leidinggevenden (het aantal medewerkers per leidinggevenden). Ook het wijzigen van de inrichting van het CTER-cluster wordt meegenomen in deze transitie. Als onderdeel hiervan zal het toezicht op informatiebeveiliging in de werkpraktijk ingeregeld worden, bijvoorbeeld ten aanzien van toegangsrechten.

b) Blijvende alertheid op mogelijk misbruik

Het tweede aspect ziet erop dat meer rekening moet worden gehouden met mogelijk misbruik door individuen die geautoriseerd toegang hebben tot bijzondere informatie. De ADR concludeert dat er te weinig alertheid was ten aanzien van mogelijke inbreuken op beveiliging. Op de situatie dat er misbruik kan worden gemaakt van gerechtvaardigde toegang, ook binnen de eigen organisatie, moet (beter) worden geanticipeerd. Dit omvat verschillende elementen, die deels overlappen met de maatregelen die hierboven zijn genoemd. Een onderdeel ziet bijvoorbeeld op het registeren en analyseren van gebeurtenissen die van invloed kunnen zijn op de betrouwbaarheid van informatie. Dit begint bij het vastleggen en analyseren van handelingen van de medewerkers die met bijzondere informatie werken.

[6] Kamerstukken II 2021-22, 29 628 nr. 1053 en 1101

Bij zowel de NCTV als de politie worden procedures, toegespitst op de eigenheid van de organisaties, ingericht die uitgaan van succesvolle pogingen tot ongeautoriseerde toegang of het misbruik maken van geautoriseerde toegang. Onderdeel daarvan is beleid over wélke handelingen vervolgens als atypisch gelden, waarbij rekening wordt gehouden met mogelijk misbruik of een *insider threat*. Dan wordt het gedrag toetsbaar. Bovendien gaat daar een bewustzijn verhogend effect van uit. Ook blijkt uit het ADR rapport dat incidenten of activiteiten niet altijd als signaal van mogelijk misbruik werden opgevat. Het is van belang dat afwijkingen van procedures of opvallende gedragingen altijd vanuit verschillende perspectieven worden bekeken. Verhoogd bewustzijn over mogelijk misbruik draagt ook daar aan bij.

Ten slotte is het van belang dat signalen samenkomen en dat afspraken over het melden van signalen, zowel intern als aan andere relevante instanties, worden opgevolgd. Dit begint bij bewustzijn maar omvat ook het verkleinen van mogelijke drempels die er kunnen zijn om signalen te melden. Het is van belang dat medewerkers niet alleen weten dat ze moeten melden, maar ook wat ze moeten melden (zoals afwijkende gedragingen) en waar ze kunnen melden. Dit wordt onder meer opgepakt door het verhogen van bewustzijn op medewerkersniveau, het inrichten van procedures om afwijkende gedragingen te ondervangen en door het samenspel tussen de verschillende toezichtslijnen te versterken.

<u>NCTV</u>
Binnen de NCTV is aandacht voor misbruik onder andere verstevigd door veel duidelijkere kaders te stellen voor de individuele medewerkers waar zij op aangesproken worden. Daarmee wordt duidelijk gemaakt waar mededeling van moet worden gedaan bij de BVA. Het gaat daarbij bijvoorbeeld om meldingen over onjuiste omgang met bijzondere informatie, maar ook om meldingen over afwijkend gedrag van medewerkers, in het bijzonder waar het raakt aan de integriteit en betrouwbaarheid. Door toestemming te vereisen van een leidinggevende om voor iemand anders staatsgeheime stukken te printen, kan er geen twijfel meer over bestaan dat dit een van de procedure afwijkende gedraging is. Door toestemming te vereisen voor het gebruiken van gegevensdragers en daar strikte administratie op te voeren, kan er geen twijfel meer over bestaan dat dit niet zomaar de bedoeling is en dat dit gecontroleerd wordt op mogelijk misbruik. Ook wordt hiermee bereikt dat verschillende signalen ook in samenhang bezien kunnen worden.

Politie
Binnen de politie zullen, om de risico's op het vlak van de omgang met bijzondere informatie alsook de bredere (veiligheid)risico's nader onder de aandacht te brengen, de teams van de politie die met bijzondere informatie werken in 2025 verplicht deelnemen aan een *awareness* training, die vervolgens structureel geborgd zal worden. Deze training zal ook gericht zijn op handelingsperspectieven voor de politiemensen die in de meest risicovolle contexten werken.

Ook treft de politie technische maatregelen, zoals hierboven toegelichte invoering van *protective monitoring* per 1 januari 2025. De basis voor de beoordeling of een handeling als atypisch wordt beschouwd door *protective* monitoring ligt in de bestaande regels voor het raadplegen van politiesystemen en de handreiking die de politie daarvoor heeft opgesteld. Deze regels en handreiking zijn van toepassing op alle politiemedewerkers en vormen onderdeel van hun opleiding. Ook zal de politie onderzoeken of, en zo ja welke, extra technische beveiligingsmaatregelen in politiesystemen gewenst en effectief zijn. Hiervoor wordt een speciaal project ingericht.

c) Het samenspel tussen verschillende organisatieonderdelen

Het derde aspect ziet op het samenspel tussen de verschillende organisatieonderdelen die een (eigen) taak hebben in de beveiliging van bijzondere informatie. In deze context is het van belang om te benoemen dat de informatiebeveiliging langs drie lijnen is opgebouwd. De eerste lijn is het lijnmanagement, dat verantwoordelijk is voor de informatiebeveiliging binnen de eigen organisatie. De tweede lijn is belegd bij de beveiligingscoördinatoren (hierna: BVC) en de *chief information security officer* (hierna: CISO). Zij adviseren het lijnmanagement en houden toezicht namens de lijnmanager binnen de organisatie op de integrale beveiliging. De derde lijn bij de NCTV en de politie is respectievelijk de Beveiligingsautoriteit van het bestuursdepartement van het ministerie van Justitie en Veiligheid en de concern audit van de politie. Uit het ADR rapport wordt duidelijk dat het samenspel tussen deze organisatieonderdelen verbeterd moet worden en dat het huidige toezichtkader niet afdoende is. De posities van de onderdelen moet worden verstevigd en er moet meer aandacht komen voor het opvolgen van aanbevelingen.

Bestuursdepartement

De derde lijn is bij het bestuursdepartement belegd bij de Beveiligingsautoriteit van het ministerie van Justitie en Veiligheid (hierna: de BVA). Uit het rapport blijkt dat de BVA niet altijd over een (voldoende) eigenstandige informatiepositie beschikte en bepaalde beveiligingsincidenten niet als door de eerste of tweede lijn als zodanig herkend en dus gemeld werden. Hierdoor kon onvoldoende invulling worden gegeven aan de toezichthoudende taak van de BVA. Deze moet worden versterkt. De BVA moet daartoe tot andersoortige samenwerkingen komen met alle onderdelen van het departement die met bijzondere informatie werken. De BVA zal daartoe in de reguliere overleggen die periodiek worden gevoerd met alle JenV organisatieonderdelen, waaronder de NCTV, structureel meer aandacht besteden aan diverse onderwerpen, waaronder bijzondere informatie. Doel daarvan is dat de BVA zelf meer informatie ophaalt bij de organisaties binnen het departement waar gewerkt wordt met bijzondere informatie en op basis daarvan aandachtspunten in de informatiebeveiliging identificeert. De versterking van de samenwerking tussen de BVA en NCTV zal prioriteit hebben, mede gelet op de te nemen stappen richting de accreditatie van de NCTV in 2025 en ten aanzien van de vertrouwensfuncties en veiligheidsonderzoeken.

Politie

Bij de politieorganisatie is de derdelijns toezichthoudende taak belegd bij de concern audit. Ten aanzien van de politie komt naar voren dat er door de concern audit wel aanbevelingen werden gedaan, maar dat deze niet altijd werden opgevolgd. Zo constateert de ADR dat de concern audit van de politie weliswaar aan de bel heeft getrokken over het ontbreken van integraal risicomanagement en intern toezicht, maar dat er niet is geacteerd op de aanbevelingen. De politie zal de doorwerking van interne audits versterken. De korpsleiding zal toezien op de opvolging en borging van aanbevelingen die door concernaudit worden gedaan. Tevens zal de politie bezien of de expertise van concern audit kan worden versterkt door politiemensen uit de operationele werkpraktijk toe te voegen aan audits op informatiebeveiliging.

3. Signalen en samenloop van functies

De ADR is ook verzocht om specifiek aandacht te hebben voor de berichtgeving over eerdere signalen en de (wenselijkheid van de) samenloop van functies.[7] Uit het ADR rapport komt niet naar voren

[7] Kamerstukken, 2023-24, 36 410-VI, nr. 16

dat er principiële bezwaren tegen de samenloop van functies waren of zijn. De ADR komt niet tot aanbevelingen op dit vlak.

Wel is de casus aanleiding geweest om te concluderen dat de combinatie van functies en vooral ook de bijbehorende informatiepositie per functie gewogen moeten worden bij verzoeken tot eventuele samenloop, omdat een grotere informatiepositie kan leiden tot grotere risico's bij schending van de geheimhoudingsplicht. Dat zal nadrukkelijker gewogen worden, waarbij vooropstaat dat dit altijd per geval en op basis van de omstandigheden van dat geval moet worden beoordeeld. Ook vraagt zo'n eventuele samenloop om een kritische periodieke evaluatie naar de houdbaarheid daarvan, waarbij actief eventuele signalen ten aanzien van de samenloop en informatiepositie worden meegenomen.

De ADR merkt op dat de NCTV aan een signaal van een NRC-journalist die tijdens een interview met de Nationaal Coördinator aangaf dat de betrokken medewerker een eigen harde schijf mee naar huis zou nemen geen opvolging heeft gegeven. Deze constatering verdient nuancering. De bewuste medewerker had toestemming voor het gebruik van een beperkt aantal specifieke datadragers die vanuit de werkgever waren verstrekt. De journalist in kwestie stelde tijdens het interview echter dat er sprake zou zijn van het gebruik van een eigen harde schijf. Het gebruik van een privéschijf zou een veiligheidsincident zijn. Dit is zorgvuldig uitgelopen. Geconcludeerd is dat er geen sprake was van het gebruik van een privéschijf. Dat misbruik van datadragers in zijn algemeenheid nadere aandacht had verdiend, onderschrijf ik. Om deze reden worden datadragers alleen nog beperkt in noodzakelijke gevallen en onder toezicht uitgegeven.

Verder constateert de ADR dat signalen niet altijd als zodanig werden herkend of doorgegeven. Daardoor kwamen mogelijke signalen niet op de plek waar het mogelijk tot maatregelen had geleid. Om dit te verbeteren zijn per organisatie maatregelen getroffen, zoals eerder in deze brief toegelicht. Bij nevenfuncties is het ook van belang dat bij signalen ook aandacht is voor de mogelijke noodzaak tot het leggen van contact met de counterpart bij de andere organisatie om te toetsen of daar ook signalen zijn. Dat moet onderdeel zijn van het maatwerk dat nodig is in de opvolging van signalen en moet op het juiste niveau worden gewogen.

Tot slot

Het is van belang dat onze informatiebeveiliging, en zeker die van bijzondere informatie, niets te wensen overlaat. De daadwerkelijke beveiliging valt of staat met de implementatie en naleving van procedures en regels. Tegelijkertijd valt niet volledig uit te sluiten dat iemand met beroepshalve gerechtvaardigde toegang daar niet goed mee omgaat. Voor dat aspect is ook meer aandacht nodig. Het is goed en waardevol dat de ADR dit inzichtelijk heeft gemaakt, en zoals aangegeven in deze brief, zijn daar stevige stappen op gezet. Ik heb waardering voor onze mensen die zich inzetten voor onze veiligheid en ik heb ervaren dat de onderzochte organisaties de urgentie voelen en de aanbevelingen van de ADR adequaat hebben opgepakt.

Voor de komende tijd is het belangrijk de vinger aan de pols te houden. Ik heb de ADR gevraagd om een aanvullend onderzoek te doen bij de NCTV naar de opvolging van de aanbevelingen en waar nodig aanvullende aanbevelingen te doen. Ik merk daarbij op dat informatiebeveiliging een cyclisch proces is, en daarmee dus nooit af. Door continu de stappen te doorlopen komen ook continu verbeterpunten naar boven. De ADR heeft aangegeven hiertoe bereid te zijn en te verwachten na 12 maanden een goed beeld van te kunnen geven. De politie gaat de aanbevelingen opnemen in de interne auditcyclus en zal aan de ADR rapporteren over de voortgang. Uw Kamer zal vanzelfsprekend over de uitkomsten worden geïnformeerd.

De minister van Justitie en Veiligheid,
D.M. van Weel