

Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport Beveiligingsproces van staatsgeheime / vertrouwelijke informatie bij NCTV en politie

Definitief 29-11-2024

Departementaal vertrouwelijk

Colofon

Titel	Onderzoeksrapport Beveiligingsproces van staatsgeheime / vertrouwelijke informatie bij NCTV en politie
Uitgebracht aan	Plaatsvervangend secretaris-generaal Ministerie van Justitie en Veiligheid
Datum	29-11-2024
Status	Definitief
Kenmerk	G2024/91

Inhoud

Colofon **2**

1. Aanleiding en scope **5**
1.1 Aanleiding 5
1.2 Wat is er onderzocht? 6
1.3 Scope 6
1.4 Aanpak 7
1.5 Leeswijzer 8

2. Hoofdboodschap: de NCTV en de politie hebben hun eigen kwetsbaarheid gecreëerd **9**

3. Beveiliging van staatsgeheime informatie bij de NCTV **14**
3.1 Risicomanagement 14
3.2 Beleid voor informatiebeveiliging 15
3.3 Selectie en inrichting van maatregelen 16
3.4 Beheersing van toegang 18
3.5 Rubricering van informatie 21
3.6 Verspreiding van staatsgeheime informatie 22
3.7 Veiligheidsonderzoek van de gebruikers van informatie 23
3.8 Logging en monitoring 25
3.9 Behandeling van inbreuken op de beveiliging 26
3.10 Aandacht van het management door controle en toezicht 27

4. Beveiliging van vertrouwelijke informatie bij de politie **29**
4.1 Risicomanagement 29
4.2 Beleid voor informatiebeveiliging 30
4.3 Selectie en inrichting van maatregelen 31
4.4 Beheersing van toegang 32
4.5 Rubricering van informatie 35
4.6 Verspreiding van vertrouwelijke informatie 37
4.7 Screening van de gebruikers van informatie 39
4.8 Logging en monitoring 40
4.9 Behandeling van inbreuken op de beveiliging 42
4.10 Aandacht van het management door controle en toezicht 43
4.11 Langdurige inzet als tolk 44

5. Signalen over de analist/tolk en de opvolging daarvan **46**
5.1 Geen van de geïnterviewden had signalen over het bezitten en naar buiten brengen van staatsgeheime of vertrouwelijke informatie 46
5.2 De samenloop van functies was algemeen bekend en heeft voor 'gedoe' gezorgd maar staat los van de casus 46
5.3 Bij de politie worden enkele voorvallen niet als signaal opgevat 49
5.4 Bij de NCTV worden meldingen van buiten niet opgepakt 49
5.5 NCTV-medewerkers hebben meldingen gedaan na bekend worden van de casus 50

6. Maatregelen na het bekend worden van de casus **51**

7. Verantwoording **55**
7.1 Afbakening 55
7.2 Gehanteerde onderzoeksvragen 56
7.3 Uitgevoerde werkzaamheden 56
7.4 Gehanteerde Standaard 58

7.5 Verspreiding van het rapport 58

Ondertekening **59**

1. Aanleiding en scope

1.1 Aanleiding

Op 26 oktober 2023 zijn twee personen aangehouden op verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Eén van de aangehouden personen was in dienst bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en heeft daar lange tijd gewerkt als analist bij de afdeling Analyse Nationale Veiligheid. Tegelijkertijd werd hij door de politie jarenlang ingehuurd als tolk en vertaler, o.a. bij het cluster Contraterrorisme, Extremisme en Radicalisering (CTER) van de Landelijke Eenheid. De tweede aangehouden persoon is een voormalig medewerker van de NCTV die vlak voor haar aanhouding bij de politie in dienst was gekomen.

Staatsgeheime informatie (NCTV) en vertrouwelijke informatie (politie)
Volgens het VIRBI 2013[1] is 'bijzondere informatie' informatie waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of één of meer ministeries.

'Gerubriceerde informatie' is bijzondere informatie waarvan het rubriceringsniveau en de rubriceringsduur zijn bepaald op basis van te verwachten nadelige gevolgen voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) deze informatie bekend wordt bij niet geautoriseerden.

De in het VIRBI 2013 bepaalde en door de NCTV gebruikte rubriceringsniveaus zijn Departementaal VERTROUWELIJK, Staatsgeheim CONFIDENTIEEL, Staatsgeheim GEHEIM en Staatsgeheim ZEER GEHEIM.

Aangezien Departementaal VERTROUWELIJKE informatie geen deel uitmaakt van de scope van dit onderzoek, spreken we voor de NCTV over 'staatsgeheime informatie'. Dat is die informatie die is gerubriceerd als staatsgeheim (CONFIDENTIEEL, GEHEIM of ZEER GEHEIM).

Het VIRBI 2013 is niet van toepassing op de politie. De politie maakt gebruik van de Rubriceringsregeling Politie 2015. De politie kent de rubriceringsniveaus Niet Vertrouwelijk, Politie INTERN, Politie CONFIDENTIEEL, Politie GEHEIM en Politie ZEER GEHEIM. De Rubriceringsregeling Politie 2015 is een nadere invulling van het classificeren van vertrouwelijkheid zoals beschreven in het Informatiebeveiligingskader voor de Politie. De Rubriceringsregeling Politie 2015 ziet naast het belang van de staat ook op het belang van de politie en de organisaties waar de politie mee samenwerkt.

De focus in dit onderzoek ligt op het politieonderdeel CTER. Ook op het CTER-cluster is de Rubriceringsregeling Politie 2015 van toepassing. Uit dit onderzoek blijkt echter dat CTER geen gebruik maakt van de Rubriceringsregeling Politie 2015. Wel wordt op andere manieren informatie voorzien van een bepaalde classificatie van vertrouwelijkheid, bijvoorbeeld op basis van artikelen van de Wet politiegegevens.

[1] Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013

Om die andere aanduidingen van vertrouwelijkheid mee te nemen, hanteren we in dit onderzoek voor de politie de term 'vertrouwelijke informatie'.

Op 3 november 2023 heeft de minister van Justitie en Veiligheid (JenV) de Kamer geïnformeerd dat een onafhankelijk onderzoek wordt ingesteld dat wordt uitgevoerd door de Auditdienst Rijk. Doel van het onderzoek is 'inzichtelijk maken op welke wijze de beveiliging van de bijzondere informatie in de in deze casus relevante processen en systemen is ingericht teneinde suggesties te doen om de beveiliging waar nodig te verbeteren.' Met 'de casus' wordt in dit rapport de verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie bedoeld.

Insider threat
Insider threat is de dreiging dat een persoon gebruik maakt van zijn toegangsrechten tot informatie, zijn kennis van de organisatie en zijn positie om informatie te verzamelen en buiten de organisatie te brengen, informatie te vernietigen of te veranderen.

De aanleiding voor de persoon om dit te doen kan zijn dat de persoon werkt voor een statelijke actor of een criminele organisatie. Het kan ook gaan om een medewerker die dit doet uit onvrede, met een commercieel doel of een ideëel doel. Ook kan sprake zijn van een medewerker die dit doet vanuit een gebrek aan deskundigheid.

1.2 Wat is er onderzocht?

De volgende onderzoeksvragen zijn beantwoord:

1. Op welke wijze hebben de NCTV en politie ingeregeld dat bijzondere informatie in de in deze casus gebruikte processen en systemen wordt behandeld conform de voorschriften van het VIRBI 2013 of de Rubriceringsregeling Politie 2015?
2. Welke bevindingen hebben wij bij de invulling van de relevante maatregelen in relatie tot deze casus?
3. Welke maatregelen kunnen waar nodig ter aanvulling of verbetering worden getroffen in de in deze casus gebruikte processen en systemen?

Op verzoek van de opdrachtgever zijn daarbij aanvullend drie elementen in het onderzoek meegenomen:

A. De berichtgeving over eerdere signalen en de opvolging daarvan;
B. De (on)wenselijkheid van samenloop van functies;
C. De maatregelen in geval van mogelijk misbruik.

1.3 Scope

Wij hebben een vooronderzoek uitgevoerd om te kunnen bepalen welke processen en systemen voor ons onderzoek het meest relevant zijn, gelet op de casus. Dit heeft geleid tot de volgende scope van het onderzoek:

- De processen en systemen binnen de NCTV rondom de behandeling van staatsgeheime informatie. Daarbij is ingezoomd op de afdeling Analyse Nationale Veiligheid (hierna: afdeling Analyse);

- De processen en systemen binnen de politie rondom de behandeling van vertrouwelijke informatie. Daarbij is ingezoomd op het cluster CTER.

Gezien de aard van de casus is het onderzoek voornamelijk gericht op het verzamelen en verspreiden van informatie door een persoon die werkzaam is binnen deze organisaties en niet op de technische beveiliging van informatie tegen ongewenste toegang van buitenaf.

Als peildatum is 1 oktober 2023 gehanteerd voor het in beeld brengen van de stand van zaken. Beleidsstukken die zijn opgesteld na deze datum en acties die zijn ingezet na deze datum zijn niet meegenomen in het onderzoek, tenzij ze relevant waren voor het in beeld brengen van maatregelen in geval van mogelijk misbruik.

1.4 Aanpak

Voor de beantwoording van onderzoeksvraag 1 is uitgegaan van de beveiliging van bijzondere informatie als continu proces volgens een Plan-Do-Check-Act-cyclus.

Bij het onderzoek naar de Plan-Do-Check-Act (PDCA) cyclus zijn 11 thema's onderscheiden:

1. Risicomanagement;
2. Beleid voor informatiebeveiliging;
3. Selectie en inrichting van maatregelen (baseline);
4. Beheersing van toegang (autorisatiebeheer);
5. Rubricering van informatie;
6. Verspreiding van staatsgeheime / vertrouwelijke informatie;
7. Screening/veiligheidsonderzoek van de gebruikers van informatie;
8. Logging en monitoring;
9. Behandeling van inbreuken op de beveiliging;
10. Aandacht van het management door controle en toezicht;
11. Langdurige inzet als tolk (dit thema is alleen van toepassing voor de politie).

Voor de beantwoording van vraag 2 is bij vier thema's ingezoomd op de invulling van de relevante maatregelen in relatie tot deze casus. Het gaat om de thema's beheersing van toegang (autorisatiebeheer), verspreiding van staatsgeheime of vertrouwelijke informatie, screening/veiligheidsonderzoek van de gebruikers van informatie en langdurige inzet als tolk.

De aanbevelingen (onderzoeksvraag 3) volgen uit de bevindingen die naar voren zijn gekomen bij de beantwoording van onderzoeksvragen 1 en 2. Bij de beantwoording van vraag 3 zijn we uitgegaan van zo weinig mogelijk beleid en zoveel mogelijk praktische handvatten (focus op fasen Do, Check en Act).

Om de onderzoeksvragen te kunnen beantwoorden, zijn documenten opgevraagd en geanalyseerd, zijn interviews gehouden met relevante functionarissen binnen beide onderzochte organisaties, is gebruik gemaakt van de door de beide organisaties opgestelde feitenrelazen en zijn bij beide organisaties waarnemingen gedaan.
In ieder interview hebben we gevraagd of er signalen over de casus bekend waren bij de betreffende medewerker.

1.5 Leeswijzer

- Hoofdstuk 2 bevat de hoofdboodschap.
- Hoofdstuk 3 beschrijft de beveiliging van staatsgeheime informatie bij de NCTV (onderzoeksvragen 1 t/m 3).
- Hoofdstuk 4 beschrijft de beveiliging van vertrouwelijke informatie bij de politie (onderzoeksvragen 1 t/m 3).
- Hoofdstuk 5 betreft de signalen over de analist/tolk en de opvolging daarvan binnen zowel de NCTV als de politie. Ook de (on)wenselijkheid van de samenloop van functies komt hier aan bod. De twee elementen (elementen A en B) zijn als één geheel benaderd vanwege hun onderlinge samenhang.
- Hoofdstuk 6 betreft de maatregelen die de NCTV en de politie hebben getroffen na het bekend worden van de casus (element C).
- Hoofdstuk 7 bevat de verantwoording van het onderzoek.

Dit rapport bevat drie kleurenkaders. De betekenis van de kaders is als volgt:

- Grijze kaders bevatten aanvullende uitleg over gebruikte terminologie, wetgeving of relevante organisatie-specifieke informatie die helpt bij het begrijpen van (de context van) dit rapport.
- Blauwe kaders beschrijven hoe zaken zijn verlopen in de casus (onderzoeksvraag 2).
- Witte kaders betreffen aanbevelingen (onderzoeksvraag 3).

De bevindingen in dit rapport geven de stand van zaken weer op de peildatum, 1 oktober 2023, tenzij anders aangegeven.

2. Hoofdboodschap: de NCTV en de politie hebben hun eigen kwetsbaarheid gecreëerd

Inleiding

Op 26 oktober 2023 zijn twee personen aangehouden op verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Eén van de aangehouden personen was in dienst bij de NCTV en heeft daar lange tijd gewerkt als analist bij de afdeling Analyse Nationale Veiligheid. Tegelijkertijd werd hij door de politie jarenlang ingehuurd als tolk en vertaler o.a. bij het cluster Contraterrorisme, Extremisme en Radicalisering (CTER) van de Landelijke Eenheid[2].

Op 3 november 2023 heeft de minister van Justitie en Veiligheid de Kamer geïnformeerd dat een onafhankelijk onderzoek wordt ingesteld dat wordt uitgevoerd door de Auditdienst Rijk. Doel van het onderzoek is 'inzichtelijk maken op welke wijze de beveiliging van de staatsgeheime of vertrouwelijke informatie in de in deze casus relevante processen en systemen is ingericht teneinde suggesties te doen om de beveiliging waar nodig te verbeteren.' Met 'de casus' wordt in dit rapport bedoeld de verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie.

Uit ons onderzoek blijkt dat de NCTV en de politie beide nog niet de basis op orde hebben wat betreft de beveiliging van staatsgeheime en/of vertrouwelijke informatie. In de volgende hoofdstukken zijn onze bevindingen bij de door ons onderzochte thema's in detail uitgewerkt. In deze hoofdboodschap hebben we de belangrijkste punten opgenomen die ertoe bijgedragen hebben dat het ongewenst verzamelen en verspreiden van staatsgeheime en/of vertrouwelijke informatie mogelijk was.

Management heeft weinig aandacht voor insider threat en gaat uit van vertrouwen

Het management van zowel de NCTV als de politie heeft weinig aandacht gehad voor insider threat. Dit blijkt onder andere uit het feit dat er geen aandacht aan geschonken is in risicoanalyses en dat er te beperkt maatregelen zijn getroffen om de ongewenste verspreiding van informatie door medewerkers tegen te gaan.

Uit de gevoerde gesprekken bij de NCTV blijkt dat de organisatie sterk vertrouwt op de veiligheidsonderzoeken van medewerkers. Andere maatregelen om het risico op het verzamelen en meenemen van staatsgeheime informatie door medewerkers te verkleinen, zijn niet getroffen (bijv. rondom toegangsrechten en het bepalen van de vertrouwelijkheid van informatie). Het is een goed uitgangspunt om de eigen medewerkers te vertrouwen, maar een Verklaring van Geen Bezwaar alleen is onvoldoende om staatsgeheime informatie te beveiligen tegen insider threat.

De tolk werd binnen de politie dermate lang ingehuurd als externe medewerker dat hij veelal werd behandeld als

[2] In relatie tot de NCTV verwijzen we naar deze persoon als 'analist'. In relatie tot de politie noemen we deze persoon 'tolk'.

politiemedewerker en het daarbij passende vertrouwen kreeg. Dit terwijl zijn screening al sinds 2016 was verlopen. De behoefte aan een vaste tolk die de context van de CTER-thematiek kent, is begrijpelijk, maar het risico dat gepaard gaat met langdurige inzet is niet erkend.

Beide organisaties hebben nog geen baseline ingericht, de politie is daarmee bezig

De NCTV heeft geen actuele baseline[3] van informatiebeveiligingsmaatregelen die is gebaseerd op de Baseline Informatiebeveiliging overheid (BIO) en het VIRBI. Er is sinds 2020 geen aandacht besteed aan de implementatie van en de controle op de werking van beveiligingsmaatregelen. De capaciteit voor de implementatie van informatiebeveiligingsmaatregelen was beperkt.

De politie beschikt over een gedegen baseline voor de beveiliging van vertrouwelijke informatie die gebaseerd is op de BIO en de Rubriceringsregeling politie. Op dit moment loopt een politiebreed BIO-implementatietraject. Het traject is gestart binnen het politiedienstencentrum. De interne auditfunctie van de politie heeft onderzoek gedaan naar de invoering van een aantal BIO-maatregelen. Zij heeft de werking van de maatregelen niet vast kunnen stellen. De implementatie van de baseline is binnen CTER nog niet gestart.

Toegangsrechten zijn niet ingericht conform het principe 'need to know'

Binnen de NCTV is het mogelijk om veel informatie te verzamelen, omdat er brede autorisaties op de systemen worden uitgegeven. Toegang tot het belangrijkste dossiersysteem in de casus (het staatsgeheime digitale archiefsysteem), betekent toegang tot alle daarin opgenomen stukken die veelal zijn gerubriceerd als staatsgeheim. Voor medewerkers met toegang tot het staatsgeheime digitale archiefsysteem is het dus ook mogelijk om stukken in te zien, op te slaan en af te drukken die niet noodzakelijk zijn voor hun eigen werkzaamheden.

Uit ons onderzoek bij de politie blijkt dat in het opsporingssysteem van de politie (Summ-IT) een groot aantal personen wordt geautoriseerd voor onderzoeken van CTER. Bovendien kan een groot deel van de geautoriseerde personen zelf weer anderen toegang verlenen tot het dossier van een onderzoek. Eenmaal uitgegeven autorisaties worden veelal niet meer ingetrokken. De controle van uitgegeven autorisaties is binnen CTER niet ingericht. Tolken hebben geen toegang tot Summ-IT.

Voor het opnamesysteem is geen toegang op basis van 'need to know' ingericht binnen CTER. Tolken hebben geen eigen autorisaties voor toegang tot het opnamesysteem, maar moeten de gesprekken wel kunnen vertalen. Daarom lenen rechercheurs hun eigen autorisatie en laptop uit om tolken toegang te verlenen tot het opnamesysteem voor de vertaling van opgenomen gesprekken. Tolken kunnen via deze weg ook andere vertrouwelijke informatie inzien en opslaan.

Wel kent de politie voorzieningen voor het beheer van toegangsrechten. Er worden standaard toegangsrechten toegekend per rol. Ook is het in twee van de drie onderzochte

[3] Set van maatregelen die samen het basisniveau informatiebeveiliging vormen.

systemen mogelijk om fijnmazige toegangsrechten in te richten. Dit biedt een basis voor de politie om op voort te bouwen.

Weinig grip op de verspreiding van staatsgeheime of vertrouwelijke informatie

Beide organisaties kennen beleid en werkinstructies over hoe om te gaan met staatsgeheime of vertrouwelijke informatie, maar er zijn meer maatregelen nodig om ongewenste verspreiding te voorkomen.

Medewerkers binnen de NCTV met toegang tot het staatsgeheime digitale archiefsysteem kunnen staatsgeheime documenten downloaden en opslaan op een persoonlijke map of afdelingsmap. Vervolgens is het mogelijk om documenten te printen. Er wordt op de afdeling Analyse veel geprint. Het gebruik van USB-sticks wordt door de NCTV beperkt, maar de analist had jarenlang wel beschikking over drie USB-sticks en een harde schijf.

Er ontbreken voorzieningen om de uitwisseling van vertrouwelijke informatie tussen rechercheurs en tolken veilig te laten plaatsvinden. Doordat binnen CTER bestanden via onveilige kanalen worden gedeeld tussen rechercheurs en tolken is het voor tolken op verschillende manieren mogelijk vertrouwelijke informatie te verzamelen en te verspreiden:

- [redacted]
- Er worden USB-sticks gebruikt om audiobestanden of te vertalen documenten te delen tussen rechercheur en tolk. Via opname- en afluisterapparatuur verzamelde audiobestanden kunnen op een USB-stick worden opgeslagen. Het is niet verboden USB-sticks mee te nemen buiten het pand.
- [redacted]
- [redacted]

Beide organisaties hebben logging op het gebruik van de meeste systemen en applicaties ingericht, maar monitoren de wijze waarop medewerkers omgaan met staatsgeheime of vertrouwelijke informatie niet. Het verzamelen en meenemen van staatsgeheime of vertrouwelijke informatie is relatief eenvoudig en wordt niet door monitoring gesignaleerd.

Beide organisaties houden geen toezicht op de werking van beveiligingsmaatregelen

Binnen beide organisaties zien we dat er weinig capaciteit beschikbaar is voor de controle van beveiligingsmaatregelen. De NCTV heeft een medewerker die lange tijd zowel beveiligingscoördinator als CISO[4] was. Binnen de politie is de CISO-functie lange tijd niet ingevuld en voeren beveiligings-coördinatoren hun taken vaak uit naast een andere rol.

Management van NCTV en CTER sturen niet op de uitvoering van controles op de werking van beveiligingsmaatregelen.

De Plan-Do-Check-Act-cyclus is niet sluitend

We hebben binnen beide organisaties vastgesteld dat er al veel, vaak nog bruikbaar, beleid is. Er is daarentegen minder aandacht voor de invoering van beveiligingsmaatregelen. Bij beide

[4] Chief Information Security Officer

organisaties hebben we een aantal ingerichte maatregelen gezien, maar er wordt niet vastgesteld of het niveau van de baseline wordt behaald en de samenhang tussen de baseline en de getroffen maatregelen ontbreekt. Er is zeer beperkt interne controle ingericht. Bij de NCTV is de afgelopen jaren geen structurele interne controle uitgevoerd. Bij de politie is een beperkte interne controle uitgevoerd door de interne auditfunctie. Geen van beide organisaties kan aantonen dat actualisatie van beleid en uitvoering plaatsvindt op basis van controles of audits. Met andere woorden: er is veel aandacht voor de fase Plan, maar te weinig aandacht voor de rest van de PDCA-cyclus.

Er zijn geen signalen geweest over het verzamelen en verspreiden van staatsgeheime of vertrouwelijke informatie

Wij hebben alle geïnterviewden bij de NCTV en de politie gevraagd of zij signalen hadden over de casus: de verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Geen van de geïnterviewden heeft aangegeven dat zij dergelijke signalen hebben gehad.

Wel is aangegeven dat er spanningen waren rondom de analist/tolk, omdat hij weinig tegenspraak duldde. De analist/tolk had bij beide organisaties een aparte status, had toegang tot veel (staatsgeheime of vertrouwelijke) informatie en de beschikking over middelen zoals USB-sticks. Ook werd hij bij beide organisaties gezien als kundig, flexibel en een harde werker.

De samenloop van zijn werkzaamheden bij de NCTV en de politie was algemeen bekend binnen beide organisaties en leidde meerdere keren tot 'gedoe', omdat de analist/tolk de rollen niet goed kon scheiden en soms informatie van de ene organisatie gebruikte binnen een andere organisatie. Dit is nooit aanleiding geweest om de samenloop van functies te heroverwegen.
Het 'gedoe' over de samenloop van functies is nooit in verband gebracht met de verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Dit is in onze ogen begrijpelijk.

Er zijn twee gebeurtenissen waarbij nader onderzoek in onze ogen passend was geweest:

-
- In 2021 is in een interview tussen een journalist van de NRC en de Nationaal Coördinator aan de orde geweest dat de analist over een harde schijf beschikte die hij ook mee naar huis zou nemen.[6]

Na het bekend worden van de casus hebben verschillende medewerkers van de NCTV aan de beveiligingscoördinator gemeld dat ze benaderd zijn door de analist om voor hem te printen vanaf het staatsgeheime netwerk (Stg.-net).

Na het bekend worden van de casus hebben de politie en de NCTV maatregelen getroffen

N.a.v. de casus zijn binnen de NCTV een Beleidsincidenten Team en een stuurgroep ingericht. Deze zijn gericht op de directe (operationele) consequenties en maatregelen voor de NCTV en de gevolgen van de casus voor de NCTV als werkgever. Eén van de getroffen maatregelen is het beperken van de toegang tot het staatsgeheime digitale archiefsysteem.

[6] Dit punt is in 2021 niet gepubliceerd door de NRC. In 2023 is dit wel vermeld door de NRC in een artikel dat betrekking heeft op de casus.

De NCTV heeft een korte eigen verkenning uitgevoerd waaruit bleek dat de potentiële schade groot was, vanwege de ruime toegang die de analist had tot staatsgeheime informatie. Er wordt onderzoek uitgevoerd door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), door de ADR en door het OM.

Binnen de NCTV loopt sinds 2023 een verbetertraject voor de beveiliging van informatie. De focus van het traject ligt in eerste instantie op het opstellen van beleidsstukken en de invoering van een baseline. Dit verbetertraject is gestart voordat de casus aan het licht kwam en uitgebreid n.a.v. de casus. Zo is besloten tot het oprichten van een specifieke afdeling Governance, Risicomanagement en Compliance en zijn de processen rond het verspreiden van staatsgeheimen en het gebruik van het Stg.-net aangepast.

Bij de politie zijn na de aanhouding van de tolk twee beleidsinterventie teams (BIT's) opgestart: het BIT Landelijke Eenheid en het BIT Korpsstaf. Het BIT Landelijke Eenheid is verantwoordelijk voor het inzichtelijk maken van personele en operationele risico's voor de Landelijke Eenheid, het reconstrueren van de gang van zaken rond de inzet van de tolk en de zorg voor het personeel van het cluster CTER. Het BIT Korpsstaf is verantwoordelijk voor de coördinatie van maatregelen binnen het gehele korps n.a.v. de aanhouding van de tolk en de afstemming met externe partijen zoals het OM.

De politie heeft n.a.v. de casus gedetailleerd onderzoek gedaan naar de inzet van de tolk (o.a. registratie in het tolkenregister, eerder gedane meldingen en screening), de toegang van de tolk tot Summ-IT (n.a.v. een waarneming door de ADR) en de werkwijze van CTER t.a.v. de omgang met tolken.
De politie doet nog nader onderzoek tot welke informatie de tolk toegang had.

Aanbevelingen op hoofdlijnen

Denk expliciet na over insider threat en de beveiliging van staatsgeheime of vertrouwelijke informatie, bijvoorbeeld in een periodieke risicoanalyse en pas beleid en maatregelen hierop aan. We onderstrepen dat de nadruk zou moeten liggen op de uitvoering van maatregelen en op de controle of de maatregelen werken zoals bedoeld. Het management is ervoor verantwoordelijk dat het toezicht plaatsvindt en moet dit actief vaststellen om te kunnen bepalen welke acties nodig zijn voor het continu verbeteren van de beveiliging van informatie.

Dit rapport bevat meerdere aanbevelingen om het ongewenst verspreiden van informatie te signaleren en voorkomen. We noemen hier enkele aanbevelingen die direct opgepakt kunnen worden:

- Richt het principe 'need to know' in voor de systemen die staatsgeheime of vertrouwelijke informatie bevatten. De door ons onderzochte systemen bieden daar voor het merendeel goede mogelijkheden voor.
- Ga medewerkershandelingen monitoren om ongewenst gedrag eerder te kunnen signaleren. Zowel de NCTV als de politie beschikken al over uitgebreide logging die monitoring mogelijk maakt.
- Richt binnen CTER (en mogelijk breder binnen de politie) voorzieningen in zodat rechercheurs en tolken veilig kunnen samenwerken.

3. Beveiliging van staatsgeheime informatie bij de NCTV

3.1 Risicomanagement

Doel van informatiebeveiliging
Het doel van informatiebeveiliging is het beheersen van de risico's die betrekking hebben op de informatievoorziening van de NCTV.

Risicomanagement
Informatiebeveiliging (als ook de overige onderdelen van de integrale beveiliging) is gebaseerd op een actueel inzicht in de potentiële risico's van de organisatie. Jaarlijks wordt met behulp van verschillende registraties en onderzoeken een actueel beeld geschetst van de potentiële risico's. Zodoende staan beveiligingsmaatregelen (zowel preventief als correctief) in verhouding met het risico. Het lijnmanagement maakt met behulp van dit beeld een bewuste keuze op de afweging van kosten versus baten/werkbaarheid. Als het gaat om specifieke risico's of dreigingen kunnen netwerkpartners adviseren over de te nemen maatregelen.
Met behulp van risicomanagement is de uitvoering van het informatiebeveiligingsbeleid actueel en doeltreffend. De uitwerking van het beleid is uiteraard alleen volledig effectief als het beleid is geborgd in de organisatie.

Beleid Informatiebeveiliging NCTV (2019)

Er is geen actuele risicoanalyse waarin o.a. insider threat is meegenomen, er zijn geen maatregelen genomen op basis van eerdere risicoanalyses

De NCTV beschikt niet over een actuele risicoanalyse die betrekking heeft op staatsgeheime informatie en er is geen sprake van ingericht risicomanagement rondom informatiebeveiliging.

In het verleden zijn er binnen de NCTV risicoanalyses uitgevoerd:

- In 2017 is een Kwetsbaarheidsanalyse Spionage (KWAS) uitgevoerd. De nota die is opgesteld n.a.v. de KWAS bevat concrete en bruikbare aanbevelingen. De CISO/BVC[7] geeft aan dat er niet veel gebeurd is met de uitkomsten van de analyse. De maatregelen die op basis van de KWAS zijn voorgesteld aan het managementteam (MT) NCTV, zijn niet geïmplementeerd.
- In 2022 zijn IB-quickscans[8] uitgevoerd van de door ons onderzochte systemen. De nota's die n.a.v. de IB-quickscans zijn opgesteld, bevatten concrete actiepunten en risico-overzichten. Er is geen zichtbare opvolging van de actiepunten. De aandacht voor informatiebeveiliging was binnen de NCTV vooral gericht op de Digitale Werkomgeving Rijk (DWR; de "standaard" werkplek) en

[7] Chief Information Security Officer / Beveiligingscoördinator

[8] Informatiebeveiliging (IB) QuickScan: toets voor het bepalen van het beveiligingsniveau van een informatiesysteem op basis van het belang van het systeem, het dreigingsprofiel en betrouwbaarheidseisen

niet op het netwerk en de systemen met staatsgeheime informatie.

De CISO/BVC had een belangrijke rol in bovenstaande initiatieven. Het management van de NCTV was hier niet bij betrokken. Ons beeld is dat de aanwezige risicoanalyses (de KWAS in 2017 en de IB-quickscans in 2022) zorgvuldig zijn uitgevoerd.

Veiligheidsonderzoeken zijn de basis voor samenwerken
In interviews is aangegeven dat binnen de NCTV veel waarde wordt gehecht aan de door de AIVD uitgevoerde veiligheidsonderzoeken. Deze veiligheidsonderzoeken en bij positieve afloop verstrekte Verklaringen van Geen Bezwaar (VGB) worden gezien als basis voor samenwerken binnen de NCTV. Het vertrouwen in veiligheidsonderzoeken en VGB's verklaart mogelijk dat insider threat binnen de NCTV weinig aandacht heeft gekregen.

Wat te doen?
Actualiseer de risicoanalyse met aandacht voor bedreigingen die vanuit de eigen organisatie komen (insider threats). Maak daarbij gebruik van de al uitgevoerde IB-quickscans. Maak risicoanalyse een vast onderdeel van het jaarplan informatiebeveiliging dat jaarlijks door het MT NCTV wordt vastgesteld en gemonitord.

3.2 Beleid voor informatiebeveiliging

Het IB-beleid is wat gedateerd maar nog steeds relevant
De NCTV heeft Informatiebeveiligingsbeleid (IB-beleid) dat door het MT is vastgesteld in 2013 en voor het laatst is bijgesteld in 2019. Het beleid beschrijft relevante thema's, o.a.:

- normen en standaarden die van toepassing zijn – er wordt hier expliciet verwezen naar het VIRBI;
- risicomanagement;
- rubricering;
- verwerken van staatsgeheime informatie;
- het buiten de organisatie brengen van (staatsgeheime) informatie;
- rollen, taken en verantwoordelijkheden.

Het beleid is verder uitgewerkt in o.a. het *Tactisch kader integrale beveiliging NCTV* (dat ook voor het laatst is bijgesteld in 2019) en de *NCTV Rubriceringskaart* (2021).

De frequentie waarmee IB-beleid moet worden geëvalueerd en bijgesteld, is niet uitgewerkt. De NCTV heeft lange tijd de rollen CISO en BVC belegd bij één persoon. Door de beperkte capaciteit was er te weinig aandacht voor het IB-beleid en zijn delen van het IB-beleid (rollen, geldende kaders) niet meer geheel actueel. Desondanks is ons beeld dat het bestaande IB-beleid nog steeds relevant is. Het wat gedateerde IB-beleid is in onze ogen geen aanleiding geweest voor de casus.

In 2023 worden na een analyse stappen gezet om het IB-beleid te vernieuwen
In het voorjaar van 2023 geeft het strategisch jaarplan IB van de NCTV aan dat de NCTV gedeeltelijk voldoet aan de eisen vanuit BIO en VIRBI. De analyse van de NCTV is dat als de NCTV

onvoldoende capaciteit vrijmaakt, de mogelijke gevolgen zijn: een lager volwassenheidsniveau dat kan leiden tot reputatieschade, onvoldoende risicobeheersing en geen inzage in de weerbaarheid van derde partijen waar de NCTV diensten van afneemt.

De analyse is de aanleiding geweest om t.a.v. IB-beleid in 2023 stappen te zetten. In september 2023 is een team geformeerd dat het nieuwe IB-beleid vorm moet geven. De rollen CISO en BVC worden belegd bij verschillende personen en het MT NCTV besluit dat er een separate risk- en compliance afdeling wordt opgericht.

Wat te doen?
Er is veel aandacht voor het formuleren van nieuw IB-beleid maar dat heeft in onze ogen niet de hoogste prioriteit. Volgens ons moet de focus liggen op het treffen van de juiste maatregelen en de controle of gekozen maatregelen (blijven) werken. M.a.w. focus op de fasen Do, Check en Act van de PDCA-cyclus en niet op de fase Plan.

3.3 Selectie en inrichting van maatregelen

BIO
De rijksoverheid beschikt al geruime tijd over een basis beveiligingsniveau voor informatiebeveiliging (een zgn. baseline informatiebeveiliging) die gebaseerd is op internationale standaarden voor beveiliging van informatie (ISO 27001 en ISO 27002).

In 2012 werd de Baseline Informatiebeveiliging Rijksdienst 2012 (BIR 2012) geïntroduceerd. In 2017 verscheen een geactualiseerde versie, de BIR 2017. Deze werd in 2019 opgevolgd door de Baseline Informatiebeveiliging Overheid (BIO). De BIO bevat 114 beheersmaatregelen. Iedere overheidsorganisatie moet de BIO hanteren als basis voor informatiebeveiliging.

Er is geen actueel overzicht van de voor de NCTV noodzakelijke beveiligingsmaatregelen
Het meest recente overzicht van beveiligingsmaatregelen waar de NCTV over beschikt, dateert van juli 2020 en is gebaseerd op de BIR 2017. Tijdens ons onderzoek is de volgende toelichting bij het overzicht gegeven:

- De opzet van ingerichte maatregelen was in 2020 nog niet op orde.
- De maatregelen voor leveranciersmanagement waren nog onvoldoende ingericht.

De actualiteit van de weergegeven status per maatregel en de verantwoordelijkheid per maatregel in het overzicht zijn onduidelijk.

De NCTV beschikt hiermee al een aantal jaren niet over een actuele set van noodzakelijke beveiligingsmaatregelen die gebaseerd is op de BIO (waar de NCTV als onderdeel van de rijksoverheid aan moet voldoen) en die aangevuld is met maatregelen rondom staatsgeheime informatie vanuit het VIRBI en maatregelen op basis van risicoanalyses door de NCTV.

In de afgelopen jaren is de werking van maatregelen niet structureel gecontroleerd
De monitoring van het functioneren van alle getroffen beveiligingsmaatregelen gebeurt niet structureel. Het afdelingshoofd Bedrijfsvoering (die de rol CIO vervult) en de

directeur Bedrijfsvoering houden geen toezicht. Alleen de CISO/BVC voerde in het verleden controles uit.

Er worden sinds 2020 geen rapportages meer gemaakt door de CISO/BVC. Na 2021 heeft geen monitoring meer plaatsgevonden op de werking van de maatregelen. Interviews geven het beeld dat rapportages over uitgevoerde controles stil zijn komen te liggen, omdat toezichtsrapportages geen impact hadden. Een eerder afdelingshoofd Bedrijfsvoering heeft aangegeven dat er geen rapportages over informatiebeveiliging naar het MT hoefden.

De NCTV heeft geen actueel beeld over de werking van beveiligingsmaatregelen en weet niet in hoeverre wordt voldaan aan BIO en VIRBI

Door het ontbreken van een actueel overzicht van alle noodzakelijke beveiligingsmaatregelen en het ontbreken van controles beschikt de NCTV niet over een actueel beeld van de werking van noodzakelijke beveiligingsmaatregelen. Dat houdt ook in dat de NCTV niet weet in hoeverre wordt voldaan aan BIO en VIRBI.

De BVA van JenV heeft niet gerapporteerd dat de NCTV niet voldoet aan de BIO- en accreditatie-eisen

De BVA van JenV houdt toezicht op integrale beveiliging in een 3-jaarlijkse cyclus. De BVA rapporteert aan de NCTV in de vorm van een nota. De meest recente nota (mei 2022) heeft betrekking op het jaar 2021. De BVA heeft geoordeeld dat "*...de voortgang op basis van de aangeleverde informatie voldoende is*". In de nota worden geen opmerking gemaakt over de gedateerde basis (BIR 2017 in plaats van BIO) voor de beveiligingsmaatregelen van de NCTV, noch over het ontbreken van accreditatie van het Stg.-net.

Er is door de BVA geen nota over 2022 opgesteld. Tijdens de uitvoering van het onderzoek was nog geen nota over 2023 beschikbaar.

In het voorjaar van 2024 is Stg.-net voorlopig geaccrediteerd

De NCTV is ervoor verantwoordelijk dat accreditatie van het Stg.-net van de NCTV plaatsvindt. De BVA adviseert de SG om een accreditatie af te geven. Op de peildatum was Stg.-net niet geaccrediteerd. De BVA heeft in het voorjaar van 2024 een onderzoek uitgevoerd dat heeft geleid tot een voorlopige accreditatie (Interim Approval To Operate) door de SG.

De NCTV heeft maatregelen bijgesteld na testen

De NCTV geeft aan dat enkele uitgevoerde testen (pentesten, red teaming en security testen) in 2022 hebben geleid tot bijstelling van maatregelen. Uit aangeleverde informatie maken wij op dat de bijstelling betrekking heeft op toegangsrechten voor beheerders en beheer van laptops.

Inspectie door de Europese Unie (2019) die begeleid werd door de NSA en rapportage door de BVA (2022) zijn geen aanleiding geweest voor bijstelling van beveiligingsmaatregelen, keuze voor nieuwe maatregelen en/of het actualiseren van de baseline.

Wat te doen?

- Voer de BIO in. Voorkom daarbij een papieren werkelijkheid. D.w.z. hanteer als uitgangspunt dat maatregelen pas zijn ingevoerd als ze aantoonbaar werken.
- Vul de maatregelen uit de BIO waar nodig aan met NCTV-specifieke maatregelen op basis van een actuele risicoanalyse en het VIRBI.
- Controleer periodiek de werking van maatregelen.

3.4 Beheersing van toegang

Voorzieningen bij de NCTV voor het raadplegen en bewerken van staatsgeheime informatie
De NCTV is aangesloten op het netwerk NL-net. Via dit netwerk krijgt de NCTV (staatsgeheime) informatie aangeleverd van de AIVD, MIVD en andere departementen. De NCTV kan ook zelf informatie via NL-net verzenden.

De NCTV beschikt zelf over een afgeschermd netwerk voor staatsgeheime informatie, het Stg.-net. Op dit netwerk kunnen medewerkers van de NCTV gebruikmaken van Office en drie informatiesystemen:

- Het staatsgeheime DMS - het documentmanagementsysteem van de NCTV dat wordt gebruikt voor de distributie van staatsgeheime informatie naar medewerkers van de NCTV;
- Het staatsgeheime digitale archiefsysteem - het documentmanagementsysteem voor de afdeling Analyse;
- Het staatsgeheime documentmanagementsysteem voor de afdeling Bewaken en Beveiligen.

In ons onderzoek hebben wij ons gericht op het staatsgeheime DMS en het staatsgeheime digitale archiefsysteem.

Naast de drie informatiesystemen hebben medewerkers de beschikking over afdelingsmappen en persoonlijke mappen voor het opslaan en bewerken van staatsgeheime informatie. (Staatsgeheime) Informatie die bij de NCTV binnenkomt via NL-net, wordt overgezet naar het staatsgeheime DMS op het Stg.-net. Dit gebeurt onder verantwoordelijkheid van het frontoffice van het Nationaal Crisiscentrum (NCC) van de NCTV. Het frontoffice plaatst staatsgeheime informatie in een zaak in het staatsgeheime DMS en geeft personen toegang tot een zaak. Personen die toegang hebben tot een zaak, kunnen de daarin opgeslagen informatie lezen, afdrukken en downloaden en vervolgens opslaan in het staatsgeheime digitale archiefsysteem, de afdelingsmap, de persoonlijke map of een USB-stick.

Het staatsgeheime digitale archiefsysteem bevat het volledige archief van ontvangen staatsgeheime stukken van AIVD en MIVD (Inlichtingenanalyses en inlichtingenberichten) en door NCTV geproduceerde analyses.

Het staatsgeheime digitale archiefsysteem is onderverdeeld in een aantal categorieën. Medewerkers kunnen in het staatsgeheime digitale archiefsysteem een bepaalde rol krijgen. Per categorie kan worden bepaald welke rol toegang heeft tot de informatie en wat de betreffende rol met die informatie mag doen. Ook vanuit het staatsgeheime digitale archiefsysteem kan informatie worden geprint en worden gedownload en opgeslagen in de afdelingsmap, in de persoonlijke map of op een USB-stick.

Het beleid rondom autorisaties is beschreven, het principe 'need to know' is niet uitgewerkt, verantwoordelijkheden zijn niet helemaal helder
In 2019 heeft de NCTV het beleid rondom autorisaties uitgewerkt. In het beleid is aandacht voor het proces van toekennen van autorisaties, de mandatering, de periodieke controle van autorisaties en de verschillende rollen bij het toekennen.

Het VIRBI schrijft voor dat staatsgeheime informatie zodanig wordt beveiligd dat alleen personen die daartoe zijn geautoriseerd deze kunnen behandelen of inzien voor zover dit noodzakelijk is voor een goede uitoefening van hun taak. Het beleid voor informatiebeveiliging van de NCTV geeft aan dat 'need to know' een uitgangsprincipe is. In het beleid ontbreekt de uitwerking van dit uitgangsprincipe voor staatsgeheime informatie in het staatsgeheime DMS, het staatsgeheime digitale archiefsysteem en afdelingsmappen.

De BVC en de systeemeigenaar hebben volgens het beleid beiden verantwoordelijkheden voor het ontwikkelen en onderhouden van beleid/documentatie. Over de verantwoordelijkheid voor het toekennen van autorisaties bestaat een eenduidig beeld. De leidinggevende is verantwoordelijk voor de uitvoering van het autorisatiebeleid, de BVC is verantwoordelijk voor het uitvoeren van een aantal controles bij het toekennen van autorisaties. Het is onduidelijk wie eindverantwoordelijk is voor het gehele proces en het beheer van uitgegeven rechten.

In het staatsgeheime digitale archiefsysteem en het staatsgeheime DMS kunnen toegangsrechten gedetailleerd worden toegekend; de mogelijkheden worden niet optimaal benut

In het staatsgeheime digitale archiefsysteem worden vijf "containers" (categorieën) onderscheiden waarin informatie is ondergebracht. Iedere medewerker van de afdeling Analyse heeft toegang tot deze vijf containers. De NCTV beschouwt dit als noodzakelijk omdat er op die manier altijd toegang is tot de noodzakelijke informatie in het geval van een calamiteit of crisis, onafhankelijk van welke medewerkers op dat moment beschikbaar zijn.

In het staatsgeheime digitale archiefsysteem is het mogelijk om een fijnmazige structuur van toegangsrechten toe te passen door per groep medewerkers te bepalen welke informatie de medewerkers in de groep mogen inzien en bewerken. Daarvoor moeten er binnen de afdeling Analyse meerdere rollen onderscheiden worden. Dat is nu niet het geval. De huidige structuur van toegangsrechten wordt door de NCTV (en door de ADR) niet gezien als invulling van het principe 'need to know'. Daarvoor heeft een te grote groep medewerkers binnen het staatsgeheime digitale archiefsysteem dezelfde toegangsrechten.

In 2022 is door de manager van de afdeling Analyse gekozen voor beperking van de toegang tot het staatsgeheime digitale archiefsysteem voor medewerkers van andere afdelingen dan Analyse. Medewerkers van andere afdelingen die toegang nodig hebben tot het staatsgeheime digitale archiefsysteem krijgen zes maanden toegang tot het staatsgeheime digitale archiefsysteem, daarna vervalt de toegang automatisch. In de praktijk bleek het automatisch na zes maanden laten vervallen van toegangsrechten technisch niet mogelijk. Daarna werd ervoor gekozen dit procedureel te regelen door een lijst aan de managers van andere afdelingen dan Analyse te sturen op basis waarvan de geldigheid van autorisaties kon worden bepaald. Deze aanpak is niet daadwerkelijk gebruikt. Toegangsrechten tot het staatsgeheime digitale archiefsysteem voor medewerkers van andere afdelingen dan Analyse worden niet na zes maanden ingetrokken. Eenmaal uitgegeven autorisaties blijven dus geldig.

In het staatsgeheime digitale archiefsysteem heeft iedere medewerker van de afdeling Analyse dezelfde rol: key-user. Een key-user heeft het recht om informatie in het staatsgeheime digitale archiefsysteem toe te voegen, te wijzigen, te raadplegen en te verwijderen. Het toekennen van

de rol key-user aan elke medewerker van Analyse betekent dat binnen Analyse geen differentiatie in toegangsrechten is gerealiseerd. De analist had hierdoor toegang tot alle informatie in het staatsgeheime digitale archiefsysteem.

In het staatsgeheime DMS bepaalt het frontoffice wie toegang heeft tot een zaak. Toegang tot een zaak (en daarmee toegang tot informatie) is mogelijk voor een grote groep gebruikers maar ook voor één of enkele gebruikers.

Net als bij het staatsgeheime digitale archiefsysteem wordt de toegang tot het staatsgeheime DMS door geïnterviewden niet gezien als toegang op basis van 'need to know'. In het staatsgeheime DMS is wel een gedetailleerde structuur van toegangsrechten volgens dat principe mogelijk. Een voorwaarde is dat het gebruik van groepen personen en het koppelen van groepen personen aan zaken beheerst wordt. Dit is nu bewerkelijk en daardoor foutgevoelig. Hierdoor bestaat de mogelijkheid dat meer personen dan bedoeld toegang krijgen tot informatie in een zaak.

Aanvragen van rechten en aanpassing na functieverandering vragen aandacht

We hebben bij een aanvraag voor toegang tot het staatsgeheime digitale archiefsysteem waargenomen dat de aanvraag per mail is gedaan en het daarvoor beschikbare aanvraagformulier niet is gebruikt. Bij de betreffende aanvraag (voor een medewerker binnen de afdeling Analyse) zijn ruimere rechten toegekend dan in de aanvraag vermeld wordt. Aangegeven wordt dat goedkeuring vaak via mail verloopt en niet altijd wordt vastgelegd bij de aanvraag.

Het aanpassen van toegangsrechten als gevolg van verandering van functie van een medewerker vraagt de aandacht. Geïnterviewden geven aan dat toegangsrechten bij verandering van functie niet altijd tijdig en juist worden aangepast.

Het beeld uit interviews dat toegangsrechten bij verandering van functie niet altijd tijdig worden aangepast, sluit aan bij onze waarneming. De autorisaties van de analist voor het staatsgeheime digitale archiefsysteem, het staatsgeheime DMS en afdelingsmappen zijn na verandering van zijn functie in mei 2023, op drie verschillende momenten ingetrokken:

- Het staatsgeheime digitale archiefsysteem - 17-5-2023;
- Het staatsgeheime DMS - 28-7-2023;
- Stg.-net en mappen van afdeling Analyse - 11-8-2023.

Na het intrekken van de toegang tot het staatsgeheime digitale archiefsysteem bleef de analist nog toegang houden tot staatsgeheime informatie via het staatsgeheime DMS en afdelingsmappen.

Er wordt niet periodiek gecontroleerd of de toegangsrechten nog juist zijn

Er is geen actueel controleplan voor de controle van autorisaties met een overzicht van alle te controleren autorisaties.

Er is geen recent overzicht van uitgevoerde controles waaruit blijkt welke controle is uitgevoerd, door wie, wat de uitkomsten zijn en hoe de uitkomsten zijn opgepakt (bijv. intrekken autorisaties).

Uit interviews ontstaat het beeld dat er na 2020 geen controles meer zijn uitgevoerd door de verantwoordelijke leidinggevenden op de autorisatiematrix en de uitgegeven autorisaties.

Wat te doen?
- Ken toegangsrechten toe in het staatsgeheime DMS, het staatsgeheime digitale archiefsysteem en afdelingsmappen volgens het principe 'need to know'.
- Verduidelijk de verantwoordelijkheid voor juiste toegangsrechten.
- Voer periodieke controle van toegangsrechten in.
- Pas toegangsrechten tijdig aan bij verandering van functie.

3.5 Rubricering van informatie

VIRBI 2013
Het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI) beschrijft hoe organisaties om moeten gaan met *Bijzondere informatie*. D.w.z. informatie waarbij na ongeautoriseerde kennisname nadelige gevolgen kunnen optreden voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries.

Het VIRBI hanteert vier niveaus van vertrouwelijkheid:
- Staatsgeheim ZEER GEHEIM (Stg.ZG)
- Staatsgeheim GEHEIM (Stg.G)
- Staatsgeheim CONFIDENTIEEL (Stg.C)
- Departementaal VERTROUWELIJK (Dep.V.)

Rubriceren is het bepalen van het niveau van vertrouwelijkheid op basis van de te verwachten nadelige gevolgen als (een deel van) informatie bekend wordt bij niet geautoriseerden.

Gerubriceerde informatie is informatie waaraan één van de vier niveaus van vertrouwelijkheid is toegekend.

Het NCTV-beleid voor rubriceren is gedateerd en onvolledig, handleidingen zijn in orde
Er is een gedetailleerde beschrijving van hoe het rubriceren bij NCTV behoort te verlopen. Die beschrijving is wel gedateerd (2017) en gaat niet in op de rubricering van informatie in het staatsgeheime DMS en het staatsgeheime digitale archiefsysteem.
Er zijn praktisch bruikbare handleidingen voor het omgaan met staatsgeheime informatie (o.a. de rubriceringskaart uit 2021). Daarin staat informatie voor verschillende vormen van informatie (papier/digitaal), verschillende opslagmedia (applicaties, netwerk, USB-stick) en verschillende rubriceringsniveaus.
De verantwoordelijkheid voor informatiehuishouding (waar juiste rubricering onderdeel van is) is binnen de NCTV belegd bij de afdeling Bedrijfsvoering. Het is de individuele verantwoordelijkheid van de medewerker dat het rubriceren van informatie goed gebeurt. Er zijn wel richtlijnen voor rubricering, er wordt niet getoetst of die richtlijnen worden nageleefd.

Rubricering is vastgelegd in documenten en niet zichtbaar aan de buitenkant
In interviews is aangegeven dat digitale informatie in het staatsgeheime digitale archiefsysteem en het staatsgeheime DMS de rubriceringen Dep V, Stg.C en Stg.G kan hebben. Informatie die is gerubriceerd als Stg.ZG mag niet in het staatsgeheime DMS, het staatsgeheime digitale archiefsysteem of op het Stg.-net worden opgeslagen.

In het staatsgeheime digitale archiefsysteem en in de afdelingsmap van Analyse is rubricering van informatie waargenomen. De in de documenten waargenomen rubricering varieert van ongerubriceerd tot Stg. G.
Er wordt geen aanduiding van de rubricering gebruikt in de naamgeving in het staatsgeheime DMS en het staatsgeheime digitale archiefsysteem of in de metadata van bestanden in het staatsgeheime DMS en het staatsgeheime digitale archiefsysteem. Daardoor is "aan de buitenkant" niet zichtbaar wat de rubricering van informatie in het staatsgeheime DMS en het staatsgeheime digitale archiefsysteem is.

3.6 Verspreiding van staatsgeheime informatie

Er werd veel informatie geprint
Medewerkers kunnen eenvoudig stukken uit het staatsgeheime digitale archiefsysteem halen en die op een eigen of afdelingsschijf zetten en vanaf daar bijvoorbeeld printen. Aangegeven is dat dit waarschijnlijk vaak gebeurt uit praktische overwegingen. Medewerkers vinden het makkelijker om documenten te lezen vanaf hun eigen schijf dan om ze te lezen vanuit het staatsgeheime digitale archiefsysteem. Het is ook mogelijk om stukken uit het staatsgeheime DMS te halen.

Medewerkers van de afdeling Analyse printten veel, dat geldt ook voor de analist. Veel printen werd niet bijzonder gevonden, het printen van staatsgeheime informatie is toegestaan.
Printen werd ook gedaan door medewerkers van de afdeling Analyse voor medewerkers van andere afdelingen die niet in het staatsgeheime digitale archiefsysteem konden. Het is onduidelijk of dit sporadisch voorkwam of structureel was.

Zicht op uitgegeven USB-sticks ontbreekt, het is grotendeels onduidelijk waar ze zijn
Er zijn specifieke werkinstructies voor het gebruik van USB-sticks, incl. een contract bij uitgifte van een USB-stick. Het beheer van USB-sticks is niet beschreven.
Het huidige USB-gebruik door de afdeling Analyse is volgens geïnterviewden beperkt. USB-sticks worden voornamelijk gebruikt voor het overzetten van stukken uit de DWR op de Stg.-omgeving. In het verleden werden USB-sticks vaker gebruikt. Zowel op de DWR-omgeving als op de Stg.-omgeving.
Er zijn volgens de administratie van de NCTV circa 200 oude (d.w.z. niet langer op het Stg.-net bruikbare) USB-sticks in omloop die mogelijk staatsgeheime informatie bevatten.

NCTV geeft aan dat het aantal USB-sticks dat in omloop is, lager is dan de 200 volgens de administratie omdat niet is vastgelegd wanneer USB-sticks zijn ingeleverd of vernietigd. Het is onduidelijk wat er met de uitgegeven USB-sticks is gebeurd, waar deze zich bevinden en welke informatie daarop is opgeslagen.

Volgens de administratie van de NCTV zijn aan de analist 3 USB-sticks en 1 harde schijf uitgegeven.

Uit analyse van de CISO/BVC blijkt dat de analist de USB-sticks niet heeft gebruikt op het Stg.-net tussen 2021 en de zomer van 2023. Er zijn geen logbestanden die informatie bevatten over gebruik van een USB-stick of harde schijf vóór 2021.

Het beeld bij de NCTV (na het bekend worden van de casus) is dat de analist veel stukken op papier mee naar huis nam en ze thuis scande en dan op een gegevensdrager zette.

Schonen gebeurt niet structureel

Kasten, kluizen en persoonlijke schijven worden niet structureel geschoond en bevatten mogelijk staatsgeheime informatie waar geen zicht op is.

Er is in 2021 een schoningsactie geweest om persoonsgegevens te verwijderen. Het ging hierbij om informatie op het reguliere- en het Stg.-net, verschillende informatiesystemen, persoonlijke schijven van medewerkers en persoonlijke mailboxen van medewerkers. De eindstand van de schoningsactie laat zien dat van 7 van de 10 bij de schoning betrokken onderdelen van de NCTV de schoningsactie van 2021 niet hebben afgerond.

Meenemen van staatsgeheime informatie mag niet, tenzij

Het is voor medewerkers duidelijk dat ze geen als Staatsgeheim gerubriceerde stukken mee naar buiten mogen nemen. Het beleid over rubriceren geeft aan: *"Indien het noodzakelijk is bijzondere informatie buiten de rijksdienst te brengen, anders dan op grond van een wettelijke verplichting tot openbaarmaking, wordt dit alleen gedaan nadat de NCTV hiervoor toestemming heeft verleend."* Het is in de praktijk wel eenvoudig om bijv. geprinte documenten mee naar buiten te nemen.

Wat te doen?

Grip krijgen op verspreiding van staatsgeheime informatie door:

- het beperken van het printen van informatie;
- het verbeteren van het beheer van USB-sticks;
- rubricering op te nemen in de naamgeving van bestanden zodat direct zichtbaar is dat het gaat om staatsgeheime informatie;
- het periodiek schonen van kasten, kluizen en persoonlijke schijven.

3.7 Veiligheidsonderzoek van de gebruikers van informatie

A-, B- en C-veiligheidsonderzoek

Als personen toegang hebben tot staatsgeheime informatie is sprake van een *vertrouwensfunctie*. Vertrouwensfuncties worden aangewezen op niveau A, B of C waarbij A de zwaarste categorie is.

Voor het vervullen van een vertrouwensfunctie is een *verklaring van geen bezwaar (VGB)* nodig. De VGB (VGB-A, VGB-B of VGB-C, afhankelijk van het niveau van de vertrouwensfunctie) wordt na het uitvoeren van een *veiligheidsonderzoek* afgegeven door de AIVD.

Een VGB verliest, conform beleid AIVD en de Wet veiligheidsonderzoeken, haar geldigheid niet.

Het ministerie van JenV heeft in 2017 bepaald dat een herhaalonderzoek voor VGB-A, -B en -C elke vijf jaar moet plaatsvinden.

Iedere NCTV-medewerker moet een VGB hebben, voor analisten van Analyse is een VGB-A vereist

De NCTV heeft bepaald dat iedere NCTV-medewerker in het bezit moet zijn van een actuele VGB om werkzaamheden uit te mogen voeren. Dit is in beleid uit 2017 vastgelegd.

Tot 2019 was een VGB-B voldoende. In 2019 is binnen de NCTV de hoogte van het veiligheidsonderzoek per functie opnieuw bepaald. Analisten van de afdeling Analyse moesten vanaf dat moment een VGB-A hebben. Dat is in onze ogen een passende eis gezien de toegang tot alle staatsgeheime informatie in het

staatsgeheime digitale archiefsysteem die alle analisten van de afdeling Analyse hebben.

Keuze voor VGB-A leidt niet direct tot herhaalonderzoek, volgens de BVA een onjuiste keuze

Voor analisten van de afdeling Analyse die op dat moment een VGB-B hadden, is niet direct een herhaalonderzoek uitgevoerd. Op het moment dat een herhaalonderzoek nodig is, wordt een VGB-A aangevraagd. Tot die tijd mag er volgens de NCTV met een VGB-B gewerkt worden. Volgens de BVA beschikken analisten van de afdeling Analyse met een VGB-B vanaf 2019 daardoor niet over een rechtsgeldige VGB.

De analist was in bezit van een VGB-B sinds 8 maart 2018. Daarna heeft geen herhaalonderzoek plaatsgevonden. Vanwege de ophoging van het niveau van de vertrouwensfunctie voor de medewerkers van de afdeling Analyse beschikt de analist volgens de BVA vanaf 2019 niet over een rechtsgeldige VGB.

De NCTV heeft ervoor gekozen herhaalonderzoeken uit te stellen. Deze keuze is niet voorgelegd aan de BVA.

Uit verslagen van MT-vergaderingen van de NCTV uit 2023 blijkt dat er in 2023 bij de AIVD beperkte capaciteit was voor het uitvoeren van veiligheidsonderzoeken. In juni 2023 is meerdere keren in het MT van de NCTV besproken hoe hiermee moest worden omgegaan vanwege de gevolgen voor werving en selectie en herhaalonderzoeken.

In het MT van 20 december 2023 wordt vastgesteld dat de doorlooptijd voor veiligheidsonderzoeken sinds september weer is genormaliseerd en dat door de CISO/BVC de herhaalonderzoeken weer moeten worden opgestart. De herhaalonderzoeken hebben daarvoor tijdelijk stilgelegen, omdat VGB's voor nieuwe medewerkers prioriteit kregen. Wij hebben geen formeel besluit gezien van het MT-NCTV om herhaalonderzoeken tijdelijk op te schorten. Het is onduidelijk door wie dit besluit is genomen.

De NCTV heeft de keuze om herhaalonderzoeken uit te stellen niet voorgelegd aan de BVA. De NCTV en de BVA hebben geen eenduidig beeld of deze afstemming had moeten plaatsvinden. Volgens de BVA moeten uitzonderingen op de beleidslijn worden afgestemd met de BVA.

De CISO/BVC ziet toe op de veiligheidsonderzoeken en houdt bij of iedere medewerker in het bezit is van een actuele VGB. Er is geen geautomatiseerd proces voor. Er komt geen melding uit een van de systemen op het moment dat een VGB vijf jaar of langer geleden is afgegeven. Managers geven aan geen zicht te hebben op het verstrijken van de door het ministerie van JenV bepaalde termijn van vijf jaar van VGB's binnen hun afdeling/team.

Uit waarnemingen blijkt dat er op de peildatums 1-10-2023 en 18-3-2024 resp. 41 en 48 medewerkers van de NCTV een VGB hadden die ouder was dan vijf jaar, terwijl VGB's volgens het beleid van JenV maximaal vijf jaar oud mogen zijn. Op een totaal van 533 medewerkers waarvoor een VGB van toepassing is, had resp. 7,7% (1-10-2023) en 9% (18-3-2024) een VGB ouder dan vijf jaar.

Wat te doen?

Bepaal of de achterstand in herhaalonderzoeken moet leiden tot acties. Bijvoorbeeld:

- Tijdelijk toegang tot staatsgeheime informatie beperken als een VGB ouder is dan vijf jaar.

- Voorrang geven aan medewerkers met bepaalde functies.

3.8 Logging en monitoring

Wat is logging en monitoring?
Om informatie te beveiligen is het noodzakelijk een logboek bij te houden van alle gebeurtenissen die van invloed kunnen zijn op de betrouwbaarheid van informatie. Het gaat hierbij om de vastlegging van activiteiten van gebruikers van informatie (raadplegen, bewerken, afdrukken, downloaden), beheer van toegangsrechten, activiteiten van beheerders van systemen en netwerken, de werking van systemen, de koppeling tussen systemen, het gebruik van USB-sticks etc.
Het logboek moet beveiligd worden tegen vervalsing en onbevoegde toegang.
Geregistreerde gebeurtenissen moeten (periodiek) geanalyseerd worden om na te gaan of er gebeurtenissen zijn opgetreden die schade (kunnen) veroorzaken.

De vastlegging van gebeurtenissen en de analyse van deze gebeurtenissen worden aangeduid met *Logging en monitoring*.

Actueel en op risicoanalyse gebaseerd beleid voor logging en monitoring ontbreekt
Er is beleid uit 2015 en 2017 waarin logging en monitoring zijn uitgewerkt voor enkele onderdelen van de informatieverwerking binnen de NCTV:

- Logging en monitoring zijn uitgewerkt voor de bewaking van de beschikbaarheid van het Stg.-net (2015).
- Logging is uitgewerkt voor de verzending van staatsgeheime informatie op papier (2017).

Er ontbreekt een actueel, NCTV-breed beleid voor logging en monitoring dat gebaseerd is op een risicoanalyse waarin ook insider threat is meegenomen. In dat NCTV-brede beleid voor logging kan verder uitgewerkt worden op welke systemen wordt gelogd, welke handelingen worden gelogd en welke gedragingen en gebeurtenissen worden gemonitord met als doel inbreuken op beveiliging te detecteren en onderzoek naar inbreuken te kunnen doen.

Handelingen m.b.t. staatsgeheime informatie worden gelogd; er is variatie in detaillering en bewaring
Hoewel beleid ontbreekt, worden handelingen m.b.t. staatsgeheime informatie in applicaties (het staatsgeheime digitale archiefsysteem, het staatsgeheime DMS) en mappen wel gelogd. Ook het printen van stukken en het gebruik van USB-sticks worden gelogd.
Er is variatie in de vastgelegde details per gebeurtenis, de bewaartermijn van loggegevens en de locatie waar loggegevens wordt verzameld. Bij de verdere uitwerking van het beleid voor logging en monitoring vraagt dit de aandacht omdat die variatie de bruikbaarheid van loggegevens kan beperken.

Er zijn faciliteiten om logging te analyseren en opvallende gebeurtenissen te signaleren
Beheerders bij de NCTV beschikken over een logging- en monitoringssysteem dat de mogelijkheid biedt om signaleringen in te stellen bij o.a. activiteiten van beheerders en gebruikers. Daardoor kunnen opvallende gebeurtenissen worden gedetecteerd. Bijvoorbeeld dat een gebruiker vijf foute inlogpogingen doet binnen vijf minuten.
De documentatie over het logging- en monitoringssysteem dateert van 2022. De documentatie beschrijft mogelijke

signaleringen bij o.a. activiteiten van beheerders en gebruikers. Geïnterviewden hebben geen eenduidig beeld welke signaleringen daadwerkelijk zijn ingericht binnen het logging- en monitoringssysteem.
Met het logging- en monitoringssysteem kunnen rapportages worden gemaakt over o.a. gebruik van het staatsgeheime DMS en het staatsgeheime digitale archiefsysteem waardoor inzichtelijk wordt welke gebruiker welke documenten heeft toegevoegd, ingezien, aangepast of verwijderd.

Aanwezige faciliteiten worden niet gebruikt, er zijn wel ontwikkelingen in gang gezet

De informatie die beschikbaar komt op basis van de (in het logging- en monitoringssysteem) ingerichte signaleringen, wordt niet geanalyseerd:

- De analyse van de logging van autorisaties is gestopt in 2020. Er is nooit een vraag uit het MT gekomen n.a.v. rapportages over monitoring.
- Er is onvoldoende gemonitord op de signaleringen die met het logging- en monitoringssysteem zijn ingericht. Aangegeven is dat er vanaf 2022 vrijwel geen tijd was om naar de signaleringen kijken.

Recent is een nieuwe versie van de handleiding van het logging- en monitoringssysteem opgesteld. In de handleiding zijn alle beschikbare faciliteiten voor monitoring uitgewerkt. Wij zien in de nieuwe handleiding geen koppeling tussen dreigingen die de NCTV ziet, signaleringen die daarom moeten worden ingericht en monitoring die plaats moet vinden.

Wat te doen?
De NCTV heeft met het logging- en monitoringssysteem een instrument in huis om gebeurtenissen binnen de systemen, activiteiten van beheerders en activiteiten van gebruikers te monitoren.
De NCTV heeft nog niet bepaald welk gedrag van medewerkers en welke gebeurtenissen moeten worden geregistreerd en gedetecteerd. In onze ogen is het de verantwoordelijkheid van het MT van de NCTV om op risicoanalyse gebaseerde keuzes te maken en uit te leggen aan medewerkers welk gedrag van beheerders en gebruikers wordt geregistreerd en hoe daarover wordt gerapporteerd.

3.9 Behandeling van inbreuken op de beveiliging

Het VIRBI over inbreuken op beveiliging
Het VIRBI schrijft o.a. de volgende stappen voor bij compromittering d.w.z. kennisname dan wel mogelijkheid tot kennisname van bijzondere informatie door niet-geautoriseerden:

- Elke ambtenaar is verplicht de Beveiligingsambtenaar (BVA) onmiddellijk mededeling te doen van een inbreuk op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromittering van bijzondere informatie.
- De BVA onderzoekt of compromittering van bijzondere informatie heeft plaatsgevonden; indien dit het geval is doet hij hiervan mededeling aan de secretaris-generaal en adviseert over de noodzaak tot het instellen van een commissie van onderzoek.
- Een commissie van onderzoek wordt ingesteld door de secretaris-generaal.

In het beleid voor het melden van mogelijke inbreuken op de beveiliging ontbreken onderdelen

Er is beleid uit 2016 en 2019 voor het melden van mogelijke inbreuken op beveiliging van informatie. In dat beleid worden verschillende aspecten van het melden uitgewerkt: bij wie kan worden gemeld, hoe kan worden gemeld, welke stappen worden gevolgd, hoe wordt geregistreerd.
Uit de verschillende documenten blijkt dat er gemeld kan worden bij de lijnmanager of de BVC. De BVC ondersteunt bij het oppakken van een melding.

Voor de volgende aspecten is een verdere uitwerking nodig:

- De bescherming van de persoonsgegevens van de melder van mogelijke inbreuken en personen op wie de melding betrekking heeft;
- De bescherming van de melder tegen juridische procedures en benadeling;
- Hoe medewerkers anoniem kunnen melden.

Volgens de *Procedure beveiligingsincidenten* (2016) stelt de BVC maandelijks een rapportage op van alle incidenten voor de bestuurder en de BVA. In de praktijk wordt de opzet niet altijd uitgevoerd. Er zijn geen maandelijkse incident-rapportages aangetroffen. Sinds 2021 wordt er bij de NCTV niet meer gerapporteerd over incidenten.

Het is onduidelijk hoe incidenten worden meegenomen in risicoanalyses

In de beschikbare documentatie zijn procedures opgenomen m.b.t. het registreren en afhandelen van incidenten. Voor de afhandeling van grote incidenten wordt ook verwezen naar de JenV-brede incidentenprocedures.

Escalatielijnen voor grote incidenten zijn beschreven. Er is niet uitgewerkt hoe wordt bepaald of een incident moet leiden tot uitvoeren of bijstellen van de risicoanalyse van de NCTV of JenV.

De BVA adviseert en voert geen eigen onderzoek uit

In het geval van de casus heeft de BVA geen eigen onderzoek uitgevoerd. De keuze hiervoor is in overleg met de pSG van JenV gemaakt omdat er al onderzoeken lopen door de CTIVD, door de ADR en door het OM. De BVA is als adviseur van de opdrachtgever betrokken geweest bij de opdracht voor het onderzoek door de ADR. De BVA voert wel onderzoek uit voor de accreditatie van de systemen voor het gebruik van staatsgeheime informatie.

Wat te doen?

- Actualiseer het beleid voor het melden van inbreuken op beveiliging.
- Neem controle/bijstelling van de risicoanalyse op als stap in de afhandeling van grote incidenten.
- Besluit over het opnieuw introduceren van periodieke incidentrapportages aan het MT NCTV.

3.10 Aandacht van het management door controle en toezicht

Het toezicht op de beveiliging van staatsgeheime informatie is niet volledig ingericht

In beleidsstukken zijn de rollen, taken en verantwoordelijkheden in het toezicht van o.a. de BVC, de CISO en de CIO vastgelegd. Binnen de NCTV is er geen plan voor het toezicht op de beveiliging van staatsgeheime informatie en het voldoen aan het VIRBI. Het is niet duidelijk hoe vaak er toezicht gehouden moet

worden, in welke vorm toezicht wordt uitgevoerd en met welke intensiteit. Uit opgeleverde documentatie en interviews blijkt dat de CISO/BVC toezicht heeft gehouden door het uitvoeren van controles. De CIO ziet voor zichzelf geen functie in het toezicht.

De uitvoering van toezicht is niet vastgesteld en de opvolging is niet bepaald

Er is geen documentatie aangetroffen waaruit blijkt dat het management van de NCTV in de periode 2021-2023 de uitvoering van het toezicht op de beveiliging van staatsgeheime informatie vaststelde en de opvolging bepaalde.
Geïnterviewden en geanalyseerde documentatie geven het beeld dat er bij de NCTV geen werkende PDCA-cyclus Informatiebeveiliging is waarin uitkomsten van uitgevoerde controles (indien nodig) leiden tot herziening van de risicoanalyse en aanscherping van maatregelen.

Het management had weinig aandacht voor toezicht, geïnterviewden zien aandacht toenemen

Uit de interviews blijkt dat het management zich niet actief bezighield met toezicht. Meerdere geïnterviewden geven aan dat er binnen de NCTV geruime tijd te weinig aandacht is gegeven aan informatiebeveiliging, terwijl de dreigingen zijn toegenomen. Het MT had geen signalen dat er zaken rondom NL-net en de omgang met staatsgeheime informatie niet op orde waren. Het beeld is dat MT-leden en afdelingshoofden binnen de NCTV uitgingen van 'geen nieuws is goed nieuws' en niet actief inzetten op toezicht.

NCTV en Nationaal Coördinator
De NCTV en het hoofd van de NCTV hebben dezelfde naam. Om deze van elkaar te kunnen onderscheiden, verwijzen wij in dit rapport met de benaming 'Nationaal Coördinator' naar het hoofd van de NCTV.

Geïnterviewden zien dat er onder de huidige Nationaal Coördinator meer aandacht is voor informatiebeveiliging dan een aantal jaren geleden.

Wat te doen?
- Stel opnieuw vast wie welke taken heeft in het toezicht.
- Stel jaarlijks een toezichtplan op dat in het MT NCTV wordt vastgesteld.
- Bespreek jaarlijks de resultaten van het toezicht in het MT NCTV.

4. Beveiliging van vertrouwelijke informatie bij de politie

4.1 Risicomanagement

De politie heeft een bruikbare maar gedateerde beschrijving van het proces risicomanagement waarin onderdelen ontbreken

In *Risicomanagement Informatievoorziening* (2015) is het proces risicomanagement beschreven. Risicosessies hebben een jaarlijkse frequentie, er zijn richtlijnen voor classificatie van risico's, de taken en verantwoordelijkheden van o.a. de directie IV, de dienst IM en de dienst ICT zijn uitgewerkt en het risicoregister wordt beschreven. De onderdelen monitoren en bewaken zijn eveneens uitgewerkt in het beleid.

Een aantal onderdelen van risicomanagement ontbreekt in de procesbeschrijving: aandacht voor insider threat, dreigingen door statelijke actoren of georganiseerde misdaad, de relatie tussen risicoanalyse en te hanteren niveaus van vertrouwelijkheid van informatie, de vertaling van risico's naar te treffen maatregelen en de vaststelling van risicoanalyses.

Geïnterviewden hebben geen eenduidig beeld welke risicoanalyses binnen de politie worden uitgevoerd

Het is bij het geïnterviewde lid van de korpsleiding (hierna: lid korpsleiding) niet bekend of een strategische risicoanalyse is uitgevoerd op de politie-omgevingen met hoge vertrouwelijkheidseisen.

Er is volgens de concern security officer te weinig zicht op de dreigingen die op de politie van toepassing zijn: ondermijning, criminele organisaties, statelijke actoren. Dit beeld komt niet overeen met aan ons aangeleverde informatie. Die laat zien dat de politie zelf en samen met de AIVD een dreigingsanalyse en dreigingsbeeld heeft opgesteld. Ook stelt de politie op basis van andere bronnen rapportages op over dreigingen.

CTER

Het cluster Contraterrorisme, Extremisme en Radicalisering (CTER) is in 2017 opgericht door de politie om informatie-uitwisseling en samenwerking op het gebied van contraterrorisme, extremisme en radicalisering te versterken tussen drie onderdelen van de Landelijke Eenheid: Dienst Landelijke Recherche, Dienst Landelijke Informatieorganisatie en Dienst Specialistische Operaties.

Recent is een reorganisatie uitgevoerd waarbij de Landelijke eenheid is opgesplitst in de eenheid Landelijke Opsporing en Interventies en de eenheid Landelijke Expertise en Operaties.

Het cluster CTER valt nu onder de eenheid Landelijke Opsporing en Interventies. Het cluster CTER bestaat momenteel uit drie integrale teams waarin tactiek, informatie en expertise gecombineerd zijn.

Voor CTER ontbreekt een actuele risicoanalyse die ingaat op de beveiliging van vertrouwelijke informatie

Een directe relatie tussen de dreigingsanalyses die de politie uitvoert en de beveiliging van vertrouwelijke informatie bij CTER ontbreekt. Wij hebben geen actuele, door het management van CTER goedgekeurde risicoanalyse aangetroffen waarin wordt

ingegaan op de risico's rondom de verwerking van vertrouwelijke informatie binnen CTER en te nemen beveiligingsmaatregelen. Voor CTER is geen risicoanalyse uitgevoerd waarin o.a. insider threats zijn geanalyseerd. Dat wordt bevestigd door geïnterviewden.

Er zijn n.a.v. een dreigingsanalyse binnen CTER wel maatregelen getroffen. In bepaalde ruimtes is het niet toegestaan telefoons, laptops, etc. mee te nemen en er zijn voorzieningen om het afluisteren van telefoons tegen te gaan (ruiskasten) en de beveiliging van de locatie is verbeterd.

Wat te doen
- Communiceer over alle initiatieven op het gebied van risicoanalyse en deel de uitkomsten van analyses.
- Actualiseer de beschrijving van het proces Risicomanagement Informatievoorziening.
- Voer binnen CTER periodiek een risicoanalyse uit rekening houdend met dreiging vanuit statelijke actoren en criminele organisaties en insider threat.

4.2 Beleid voor informatiebeveiliging

Het beveiligingsbeleid van de politie uit 2018 is nog grotendeels bruikbaar

De politie heeft een *Strategisch Beleidskader Integrale Beveiliging* dat is opgesteld in 2018. Dit beleid gaat in op o.a. de geldende kaders, rollen, het toezicht, risicomanagement, de PDCA-cyclus en bewustwording. Volgens het beleidskader moet het beleid iedere vier jaar geëvalueerd worden. Dat is niet gebeurd. Als oorzaak wordt het ontbreken van de CISO genoemd. Deze is volgens betrokkenen verantwoordelijk voor het IB-beleid, maar de rol was lange tijd niet belegd.
In het beleid missen wij de positionering van de BIO en maatregelen die aanvullend op de BIO zijn bepaald voor vertrouwelijke informatie (Is de BIO verplicht of niet verplicht? Geldt de BIO uitsluitend voor centraal beheer beheerde IT-voorzieningen of voor alle IT-voorzieningen?).

Voor CTER is het beleid voor (informatie)beveiliging niet uitgewerkt in concrete afspraken

Ons valt op dat er voor CTER geen afspraken zijn over de verdere invulling van het (informatie)beveiligingsbeleid. Relevante onderwerpen om afspraken over te maken, zijn de door CTER zelf beheerde applicaties, controle en toezicht.

Beveiligingsbeleid wordt niet bijgesteld n.a.v. uitgevoerde controles, signalen of onderzoeken; de Act van de PDCA-cyclus ontbreekt

Er is geen documentatie aangetroffen over de manier waarop het (informatie)beveiligingsbeleid wordt aangepast n.a.v. uitgevoerde controles, signalen of onderzoeken.
Aangegeven is dat er te weinig sprake is van terugkoppeling uit de organisatie over de implementatie van het opgestelde beleid en dat de fase Check dus ontbreekt in de politieorganisatie. Ook is in interviews door meerdere functionarissen aangegeven dat de fase Act in de PDCA-cyclus onvoldoende is in gericht.

Wat te doen
- Maak afspraken over de beveiliging van de door CTER zelf beheerde applicaties, controle en toezicht.
- We bevelen de organisatie nadrukkelijk niet aan om de focus te leggen op het bijstellen van het gehele IB-beleid.

De fasen Do, Check en Act vragen wat ons betreft op dit moment meer aandacht.

4.3 Selectie en inrichting van maatregelen

De politie beschikt over een actuele, op de BIO gebaseerde baseline die ook maatregelen bevat voor gerubriceerde informatie
De politie gebruikt de BIO als basis voor informatiebeveiligings-maatregelen. Aanvullend heeft de politie een *Addendum BIO Politie-specifieke maatregelen* (2022) (hierna addendum op de BIO). Het addendum op de BIO beschrijft per BIO-maatregel welke aanvullende maatregelen van toepassing zijn voor informatie die is gerubriceerd als Politie Intern, Politie Confidentieel, Politie Geheim of Politie Zeer Geheim.

De BIO plus het addendum op de BIO vormen voor de politie de baseline die van toepassing is voor de hele politieorganisatie. CTER gebruikt de rubriceringsregeling niet, dus het addendum op de BIO is hier niet van toepassing. Er zijn geen aanvullingen op de BIO voor politieomgevingen met hoge vertrouwelijkheidseisen die de rubriceringsregeling niet toepassen (zoals CTER).

De politie voert de BIO in, het tijdspad voor CTER is niet duidelijk
In 2020 heeft de politie besloten een BIO-implementatietraject op te starten. Het traject is gestart bij het Politie Dienstencentrum (PDC), dat de meerderheid van de door de politie gebruikte systemen en applicaties beheert. De implementatie binnen het PDC loopt nog. De CISO heeft aangegeven dat de implementatie van de BIO binnen het PDC in 2024 afgerond moet zijn.

Binnen CTER zijn de BIO en het addendum op de BIO nog niet ingevoerd. De door CTER zelf beheerde applicaties vallen niet onder het traject dat loopt binnen het PDC. Ook is er niet gestart met de door CTER zelf in te voeren maatregelen, bijvoorbeeld rondom autorisatiebeheer. Het is onduidelijk wat het tijdspad is voor de invoering van de baseline binnen CTER.

Uit onderzoek van Concern Audit blijkt dat BIO-maatregelen binnen het PDC deels zijn geïmplementeerd
In 2023 heeft Concern Audit, de interne auditorganisatie van de politie, onderzoeken uitgevoerd naar de invoering van BIO-maatregelen binnen twee onderdelen van het PDC; Dienst ICT Infrabedrijf en de sector Dienstverlening partners. De uitkomsten van de twee onderzoeken zijn als volgt:

- Bij de Dienst ICT Infrabedrijf blijkt dat van negen productielijnen de meeste niet klaar zijn om een audit uit te laten voeren, mede door gebrek aan tijd/prioriteit.
- Binnen de sector Dienstverlening partners zijn 24 onderzochte beheersmaatregelen verdeeld over acht hoofdstukken van de BIO grotendeels ingericht (opzet en bestaan), de borging is onvoldoende ingevuld.

De werking van de ingerichte BIO-maatregelen heeft Concern Audit niet vast kunnen stellen.

Uit het onderzoek door Concern Audit blijkt niet op welke manier invulling wordt gegeven aan de maatregelen die zijn bepaald in het addendum op de BIO. Het addendum op de BIO is door Concern Audit buiten beschouwing gelaten.

Het functioneren van de getroffen beveiligingsmaatregelen wordt beperkt gemonitord; er is geen controle of de getroffen maatregelen werken
Informatiebeveiliging staat in de periode 2021 t/m 2024 ieder jaar op het auditjaarplan van Concern Audit. Elk jaar worden

andere thema's onderzocht. De onderwerpen rubricering en de omgang met gerubriceerde informatie zijn geen onderwerp van onderzoek in de auditjaarplannen van Concern Audit. Ook zijn er geen audits bij CTER uitgevoerd. Wel staat er in de jaarplannen voor 2023 en 2024 een onderzoek binnen CTER op de lijst, maar met een lage prioriteit. Dat betekent in de praktijk dat deze audit niet wordt uitgevoerd.
Het toezicht op informatiebeveiliging binnen CTER is de verantwoordelijkheid van de CTER-leiding. Er zijn geen resultaten van dit toezicht aangetroffen

De voorwaarden voor succesvolle invoering van een baseline ontbreken
Volgens betrokkenen is de fase Check in de PDCA-cyclus binnen de politie nog niet volledig ingevuld. Er worden wel kaders en richtlijnen opgesteld, maar er komt geen terugkoppeling vanuit de organisatie over de implementatie. Ook is aangegeven dat het onzeker is of het beeld dat uit de uitgevoerde audits blijkt, sluitend is. Tot slot is benoemd dat de politie alles op alles zet om politiezaken op te lossen onder hoge tijdsdruk en dat dit in sommige gevallen ten koste gaat van compliance. In deze context is het onzeker of de baseline succesvol ingevoerd kan worden binnen de hele politie.

Wat te doen
- Maak een realistisch tijdspad voor de invoering ven de baseline.
- Richt de terugkoppeling in vanuit de organisatie over de implementatie.
- Wacht binnen CTER niet op het centrale traject om de baseline in te voeren. Start op basis van de uitkomsten van intern onderzoek n.a.v. de casus en het onderzoek door de ADR met het treffen van maatregelen uit de baseline.

4.4 Beheersing van toegang

Informatiesystemen bij CTER in scope van het onderzoek

Summ-IT
Summ-IT is het opsporingssysteem van de politie. Het systeem ondersteunt het gehele opsporingsproces vanaf een aangifte of signaal tot aan de oplevering van het procesdossier dat naar het Openbaar Ministerie gaat. In Summ-IT wordt per onderzoek een zaak (synoniem voor dossier) aangemaakt waarin de opsporingsinformatie van het betreffende onderzoek wordt vastgelegd.

Het tapsysteem
Het tapsysteem dat de politie gebruikt voor de verwerking van telefoontaps. In het tapsysteem kunnen rechercheurs en tolken de audio van tapgesprekken beluisteren en kunnen tolken een vertaling vastleggen.

Het opnamesysteem
De politie kan met apparatuur op afstand gesprekken afluisteren.

Het autorisatiebeleid gaat in op relevante onderwerpen maar is wat gedateerd; Controle en toezicht zijn onderbelicht

Het autorisatiebeleid (voor politiemedewerkers en externen) en de beschrijving van het proces Identity & Access Management (IAM) zijn opgesteld in 2017. Veel relevante onderwerpen vinden we terug in het beleid, zoals de uitwerking van het principe 'need to know', mandaten rondom autorisaties en het proces van toekennen van autorisaties en omgaan met extern personeel. Wel zijn de beschrijvingen van organisatieonderdelen, taken, verantwoordelijkheden en bevoegdheden toe aan een update. We missen in het autorisatiebeleid de uitwerking van controle en toezicht. Het is niet duidelijk wie controles uitvoert op uitgegeven toegangsrechten en wie eindverantwoordelijk is voor de periodieke controle.

Er is geen CTER-specifiek autorisatiebeleid aangetroffen. Wel blijkt uit interviews binnen CTER dat er in de praktijk autorisatiebeleid is rondom het verstrekken van toegang tot zaken in Summ-IT:

- De toegang tot Summ-IT is in principe alleen voor politiepersoneel, maar uitzonderingen zijn mogelijk.
- Tolken hebben een basispolitieaccount met beperkte mogelijkheden en in principe geen toegang tot Summ-IT.
- Medewerkers van team Tactiek hebben toegang tot Wet politiegegevens (Wpg) art. 8 en 9 informatie. Medewerkers van [redacted] hebben daarbovenop nog toegang tot Wpg art. 10 informatie.

Eigen beheerde omgeving

CTER maakt gebruik van informatiesystemen die centraal worden beheerd en informatiesystemen die binnen de eigen eenheid worden beheerd. Binnen de politie wordt de laatste categorie aangeduid als Eigen beheerde omgeving. Het opnamesysteem is zo'n Eigen beheerde omgeving.

Op een Eigen beheerde omgeving zijn het centrale beleid (voor o.a. autorisaties, logging en monitoring) en centraal ingerichte beveiligingsmaatregelen niet zonder meer van toepassing.

Voor CTER betekent dat o.a. dat het toekennen van toegangsrechten en de invoering van de baseline voor elke Eigen beheerde omgeving afzonderlijk geregeld moet worden.

Er zijn autorisatieprofielen voor het geautomatiseerd toekennen van toegangsrechten

Het IAM-proces hanteert autorisatieprofielen. Een autorisatieprofiel is een uitwerking van het autorisatiebeleid waarmee geautomatiseerd toegangsrechten kunnen worden toegekend die horen bij een bepaalde rol. Een autorisatieprofiel bepaalt tot welke applicaties een medewerker toegang krijgt. Autorisatieprofielen zijn ook van toepassing voor medewerkers van CTER. Een autorisatieprofiel specificeert niet welke rechten een medewerker heeft binnen een applicatie.
De verantwoordelijkheid voor het toekennen en intrekken van autorisaties ligt binnen CTER bij de teamleider van een onderzoek.

Toegang volgens het principe 'need to know' is mogelijk in Summ-IT maar wordt niet toegepast

Summ-IT biedt de mogelijkheid om fijnmazig toegang te verlenen tot informatie door binnen een zaak onderscheid te maken in verschillende autorisatieniveaus. Tolken hebben - in principe - geen toegang tot Summ-IT.

Uit meerdere interviews blijkt dat voor CTER-onderzoeken in Summ-IT een groot aantal personen geautoriseerd is. Wij hebben van drie onderzoeken van CTER waargenomen dat resp. 95, 114 en 170 personen toegang hebben. Bovendien kan een groot deel van de geautoriseerde personen zelf weer anderen toegang verlenen tot een zaak. Binnen de door ons bekeken onderzoeken waren er voor ieder onderzoek 35-45 personen gemachtigd om anderen te autoriseren. De autorisaties van medewerkers die op tijdelijke basis toegang nodig hebben tot een zaak in Summ-IT blijven in veel gevallen bestaan. Eenmaal uitgegeven autorisaties tot een zaak worden niet ingetrokken en blijven geldig zolang een Summ-IT-account actief is.

Ons beeld is dat hiermee geen invulling gegeven wordt aan het principe 'need to know' en dat de toegang tot onderzoeken in Summ-IT onvoldoende beheersbaar is als zoveel personen gemachtigd zijn om anderen toegang te geven.

Toegang tot het tapsysteem gebeurt op basis van 'need to know'; er is een beperkt aantal tolken gekoppeld aan een onderzoek

In het tapsysteem bestaat de mogelijkheid om fijnmazig toegang te verlenen door de toegang tot een onderzoek verder te beperken tot specifieke taplijnen binnen een onderzoek. Dit wordt bepaald door de teamleider

We hebben vier onderzoeken geselecteerd van verschillende omvang en gezien welke medewerkers in het onderzoek gekoppeld zijn aan het tapsysteem. Aan het grootste onderzoek zijn dertien tolken gekoppeld. Het aantal tolken dat toegang heeft tot een onderzoek in het tapsysteem is beperkt en daarmee goed beheersbaar.

Teamleiders hebben geen inzicht in de autorisaties in het tapsysteem, maar kunnen op verzoek wel een overzicht ontvangen van de beheerders van het tapsysteem.

Bij het opnamesysteem is geen toegang op basis van 'need to know' mogelijk

Voor het opnamesysteem is geen toegang op basis van 'need to know' ingericht.

Tolken die binnen CTER werkzaam zijn, hebben geen toegang tot het opnamesysteem. Zij krijgen toegang tot het opnamesysteem via het account van rechercheurs. Dit wordt in paragraaf 4.5 Rubricering van informatie verder toegelicht.

Volgens het huidige beleid hebben tolken geen toegang tot politiesystemen. In interviews bij CTER wordt dit bevestigd: tolken hebben geen Summ-IT-account. Tolken hebben een basis politieaccount met beperkte mogelijkheden, d.w.z. toegang tot de kantoorautomatisering (outlook, tekstverwerking) en het tapsysteem.

Bij een waarneming van Summ-IT zagen wij accounts in Summ-IT op naam van de tolk. N.a.v. deze waarneming heeft de politie een analyse uitgevoerd. Daaruit blijkt het volgende:

- De tolk heeft zowel een regulier politieaccount als een basis politieaccount.

- Het reguliere politieaccount heeft volgens de politie geen autorisatie voor systemen waarin politie-informatie is opgeslagen.
- Het basis politieaccount heeft volgens de politie de gebruikelijke autorisaties voor tolken en vertalers.
- Beide accounts zijn volgens de politie in de twaalf maanden voorafgaand aan de peildatum niet gebruikt.
- De tolk heeft in Summ-IT een account dat gekoppeld is aan twee zaken van de eenheid Haaglanden. Deze zaken zijn meer dan tien jaar geleden opgestart. Volgens de politie is er operationeel op deze onderzoeken al lang geen actieve inzet gepleegd, maar staan de zaken nog wel open in Summ-IT.
- [redacted]

Er is geen periodieke controle van uitgegeven toegangsrechten

CTER beschikt niet over een overzicht van alle binnen CTER gebruikte informatiesystemen en bijbehorende uitgegeven autorisaties. Dit maakt het controleren van autorisaties lastig.

Zowel de teamchef als diverse medewerkers binnen CTER geven aan dat er geen controles plaatsvinden op toegekende autorisaties. Het is voor de medewerkers niet duidelijk wie verantwoordelijk is voor de controles. Er is geen plan aangetroffen voor de controle van autorisaties met een volledig overzicht van alle te controleren autorisaties. Ook zijn er geen resultaten aangetroffen van uitgevoerde controles van de autorisatiematrix en uitgegeven toegangsrechten.

Controle van de via IAM uitgegeven autorisaties is niet structureel ingericht. Het is wel mogelijk rapportages uit IAM te halen die als basis voor de controle van autorisaties zouden kunnen dienen. Een geïnterviewde medewerker van CTER controleert op eigen initiatief de autorisaties in diens zaken in Summ-IT, maar geeft aan dat de controle lastig is omdat niet alleen medewerkers die direct aan een zaak werken autorisaties hebben. Ook meerdere medewerkers van andere afdelingen hebben toegang. Er is niet altijd zicht op wie deze mensen zijn en of ze de autorisatie nodig hebben.

De functioneel beheerder van het tapsysteem geeft aan periodiek te controleren of een account nog actief gebruikt wordt.

Wat te doen?

- Beperk het aantal personen per zaak in Summ-IT dat gemachtigd is om anderen toegang te geven tot de zaak.
- Controleer periodiek de toegang tot een zaak en trek overbodige toegangsrechten in.
- Onderzoek de mogelijkheid om tijdelijk rechten toe te kennen in Summ-IT die automatisch vervallen.

4.5 Rubricering van informatie

De politie hanteert verschillende termen om vertrouwelijkheid aan te geven

De politie heeft verschillende manieren om vertrouwelijkheid van informatie en systemen aan te geven. In ons onderzoek zijn wij de volgende aanduidingen tegengekomen:

- Politie Vertrouwelijk, Politie Confidentieel en Politie Geheim;

- Gebruik van artikelen in de Wpg. Wpg artikel 9 is een hoger niveau van vertrouwelijkheid dan Wpg artikel 8;
- De termen "paarse omgeving" en "hoog beveiligde omgeving" voor systemen waarin vertrouwelijke informatie wordt verwerkt;
- Zaken in Summ-IT "onder embargo" d.w.z. dat de zaak voor een beperkte groep medewerkers toegankelijk is. Dit kan alleen als er sprake is van zeer vertrouwelijke gegevens op basis van het Besluit politiegegevens (Bpg).

De verschillende aanduidingen van vertrouwelijkheid zijn niet aan elkaar gekoppeld.

De politie heeft een rubriceringsregeling die aansluit op het VIRBI

Rubriceringsregeling Politie 2015
Aangezien de politie zeer veel vanuit de keten werkt is er veelvuldig sprake van informatie-uitwisseling met onderdelen van de Rijksoverheid. Voor de Rijksoverheid is het VIRBI van toepassing. Het VIRBI is niet van toepassing voor de politie. Om toch zoveel mogelijk aansluiting te zoeken en te houden met de ketenpartners is naar analogie van het VIRBI de *Rubriceringsregeling Politie 2015* opgesteld.

De rubriceringsregeling beschrijft hoe de politie informatie moet behandelen en rubriceren rekening houdend met nadelige gevolgen van ongeautoriseerde kennisname voor de belangen van de Staat, van zijn bondgenoten, de politie of één of meerdere ketenpartners.

De rubriceringsregeling hanteert vijf niveaus van vertrouwelijkheid:
- Politie ZEER GEHEIM (Pol.ZG);
- Politie GEHEIM (Pol.G);
- Politie CONFIDENTIEEL (Pol.C);
- Politie INTERN (Pol.I);
- Niet Vertrouwelijk (NV).

Het niveau dat gekozen wordt, hangt af van de te verwachten nadelige gevolgen als (een deel van) informatie bekend wordt bij niet geautoriseerden.

De basis voor rubricering binnen de politie is de *Rubriceringsregeling Politie 2015*. Er is ook een gedetailleerde instructie beschikbaar, het schema *Veilig omgaan met informatie* (2023) dat beschrijft hoe om te gaan met gerubriceerde informatie. Deze instructie is voor iedereen van toepassing, dus ook voor tolken/vertalers. De rubriceringsregeling en het schema geven handvatten voor het juist rubriceren van informatie.

De CISO is verantwoordelijk voor het beleid rondom rubricering, maar houdt geen toezicht op de naleving van het beleid. De CISO geeft aan dat de eigenaar van de informatie verantwoordelijk is voor de juiste rubricering. Er worden geen controles uitgevoerd op het juist rubriceren van informatie. In de praktijk gaat de eigenaar van een zaak in Summ-IT (bijvoorbeeld de teamleider) over de rubricering van informatie binnen de zaak.

Er is in 2023 een campagne gestart om medewerkers van de politie bewust te maken van beveiliging van informatie waarin ook aandacht wordt besteed aan rubricering. Dit gaat door middel van de e-learning *Altijd alert*.

De rubriceringsregeling sluit niet aan op de Wpg en wordt door CTER niet gebruikt

Wpg-artikelen geven een indicatie van vertrouwelijkheid

Wpg Artikel 8	Uitvoering van de dagelijkse politietaak
Wpg Artikel 9	Onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval
Wpg Artikel 10	Inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde
Wpg Artikel 12	Informanten

De politie heeft bewust gekozen om geen relatie te leggen tussen de rubriceringsregeling en de Wpg. De gegevensautoriteit geeft aan dat het niet mogelijk is om de rubriceringsregeling en de Wpg op elkaar te leggen. Binnen de Wpg-artikelen zijn verschillende rubriceringsniveaus mogelijk. Het is volgens de gegevensautoriteit voor de politiemedewerkers logischer om met de Wpg te werken dan met de rubriceringsregeling. CTER past de rubriceringsregeling dan ook niet toe. De rubriceringen Politie Confidentieel, Politie Geheim en Politie Zeer Geheim worden binnen CTER niet gebruikt. CTER labelt een zaak volgens de Wpg. Het gekozen Wpg-artikel geldt voor een heel dossier.
Het nadeel van deze keuze is dat iedere politiemedewerker die werkt met de Wpg-artikelen zelf het bijbehorende rubriceringsniveau en de bijbehorende maatregelen moet bepalen, bijvoorbeeld bij uitwisseling van informatie met de Rijksoverheid of andere ketenpartners. Doordat er geen relatie is gelegd tussen de Wpg en de rubriceringsregeling is het niet helder wanneer aanvullende beveiligingsmaatregelen zoals omschreven in het addendum op de BIO noodzakelijk zijn.

Binnen Summ-IT wordt informatie gerubriceerd volgens de Wpg en 'onder embargo'
Functioneel beheer voegt een Wpg-artikel toe aan Summ-IT bij het aanmaken van een dossier. Het startscherm van een dossier in Summ-IT toont geen rubriceringsniveau of Wpg-artikel. Het Wpg-artikel is wel zichtbaar in de instellingen van een dossier. Het Wpg-artikel bepaalt welke medewerker toegang krijgt tot informatie en wat de bewaartermijn is.

Daarnaast kent Summ-IT twee kleurencoderingen: groen is 'regulier' en rood is 'onder embargo'. Aangegeven is dat binnen CTER veel onderzoeken een status 'onder embargo' hebben. Uit waarnemingen blijkt dat informatie in het tapsysteem en in het opnamesysteem niet gerubriceerd wordt. Noch volgens de rubriceringsregeling, noch volgens de Wpg, noch volgens de indeling 'regulier'/'onder embargo'.

4.6 Verspreiding van vertrouwelijke informatie

Er is binnen CTER geen grip op de verspreiding van vertrouwelijke informatie; passende voorzieningen voor tolken ontbreken
Uit verschillende interviews maken wij op dat er geen grip is op het delen van informatie tussen politie en tolken en de verspreiding van informatie buiten CTER. Ongeacht of de informatie gerubriceerd/vertrouwelijk is of niet. De belangrijkste oorzaak is in onze ogen het ontbreken van de juiste voorzieningen voor tolken om veilig om te kunnen gaan met informatie.

Gebruik van autorisatie en laptop van rechercheurs

Tolken binnen CTER hebben geen eigen autorisaties voor het opnamesysteem, maar dienen wel vertaalwerkzaamheden uit te voeren in dit systeem. Daarom lenen rechercheurs hun eigen autorisatie en laptop uit om tolken toegang te verlenen tot het opnamesysteem voor vertaling van opgenomen gesprekken. Tolken werken hun vertaling soms ook uit op een laptop van een rechercheur. In de praktijk krijgen tolken binnen CTER daarmee toegang tot al dan niet vertrouwelijke informatie via de accounts van rechercheurs die hun inloggegevens delen of hun apparatuur ter beschikking stellen. Tolken kunnen via deze weg ook vertrouwelijke informatie inzien en opslaan.



Gebruik van USB-sticks

Er worden USB-sticks gebruikt om audiobestanden of te vertalen documenten te delen tussen rechercheur en tolk. Via opname- en afluisterapparatuur verzamelde audiobestanden kunnen op een USB-stick worden opgeslagen. Er wordt dan gebruik gemaakt van beveiligde USB-sticks. Het is niet verboden deze USB-sticks mee te nemen buiten het pand.



Printen via autorisaties van rechercheurs

Tolken hebben geen autorisatie om te printen. Printen verloopt via rechercheurs die hun autorisaties uitlenen aan de betreffende tolk.



De tolk had thuis een politiekluis voor opslag van vertrouwelijke informatie. Hij nam digitaal stukken mee om ook thuis te kunnen werken.

Thuiswerken door tolken

Er bestaan binnen CTER verschillende beelden of thuiswerken voor tolken was toegestaan. Het wordt niet wenselijk geacht, maar het gebeurde in de praktijk wel. Het is onduidelijk of dit veel voorkwam of dat tolken sporadisch thuiswerkten.

Nadat zijn duidingswerkzaamheden binnen CTER niet meer nodig waren, kreeg de tolk de rol van kwaliteitscontroleur. Hij controleerde de vertaalwerkzaamheden van andere tolken. Op die manier had hij toegang tot veel opgenomen gesprekken en vertalingen.

Wat te doen

- Geef tolken passende faciliteiten om hun werk te doen: laptop en account voor het beluisteren en vertalen van via opname- en afluisterapparatuur verzamelde audiobestanden, een voorziening voor het ontvangen van vertrouwelijke stukken via mail en een voorziening om te printen. Zorg dat deze faciliteiten deze in de praktijk ook gebruikt worden.

- Verbied de verspreiding van vertrouwelijke informatie via [redacted]
- Verduidelijk de relatie tussen de rubriceringsrichtlijn en de Wpg. Kies daarbij voor een vuistregel die bruikbaar is bij risicoanalyse, rubricering van informatie en de selectie van maatregelen. Bijvoorbeeld: Wpg artikel 8 – Politie Vertrouwelijk; Wpg artikel 9 – Politie Confidentieel; Wpg artikel 10 en 12 - Politie Geheim.
- Vertaal "onder embargo", "paars" en "hoog beveiligd" naar Wpg-artikelen en rubricering.

4.7 Screening van de gebruikers van informatie

Er is veel beleid over screening, wat kan leiden tot onduidelijkheid

De politie kent veel beleidsdocumenten met betrekking tot screening. De aan ons opgeleverde stukken zijn opgesteld tussen 2014 en 2023. De hoeveelheid beleidsdocumenten roept de vraag op of het screeningsbeleid eenduidig is en of het voor politiemedewerkers mogelijk is om de weg hierin te vinden.

In dit onderzoek hebben wij ons beperkt tot recente documentatie (2022-2023) en met name gekeken naar screeningsbeleid rondom externe deskundigen, zoals tolken en vertalers.

De politie hanteert vier niveaus van screening

Voor medewerkers die werkzaamheden verrichten waarbij er sprake is van een laag integriteitsrisico is een Verklaring Omtrent Gedrag (VOG) van toepassing. Naast de VOG kent de politie drie screeningsniveaus:

- Betrouwbaarheidsonderzoek (BO) – dit wordt uitgevoerd door de politie en is van toepassing als een medewerker voor diens functie kennisneemt van politiegegevens die vallen onder Wpg artikel 9.
- Betrouwbaarheidsonderzoek en omgevingsonderzoek (BO+) – dit wordt uitgevoerd door de politie en is van toepassing als een medewerker voor diens functie kennisneemt van politiegegevens die vallen onder Wpg artikelen 10 en 12. Onder omgeving wordt in ieder geval verstaan de partner, inwonende ouders en kinderen. Er wordt dan ook gekeken of deze personen voorkomen in de politiële en justitiële systemen.
- Een veiligheidsonderzoek – dit wordt uitgevoerd door de AIVD en is mogelijk van toepassing als een medewerker ondersteuning biedt aan het heimelijk domein, het domein cryptobeheer, interne veiligheid of nationale veiligheid. Bij positieve afloop van het veiligheidsonderzoek leidt dit tot verstrekking van een Verklaring van Geen Bezwaar (VGB) door de AIVD.

Er is geen eenduidig beeld of een AIVD A-veiligheidsonderzoek voor medewerkers van CTER nodig is

De *Aanwijsgronden vertrouwensfuncties Nationale Politie* (2022) bevat een lijst met vertrouwensfuncties. Voor politiemedewerkers met werkzaamheden op het terrein van contra-terrorisme, extremisme en radicalisering wordt aangegeven dat hier sprake is van een vertrouwensfunctie op A-niveau. Onduidelijk is op welke functies binnen CTER dat betrekking heeft.

Geïnterviewden binnen CTER geven aan dat CTER-medewerkers minimaal een screening BO+ hebben en dat medewerkers binnen team Informatie (Intel) een VGB-A hebben.

Enkele geïnterviewden zijn van mening dat alle medewerkers van CTER een VGB-A zouden moeten krijgen.

Screening van de tolk
In de administratie van het Nationaal Tolken Coördinatiepunt Politie Nederland is vastgelegd dat de tolk op 11-10-2011 een screening VGB-lang (destijds de terminologie voor een door de politie uitgegeven screening) heeft gekregen.
De herscreening moest uiterlijk op 11-10-2016 worden uitgevoerd. Deze herscreening heeft niet plaatsgevonden. Na 2016 beschikte de tolk dus niet over de juiste screening.

Voor tolken geldt een screening BO of screening BO+ en soms een AIVD A-veiligheidsonderzoek
Voor tolken is aangegeven dat ze een screening BO of screening BO+ behoren te krijgen. Geïnterviewden binnen CTER geven aan dat een veiligheidsonderzoek door de AIVD mogelijk wenselijk is voor tolken binnen CTER gezien de toenemende dreiging van inmenging van statelijke actoren en criminele organisaties. Zeker als deze tolken over een lange periode meedraaien binnen een of meerdere CTER-onderzoeken en dus toegang krijgen tot vertrouwelijke informatie en embargo-onderzoeken. Volgens het beleid is het voor tolken/vertalers maatwerk om te bepalen wanneer een AIVD A-veiligheidsonderzoek nodig is.

Inschrijving van de tolk
Volgens de Wet beëdigde tolken en vertalers is de politie verplicht om in straf- en vreemdelingenzaken beëdigde tolken en vertalers in te zetten (er zijn uitzonderingen).
Beëdigde tolken en beëdigde vertalers staan ingeschreven in het Register beëdigde tolken en vertalers (Rbtv). De tolk was tot 2016 in het Rbtv ingeschreven als vertaler. Hij is nooit ingeschreven geweest als tolk.
Na de beëindiging in 2016 van de inschrijving in het Rbtv heeft de tolk nog tot mei 2021 binnen de politie op een lijst met tolken/vertalers gestaan van het tolkenbureau.
Bij de uitbesteding van tolkenbureaus in 2021 bleek dat de tolk niet in het Rbtv stond. De tolk is toen verwijderd van de lijst met tolken/vertalers van het tolkenbureau.
Ondanks het feit dat de tolk in 2021 van de lijst is verwijderd, heeft de politie zijn inzet gecontinueerd, zowel binnen de Landelijke Eenheid als binnen regionale eenheden.

Wat te doen
- Schoon het beleid over screening op.
- Schep duidelijkheid over de vereiste screening voor CTER-medewerkers.
- Geef richting aan het maatwerk om te bepalen wanneer een AIVD A-veiligheidsonderzoek nodig is voor een tolk die werkzaam is voor CTER.

4.8 Logging en monitoring

Het loggingbeleid is actueel en uitgebreid, maar geeft weinig richting aan monitoring om onrechtmatig gebruik te voorkomen
Het *Beleidskader logging* (2023) gaat in op een groot aantal aspecten van logging. In het beleid wordt bijvoorbeeld benoemd waarom wordt gelogd, wat de grondslagen zijn voor logging (AVG, Wpg, BIO), welke gebeurtenissen worden gelogd (handelingen van gebruikers, activiteiten van beheerders, wijziging van autorisaties, verstoringen, beveiligingsincidenten), welke details worden vastgelegd, de bewaartermijn van

loginformatie, wie toegang heeft tot loginformatie en met welk doel.
Er is geen gedetailleerd beleid voor monitoring van het gebruik van informatie door medewerkers en geen beleid voor analyse van de logging. Er wordt in het loggingbeleid wel aandacht besteed aan protective monitoring. Er wordt aangegeven dat het noodzakelijk is om met tools naar atypische signalen te zoeken en op die manier preventief te sturen op het voorkomen van onrechtmatig gebruik en zo mogelijk onrechtmatig gebruik real time te detecteren. Overigens werd in het autorisatiebeleid uit 2016 al benoemd dat ernaar moet worden gestreefd dat afwijkend gedrag in het bevragen van gegevens kan worden herkend.

Protective monitoring volgens het *Beleidskader logging (2023)*
Om optimaal te voldoen aan de doeleinden van logging is het noodzakelijk om met behulp van geautomatiseerde tools proactief naar atypische signalen te zoeken en op die manier preventief te sturen op het voorkomen van onrechtmatig gebruik en zo mogelijk onrechtmatig gebruik real time te detecteren. De aanleiding om hiermee te starten ligt in toenemende dreiging, toename van consequenties van een inbreuk door centralisatie en de onmogelijkheid 'derden' altijd buiten te houden. De Autoriteit Persoonsgegevens ziet dit bovendien als een noodzakelijke maatregel om als verwerkingsverantwoordelijke aan de verplichtingen rond informatiebeveiliging te kunnen voldoen.

Protective monitoring wordt in het beleid niet verder gedetailleerd. Zo is bijvoorbeeld nog niet uitgewerkt welke gebruikershandelingen een atypisch signaal zijn (bijvoorbeeld het raadplegen van informatie op opvallende tijden, het raadplegen van informatie buiten het eigen werkgebied, het downloaden van grote hoeveelheden informatie) en wie de signalen moet oppakken.

Summ-IT en het tapsysteem loggen "alle" gebruikershandelingen; het opnamesysteem niet
In de systemen Summ-IT en het tapsysteem vindt uitgebreide logging plaats van de handelingen van gebruikers. Daarnaast worden handelingen rondom het toekennen van autorisaties in de logging vastgelegd. Beheerders van Summ-IT en het tapsysteem geven aan dat loginformatie voor het tapsysteem en Summ-IT respectievelijk 11 en 13 jaar bewaard wordt.

In tegenstelling tot Summ-IT en het tapsysteem is over het gebruik van het opnamesysteem geen logging beschikbaar. Rechercheurs van CTER en tolken maken bij het benaderen van het opnamesysteem gebruik van één gedeeld (niet persoonsgebonden) account. Dit heeft tot gevolg dat handelingen, ook als deze wel zouden worden gelogd, niet te herleiden zijn naar individuele gebruikers.

Geen structurele monitoring van gebruikershandelingen bij CTER
Hoewel de systemen Summ-IT en het tapsysteem uitgebreide logging van gebruikershandelingen bieden, vindt er niet standaard analyse plaats van deze logging om inbreuken op de beveiliging door handelingen van gebruikers te detecteren. De politie heeft aangegeven dat analyse van logging wel onderdeel kan zijn van bijv. een integriteitsonderzoek dat achteraf plaatsvindt. Hiermee is er geen structurele monitoring op de handelingen van gebruikers van deze systemen aanwezig. Het gebruik van het opnamesysteem kan niet worden gemonitord, vanwege het ontbreken van logging.

De politie heeft een pilot atypisch gedrag uitgevoerd in Amsterdam. Deze pilot gaat met name over het monitoren van bevragingen van politiesystemen en is een eerste stap in de inrichting van protective monitoring. Binnen CTER is protective monitoring niet ingericht. Wij hebben geen informatie ontvangen waaruit we kunnen opmaken of en wanneer er binnen CTER protective monitoring wordt ingericht.

Wat te doen

- Richt structurele monitoring in op basis van de in het tapsysteem en Summ-IT gelogde gebruikershandelingen.
- Maak een begin met protective monitoring door in beeld te brengen wat de atypische signalen zijn bij CTER die via protective monitoring naar voren moeten komen.
- Ga na welke faciliteiten de logging van Summ-IT en het tapsysteem nu al bieden om die atypische signalen te rapporteren.

4.9 Behandeling van inbreuken op de beveiliging

De Rubriceringsrichtlijn Politie 2015 over inbreuken op beveiliging

De rubriceringsrichtlijn schrijft de volgende stappen voor bij compromittering, d.w.z. kennisname dan wel mogelijkheid tot kennisname van vertrouwelijke informatie door niet geautoriseerden:

- Een inbreuk op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromittering van informatie dient onmiddellijk afgehandeld te worden conform de uitgangspunten van het informatiebeveiligingskader Nationale Politie.
- De CISO heeft bij incidenten de bevoegdheden en verantwoordelijkheden zoals beschreven in het door de korpsleiding vastgestelde document 'inrichting CISO directie IV'. De CISO kan bij incidenten nader onderzoek instellen om herhaling van incidenten te voorkomen.
- In de afhandeling van incidenten worden relevante partijen geïnformeerd.

Het beleid voor het melden van mogelijke inbreuken op beveiliging is alleen van toepassing op systemen die worden beheerd door het PDC

De politie kent de *Procedure registratie en afhandeling beveiligingsincidenten* uit 2022. Hierin is omschreven hoe en bij wie een beveiligingsincident kan worden gemeld, wat er vervolgens met een melding wordt gedaan en hoe deze wordt geregistreerd. Er is in de *Procedure registratie en afhandeling beveiligingsincidenten* niet beschreven hoe er anoniem kan worden gemeld en of medewerkers beschermd worden tegen juridische procedures en benadeling als ze een melding doen[9]. De scope van de procedure is beperkt tot systemen die worden beheerd door de dienst ICT, gebruikers van de systemen van de dienst ICT en het handelen door medewerkers van de dienst ICT. Er is geen informatie aangetroffen over de afhandeling van mogelijke inbreuken op de beveiliging van systemen die niet door de dienst ICT worden beheerd (eigen beheerde omgevingen). Bijvoorbeeld het opnamesysteem dat in gebruik is bij CTER.

[9] Er bestaan bij de politie verschillende mogelijkheden om een (anonieme) melding te doen. De *Procedure registratie en afhandeling beveiligingsincidenten* verwijst daar niet naar.

Er is beleid hoe te handelen in geval van klachten over tolken
De politie heeft een *Stroomschema integriteitskwesties tolken* (2018) dat beschrijft hoe te handelen in het geval van klachten over tolken, klachten van tolken of gevallen waarbij een tolk is betrokken bij een incident.

Rapportage waarin alle incidenten met systemen en informatie binnen de politie samenkomen, ontbreekt
De politie beschikt niet over een incidentenrapportage met een overzicht van alle incidenten met systemen en informatie die zich bij de politie hebben voorgedaan. Er is daardoor geen politie breed zicht op hoeveel inbreuken op de beveiliging van informatie er zijn, wat de aard is van de inbreuken en welke schade daarmee wordt aangericht.

Wat te doen
- Richt de registratie en afhandeling in van inbreuken op de beveiliging van Eigen beheerde omgevingen.
- Richt een incidentenrapportage in van alle incidenten met systemen en informatie die zich bij de politie hebben voorgedaan.

4.10 Aandacht van het management door controle en toezicht

Het toezicht op het voldoen aan de rubriceringsregeling is niet uitgewerkt in een concreet plan
Volgens de rubriceringsregeling is de concern security officer belast met het toezicht op de integrale beveiliging. De lijnmanager moet zorgen voor toereikende beveiliging en de mogelijkheid om toezicht en controle uit te oefenen in het geval dat gerubriceerde informatie buiten de politie wordt gebracht. Daarnaast eist de rubriceringsregeling dat gedurende de gehele levenscyclus van een informatiesysteem (waarin gerubriceerde informatie wordt verwerkt) periodieke audits, inspecties, reviews en tests uitgevoerd worden om te controleren of de beveiligingsmaatregelen effectief zijn.

Er is niet uitgewerkt hoe de politie het toezicht op het voldoen aan de rubriceringsregeling heeft ingericht. Wij hebben geen plan voor het toezicht aangetroffen waarin is uitgewerkt:
- de rolverdeling;
- de rapportagelijnen;
- de frequentie en intensiteit van toezicht;
- het roulerend toetsen van organisatieonderdelen en beveiligingsmaatregelen, gebaseerd op een risicoafweging.

Er is nauwelijks capaciteit voor toezicht, het voldoen aan de rubriceringsregeling wordt niet getoetst
Aangegeven is dat er beperkte capaciteit is voor toezicht. Eenheden hebben meestal één beveiligingscoördinator die het werk vaak in deeltijd of in combinatie met andere werkzaamheden moet doen. De tweede lijn van het "three lines" model is volgens de CISO op dit moment niet op orde en moet nog worden opgebouwd.

Three lines
Het three lines model (ook aangeduid als het three lines of responsibility model) is een beheersingsmodel dat uitgaat van drie lagen bij de beheersing van risico's: management (laag 1), interne controle (laag 2) en audit (laag 3).

Het toezicht wordt op dit moment met name ingevuld door Concern Audit en door het uitvoeren van Wpg-audits door een externe partij. Het voldoen aan de rubriceringsregeling blijft hierbij buiten beschouwing. De jaarplannen van Concern Audit in de periode 2021 – 2024 bevatten geen onderzoeken naar het voldoen aan de rubriceringsregeling. In het rapport van een uitgevoerde Wpg-audit (september 2023) wordt de rubriceringsregeling niet genoemd.

Ook voor CTER is geen sprake van ingericht toezicht op het voldoen aan de richtlijnen voor beveiliging van informatie zoals de rubriceringsregeling. Het plaatsvervangend hoofd Landelijke Recherche geeft aan dat in het MT Landelijke Opsporing en Interventies een paar keer per jaar onderwerpen als privacy, de stand van zaken van de Wpg en beveiligingsmaatregelen op de agenda komen. Er is vooral aandacht voor bij een directe aanleiding bijv. een incident of een dreiging van buiten.

Concern Audit heeft aan de bel getrokken over het ontbreken van toezicht

In de 8-maandsrapportage 2023 (1-12-2023) signaleert Concern Audit *'de organisatie loopt langzaam vast door de huidige inrichting en stelselkeuze, de werking van de governance, het ontbreken van integraal risicomanagement en intern toezicht.'*

Het voorstel van Concern Audit is:
'Eerst bepalen wat de strategische koers is, hoe die te bereiken en met welke prioriteiten. Scherp hebben wat de risico's zijn die de realisatie bedreigen en welke risico's wel en niet acceptabel zijn. Hoe en op welke momenten moeten de opdrachtnemers zich verantwoorden over de realisatie van hun opdracht. Dan het intern toezicht verbeteren en verantwoording afdwingen.'

Een externe prikkel kan helpen maatregelen te treffen maar daarmee is toezicht nog niet ingericht

N.a.v. het rapport van een uitgevoerde Wpg-audit (2023) heeft de politie een verbeterrapport opgesteld. De *Regeling periodieke audit politiegegevens* (2019) schrijft voor dat die reactie er binnen drie maanden moet zijn als er tekortkomingen zijn geconstateerd.

Volgens het verbeterrapport worden in de periode 2024-2026 door de politie verbetermaatregelen doorgevoerd. Onder andere op het gebied van autorisatiebeleid, risicoanalyse voor hoog-risico verwerkingen, logging en monitoring. De voortgang wordt bewaakt door de gegevensautoriteit en Concern Audit doet jaarlijks een hercontrole.

Blijkbaar helpt een externe prikkel om onderdelen van informatieverwerking te verbeteren. Het interne toezicht op het blijvend voldoen aan de rubriceringsregeling is daarmee niet ingericht.

Wat te doen?
Stel een beveiligingscoördinator aan bij de eenheid Landelijke Opsporing en Interventies die toezicht houdt op de beveiliging van informatie bij CTER.

4.11 Langdurige inzet als tolk

Er is geen beleid dat langdurige inzet van een tolk verbiedt

Het *Beleidskader tolken en vertalers* (2021) geeft aan dat het in grote onderzoeken die langer duren onwenselijk is om gedurende het onderzoek te wisselen van tolk. De politie wil dan dezelfde tolk in kunnen zetten, zonder opnieuw de vraag aan het

tolkenbureau te moeten stellen en een andere tolk aangeboden te krijgen.

De tolk is ingezet in de periode 2002 – 2023
De tolk werd bij de politie vanaf 2002 ingehuurd op het aandachtsgebied contraterrorisme, extremisme en radicalisering, vanwege zijn specifieke expertise die in de beginperiode van de inhuur binnen de politie nog niet ruim voorhanden was. Rond 2016 heeft de politie meer experts in dienst genomen. De tolk is wel aangebleven. Zijn rol is toen gaandeweg veranderd van tolk/duider naar tolk/kwaliteitscontroleur. Zijn inzet is gecontinueerd tot zijn arrestatie in 2023.

Langdurige inzet wordt niet door alle betrokkenen opgevat als risico
Geïnterviewden hebben geen eenduidig beeld over de (on)wenselijkheid van langdurige inzet. Een aantal geïnterviewden binnen CTER is positief over langdurige inzet van tolken vanwege betrokkenheid vanaf het begin van een onderzoek, inhoudelijke kennis en de mogelijkheid om snel in te huren. Langdurige inzet wordt in het beleid niet als risico benoemd. Wel wordt als risico gezien dat door politie ingezette tolken en vertalers informatie verstrekken aan kwaadwillende belanghebbenden (bijvoorbeeld tegen betaling of onder bedreiging), of dat ze informatie verliezen door het onzorgvuldig gebruik van elektronische gegevensdragers.

Langdurige inhuur en afhankelijkheid van bijzondere expertise vormen volgens het geïnterviewde lid korpsleiding een risico voor de politie. Het lid korpsleiding geeft aan dat het langdurig uitvoeren van een functie niet wenselijk is. Vooral niet in een functie waarin veel vertrouwelijke informatie wordt behandeld. Het lid korpsleiding geeft aan niet betrokken te zijn geweest bij de afwegingen rondom de langdurige inzet van de tolk.

Langdurige inzet van de tolk heeft vertrouwen gewekt waardoor informatie werd gedeeld
De politie geeft aan dat in de loop der jaren tussen medewerkers van CTER en de tolk een verstandhouding is gegroeid, die gekenmerkt werd door een hoge mate van vertrouwen. Met name door de aantoonbare toegevoegde waarde die de tolk in vele onderzoeken heeft geleverd en zijn flexibele instelling. Die verstandhouding heeft er mede aan bijgedragen dat zonder terughoudendheid door de teamleden veel informatie werd gedeeld op een wijze die niet veilig was en niet in lijn met de voorschriften.

Wat te doen?
- Bij langdurige inzet van een tolk periodiek een bewuste afweging maken (door het management van CTER) of de inzet voortgezet moet worden.
- Screening van tolken periodiek controleren.

5. Signalen over de analist/tolk en de opvolging daarvan

5.1 Geen van de geïnterviewden had signalen over het bezitten en naar buiten brengen van staatsgeheime of vertrouwelijke informatie

Wij hebben alle geïnterviewden bij de NCTV en de politie gevraagd of zij signalen hadden met betrekking tot de casus: de verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Geen van de geïnterviewden heeft aangegeven dat zij dergelijke signalen hadden.

5.2 De samenloop van functies was algemeen bekend en heeft voor 'gedoe' gezorgd maar staat los van de casus

De samenloop van functies was binnen politie en NCTV breed bekend en werd als nuttig gezien

De persoon in de casus was lange tijd (vanaf 2005) zowel analist bij de NCTV als tolk bij de politie. Deze samenloop van functies was binnen beide organisaties algemeen bekend.
Beide organisaties zagen de samenloop van functies als logisch en nuttig. De analist/tolk had specifieke expertise en zijn inzet was daarom bij zowel de NCTV als de politie nodig. Dit was in het begin van de samenloop van functies een logische keuze, in de context van kennisopbouw bij de politie rondom dreigingen van terrorisme. Er waren geen specifieke afspraken over hoe de analist/tolk om moest gaan met NCTV-informatie bij de politie of met politie-informatie bij de NCTV. Desondanks was het volgens geïnterviewden bij de NCTV voor iedereen duidelijk dat je geen informatie van de NCTV mocht delen met derden.
De analist was binnen de NCTV werkzaam voor de afdeling Analyse tot en met 2022. Daarna werkte de analist bij de NCTV-Academie.

Beeld uit interviews over de analist/tolk

De analist had een aparte status binnen de NCTV met informele macht die was gebaseerd op zijn gedetailleerde kennis en langdurig dienstverband. Hij stond moeilijk open voor andere meningen, wat tot spanningen op de werkvloer leidde. Hij had veel middelen tot zijn beschikking (harde schijf, USB-sticks) en maakte lange dagen.

Het beeld dat bij de politie wordt geschetst kent overeenkomsten met het beeld bij de NCTV. Ook binnen CTER had de tolk een aparte status. Dit kwam onder andere door zijn NCTV-werk. Hij werd of gezien als "meer deskundig" of als "vooruitgeschoven post van de NCTV". De politie had baat bij zijn kennis. De tolk had een sleutelpositie waarmee hij toegang had tot gevoelige dossiers, zoals over de aanslagen in Brussel en Parijs en het dossier over uitgereisde Nederlanders. Op informeel niveau had hij toegang tot veel informatie. Hij maakte ook bij de politie lange dagen, werkte ook op ongebruikelijke tijdstippen en had bij de politie de beschikking over eigen middelen (laptop, USB-stick, kluis).

In de omgang bij de politie was de tolk aardig, beleefd en presenteerde hij zich goed. De aanname was dat hij gescreend was en dus te vertrouwen. Daarbij speelde ook mee dat het

vertrouwen groeide doordat hij zo vaak over de vloer kwam.

Binnen de NCTV is de samenloop van functies goedgekeurd, binnen de politie is dat onduidelijk

Uit verslagen van personeelsgesprekken bij de NCTV in 2014 en 2016 blijkt dat in die jaren de samenloop van inzet bij de NCTV en de politie is besproken en goedgekeurd. De analist heeft zijn inzet bij de politie op verzoek van de Nationaal Coördinator in 2019 opnieuw geregistreerd in het personeelssysteem. Een expliciete goedkeuring van die registratie ontbreekt.

Bij de politie is niet duidelijk door wie en wanneer afspraken zijn gemaakt over de samenloop van functies en of de afspraken zijn vastgelegd. Volgens geïnterviewden heeft de politie wel gesprekken gevoerd met de NCTV over de combinatie van werken bij de NCTV en optreden als tolk bij de politie. Steeds werd in die gesprekken vastgesteld dat er sprake was van twee te onderscheiden rollen: tolk/vertaler bij de politie en analist bij de NCTV.

In interviews bij de politie is aangegeven dat het vaker voorkomt dat politiemedewerkers of door de politie ingehuurde personen een andere functie hebben buiten de politieorganisatie. Dat is volgens een aantal geïnterviewden geen probleem zolang er geen tegenstrijdig belang is tussen functies. Volgens het voor dit onderzoek geïnterviewde lid korpsleiding is dat wel een probleem. Hij verbaast zich over de samenloop van functies van de tolk en geeft aan dat hij hier niet van op de hoogte was. Dat de politie deze keuze maakt, heeft volgens hem te maken met schaarse expertise. Overigens was het lid van de korpsleiding dat verantwoordelijk is voor de Landelijke Eenheid wel op de hoogte van de samenloop van functies.

Vanaf 2015 zijn er meerdere geluiden dat de analist/tolk zijn twee rollen niet goed kan scheiden

De politie beschrijft in een feitenrelaas dat in 2015 drie medewerkers van CTER melding doen aan de teamleider CTER. Zij geven aan dat de tolk zijn rol binnen de NCTV en binnen de politie niet goed kan scheiden. De tolk heeft kennis van (opsporings)informatie die valt onder de reikwijdte van de Wpg. Dergelijke informatie mag alleen volgens wettelijke voorschriften worden gedeeld met een instantie zoals de NCTV. Wij hebben geen concretere informatie over wat er destijds gemeld is. In het feitenrelaas is opgenomen dat volgens de melders geen actie is ondernomen op de melding.

Rond 2017 deelt de analist/tolk vertrouwelijke politie-informatie buiten het politiedomein richting een ambtenaar van SZW. Dit leidt tot een 'sfeer van wantrouwen' tussen SZW en analisten van de NCTV. In een artikel in de NRC van 10 april 2021 wordt later aan deze situatie gerefereerd. Ook is er binnen de NCTV een ander signaal bekend dat de analist/tolk zijn twee rollen niet goed kan scheiden: in 2021 deelt de analist/tolk operationele politie-informatie tijdens analyses bij de NCTV.

Bij CTER leidde de samenloop van functies tot een ongemakkelijk gevoel bij sommige medewerkers. Ze vonden het onduidelijk in hoeverre de tolk voor de politie werkte en in hoeverre voor de NCTV. Ze vroegen zich af tot welke politie-informatie de NCTV toegang had via de tolk en of het überhaupt mogelijk was voor de tolk om beide rollen te scheiden. Door deze medewerkers werd de tolk als 'verlengstuk' van de NCTV gezien. Enkele geïnterviewden vragen zich af of het wenselijk was dat de tolk duider was binnen de politie, naast zijn werkzaamheden als duider bij de NCTV. Deze geluiden hebben niet geleid tot een formele melding.

In 2021 vindt bij de politie onderzoek plaats. Conclusie: geen risico; de samenloop van functies blijft bestaan

Op 15 april 2021 doet een medewerker van het cluster CTER die naar eigen zeggen al lange tijd zorgen uitte over de rol van de tolk een melding van integriteitsschendingen door de tolk; een artikel in de NRC op 10 april 2021 was hiervoor deels de aanleiding. De melding ging in de kern om het onjuiste gebruik van politie-informatie door de tolk buiten het politie-domein (d.w.z. bij de NCTV).

De melding wordt behandeld door de afdeling Veiligheid, Integriteit en Klachten (VIK) van de Landelijke Eenheid. De afhandeling door VIK ziet er op hoofdlijnen als volgt uit:

- Het OM wordt geïnformeerd. Het OM geeft aan dat een strafrechtelijk onderzoek niet opportuun is. Wel adviseert het OM een gesprek met de tolk aan te gaan en zijn werkzaamheden tegen het licht te houden op gebied van vertrouwelijkheid en verenigbaarheid van werkzaamheden voor politie en NCTV.
- De leiding van de Landelijke Eenheid en de leiding van het tolkencoördinatiepunt worden op de hoogte gesteld van de melding.
- De programmaleider CTER verspreidt een interne memo naar de betrokkenen waarin de bestaande werkafspraken over de verschillende rollen van de tolk uiteen zijn gezet.
- Er volgt een gesprek tussen de tolk, de verantwoordelijke voor het tolkencoördinatiepunt en de liaison van de landelijke eenheid voor het tolkencoördinatiepunt.
- De conclusie is dat er geen risico is en geen verdere actie benodigd is.
- Het OM wordt op de hoogte gesteld van de afhandeling.

Deze melding en de opvolging ervan zijn volgens een van de geïnterviewden bij de politie besproken met de analist/tolk en zijn leidinggevende van de NCTV.
Na het feitenonderzoek van VIK blijft de samenloop van functies bestaan.

Bij de behandeling heeft VIK niet gekeken naar:

- het beeld dat het signaal al eerder zonder succes aan de teamleider gemeld is;
- de screening van de tolk (die dan al vijf jaar verlopen is);
- de (ontbrekende) registratie van de tolk op de lijst van beëdigde tolken/vertalers.

NCTV laat in 2021 de afhandeling over aan de politie en de samenloop van functies blijft bestaan

Ook binnen de NCTV is bekend dat de tolk zijn twee rollen niet goed kan scheiden. De Nationaal Coördinator heeft naar aanleiding van het artikel in de NRC in 2021 contact opgenomen met de politie met de vraag of het signaal m.b.t. SZW bij hen tot verder onderzoek zou moeten leiden. De politie gaf aan dat dit niet het geval was. De Nationaal Coördinator heeft toen de afweging gemaakt geen verdere actie te ondernemen.

In oktober 2021 is de Nationaal Coördinator gebeld door de inspecteur-generaal Inspectie JenV met de mededeling dat er uit het onderzoek dat de inspectie JenV bij CTER had uitgevoerd signalen kwamen dat er spanningen waren rondom de analist/tolk. De Nationaal Coördinator heeft kennisgenomen van dit signaal en heeft het geplaatst in de context dat er binnen de politie altijd veel discussie is over tolken vanwege o.a. het verschil in financiële vergoeding tussen tolken en politiepersoneel. De Nationaal Coördinator heeft aan de inspecteur-generaal aangegeven het signaal bij de politie te

melden, omdat het betrekking had op het werk van de analist/tolk bij de politie. Voor de Nationaal Coördinator was dit signaal een bevestiging van het beeld dat er spanningen waren rondom de analist en daarmee geen nieuw signaal. De Nationaal Coördinator heeft toen de afweging gemaakt geen verdere actie te ondernemen dan de overplaatsing naar de NCTV-Academie die op dat moment al in gang was gezet.

Binnen de NCTV bestaan verschillende beelden of het niet goed kunnen scheiden van rollen meespeelde bij de overplaatsing van de analist

In 2022 zet de NCTV de overplaatsing van de analist in gang. Hij wordt overgeplaatst van de afdeling Analyse naar de NCTV-Academie. Hij zou dan geen analysewerkzaamheden meer uitvoeren voor de NCTV maar wel toegang houden tot de informatie in het staatsgeheime digitale archiefsysteem, inclusief staatsgeheime informatie, om zijn werkzaamheden bij de NCTV-Academie te kunnen uitvoeren.

Er zijn binnen de NCTV verschillende beelden over de rol die 'het gedoe' rondom de samenloop van functies heeft gespeeld bij deze overplaatsing. Enerzijds komt het beeld naar voren dat het signaal dat de analist zijn rollen niet goed kon scheiden geen invloed heeft gehad op zijn overplaatsing. De aanleiding zou zijn dat de analist een persoon was die moeilijk openstond voor andere meningen, wat tot spanningen binnen de afdeling Analyse leidde. Bovendien zou de tolk zich bedreigd voelen door de NRC-artikelen.

Anderzijds wordt aangegeven dat de samenloop van functies van de analist is heroverwogen omdat de analist informatie van de politie zou hebben gedeeld binnen de NCTV. Dat zou vervolgens hebben geleid tot de interne overplaatsing en contact met de politie. Er is toen ook gekeken of de toestemming voor zijn werkzaamheden als tolk bij de politie ingetrokken kon worden, maar dat bleek juridisch moeilijk.

In mei 2023 is de overplaatsing van de analist afgerond. De analist is dan niet meer bij de afdeling Analyse werkzaam, maar hij blijft werkzaam voor zowel de NCTV als de politie.

5.3 Bij de politie worden enkele voorvallen niet als signaal opgevat

Uit een feitenrelaas van de politie komt naar voren dat de tolk in 2018 buiten kantoortijd wordt aangetroffen in een werkruimte terwijl hij ogenschijnlijk een kast doorzoekt. De medewerker van CTER heeft dit naar eigen zeggen mondeling gemeld aan zijn leidinggevende maar deze herinnert zich de melding niet. Dit voorval heeft niet geleid tot een vervolgactie.

In de afgelopen vijf jaar heeft een leidinggevende van het cluster CTER de tolk regelmatig (een keer per drie maanden) als laatste aan het werk gezien terwijl de CTER-etage verder leeg was. Tolken mogen volgens het beleid alleen onder begeleiding van een politiemedewerker op de CTER-etage aan het werk zijn. De leidinggevende heeft de tolk in die gevallen naar huis gestuurd. Verdere actie heeft niet plaatsgevonden.

5.4 Bij de NCTV worden meldingen van buiten niet opgepakt

Naast het signaal over het niet goed kunnen scheiden van zijn rollen, zijn er binnen de NCTV twee andere signalen geweest rondom de analist. Deze signalen zijn niet opgepakt.





In 2021 is in een interview tussen een journalist van de NRC en de Nationaal Coördinator aan de orde geweest dat de analist een harde schijf gebruikte en mee naar huis zou nemen. Dit punt is in 2021 niet gepubliceerd door de NRC. In 2023 is dit wel vermeld door de NRC in een artikel dat betrekking heeft op de casus. De Nationaal Coördinator heeft het gebruik en het mee naar huis nemen van een harde schijf door de analist niet gezien als aanleiding voor verdere actie.

Met het gebruik van een harde schijf ontstaat de mogelijkheid tot het verspreiden van staatsgeheime informatie. In onze ogen heeft de NCTV hier nagelaten het signaal over het mee naar huis nemen van de harde schijf verder te onderzoeken door na te gaan: Wordt inderdaad een harde schijf meegenomen? Waar naartoe? Welke informatie wordt op de harde schijf opgeslagen? Hoe is de informatie beveiligd?

5.5 NCTV-medewerkers hebben meldingen gedaan na bekend worden van de casus

Nadat de casus bekend is geworden, is naar voren gekomen dat de analist verschillende medewerkers van de NCTV heeft gevraagd voor hem te printen vanaf de Stg.-omgeving. Na zijn overplaatsing en het intrekken van zijn autorisaties had de analist hier niet langer zelf toegang toe. De betreffende NCTV-medewerkers hebben dit niet direct gemeld, maar hebben dit aangegeven bij de leidinggevende of de CISO/BVC nadat de casus bekend is geworden. De CISO/BVC heeft het signaal gemeld bij de Nationaal Coördinator. Nadat de casus bekend is geworden, was er geen noodzaak meer voor directe actie.

6. Maatregelen na het bekend worden van de casus

Politie is gestart met twee teams die de mogelijke gevolgen analyseren, onderzoek doen en maatregelen treffen

Na de aanhouding van de tolk zijn twee beleidsinterventieteams (BIT's) opgestart: het BIT Landelijke Eenheid en het BIT Korpsstaf.

Het BIT Landelijke Eenheid is verantwoordelijk voor het inzichtelijk maken van personele en operationele risico's voor de Landelijke Eenheid, het reconstrueren van de gang van zaken rond de inzet van de tolk en de zorg voor het personeel van het cluster CTER.

Het BIT Korpsstaf is verantwoordelijk voor de coördinatie van maatregelen binnen het gehele korps n.a.v. de aanhouding van de tolk, voor de afstemming met het ministerie van JenV, voor de afstemming met nationale en internationale stakeholders, voor de mogelijke internationale consequenties en voor de begeleiding van het externe onderzoekstraject (het ADR-onderzoek).

Aangegeven wordt dat vanuit de beide BIT's de volgende activiteiten zijn gestart:

- Het BIT Landelijke Eenheid heeft ingezet op voorlichting voor het cluster CTER, waarbij er gefocust is op bewustwording rondom veiligheid en procedures rondom de inzet van tolken/vertalers.
- Er is onderzocht wat de gevolgen zijn van de aanhouding van de tolk voor de politie. Er is o.a. gekeken naar eventuele veiligheidsrisico's voor individuele medewerkers en lopende onderzoeken.
- Er zijn waar nodig maatregelen getroffen in de operatie om mogelijke schadelijke gevolgen te beheersen.
- De autorisaties van de tolk, mogelijke veiligheidsrisico's en het declaratiegedrag van de tolk zijn onderzocht.
- Er is een tijdlijn opgesteld met daarop de inzet van de tolk binnen de Landelijke Eenheid, ontvangen signalen over de tolk, een overzicht van uitgegeven autorisaties en loginactiviteiten van de tolk, op welke onderzoeken de tolk actief was en wat er is opgepakt aan maatregelen naar aanleiding van het door de Inspectie JenV uitgebrachte rapport.
- Bij de Autoriteit Persoonsgegevens is formeel melding gedaan van een datalek.
- In de periode kort na de aanhouding zijn diverse ruimtes gecontroleerd op aanwezigheid van opname- of afluisterapparatuur en is een controle uitgevoerd op aanwezigheid van mogelijke malware op de systemen. Digitale en fysieke autorisaties op de locatie van het cluster CTER worden opgeschoond.
- Herscreening van tolken/vertalers is in gang gezet als bleek dat de screening verlopen was. Het juiste screeningsniveau moet daarbij worden bepaald door de teamleider van het onderzoek waarop de tolk/vertaler wordt ingezet.

Vanuit CTER is een werkgroep opgericht die zich in bredere zin bezighoudt met de omgang met tolken binnen de landelijke eenheid. De eerste maatregel uit deze werkgroep is dat tolken niet langer gebruik maken van USB-sticks.

Binnen CTER worden de autorisaties nagekeken van onderzoeken die vallen onder art. 9 Wpg.

Opgeleverde informatie laat zien dat door de politie gedetailleerd onderzoek gedaan is

De politie heeft n.a.v. de casus een feitenrelaas opgeleverd aan de ADR. Hieruit blijkt dat de politie gedetailleerd onderzoek heeft gedaan naar de volgende aspecten:

- de inzet van de tolk bij de politie, zijn rol binnen CTER, zijn screening en registratie in het tolkenregister, meldingen over de tolk;
- de werkwijze binnen CTER t.a.v. informatie-uitwisseling met tolken en gebruik van accounts van CTER-medewerkers door tolken;
- toegang van de tolk tot informatie in Summ-IT.

Bij de afsluiting van ons onderzoek heeft de politie aangegeven dat er nog nader onderzocht wordt tot welke informatie de tolk toegang had.

Er is geen eenduidig beeld over alle bij de politie getroffen maatregelen

Uit interviews binnen CTER blijkt dat er niet op alle punten een eenduidig beeld is over de genomen maatregelen. Zo is het niet duidelijk of tolken nog thuis mogen werken en is er geen duidelijkheid of er onderzoek wordt gedaan binnen de politie naar mogelijke vergelijkbare gevallen zoals de casus.

NCTV heeft een BIT en een stuurgroep ingesteld, de toegang tot staatsgeheime informatie is ingeperkt; NCTV voert zelf beperkt onderzoek uit.

N.a.v. de casus zijn binnen de NCTV een Beleidsincidenten Team (BIT) en een stuurgroep ingericht. Het BIT en de stuurgroep zijn gericht op de directe (operationele) consequenties en maatregelen voor de NCTV en de gevolgen van de casus voor de NCTV als werkgever. Het BIT heeft een feitenrelaas opgesteld. N.a.v. de casus zijn maatregelen getroffen die de toegang tot het staatsgeheime digitale archiefsysteem beperken. Per 1 november 2023 is het staatsgeheime digitale archiefsysteem afgesloten voor de meeste medewerkers van de NCTV. Slechts een klein aantal medewerkers heeft toegang tot het staatsgeheime digitale archiefsysteem behouden.
Verspreiding van Inlichtingenanalyses (IA's) en Inlichtingen-berichten (IB's) van de AIVD gebeurt op papier volgens een ingestelde procedure. IA's en IB's worden binnen de NCTV niet meer breed besproken, mondelinge toelichting gebeurt bij de AIVD. Deze maatregelen zijn bepaald door het BIT.

Communicatie over de casus heeft, voorafgaand aan het verspreiden van het ambtsbericht door de AIVD, mondeling plaatsgevonden aan de SG en de minister van JenV. De BVA is later op verschillende momenten geïnformeerd door de Rijksrecherche, de NCTV en de AIVD.

Geïnterviewden geven aan dat er meer aandacht wordt besteed aan het risico vanwege insider threat:

- In MT-besprekingen is meer aandacht geweest voor risicomanagement. In die gesprekken is o.a. bepaald dat een VGB als mitigerende maatregel niet voldoende is voor het beheersen van het risico vanwege insider threat.
- Er is meer aandacht voor de mogelijkheid dat medewerkers van de NCTV worden gerekruteerd door buitenlandse mogendheden. Dit gebeurt o.a. door het onderwerp te bespreken in Personeelsgesprekken.

Beheerders van het Stg.-net nemen maatregelen:

- Om te voorkomen dat niet-geregistreerde, zelf aangeschafte USB-sticks worden gebruikt op het Stg.-net, worden USB-sticks geregistreerd. Alleen geregistreerde USB-sticks kunnen worden gebruikt.
- Beheerders brengen nieuwe gebeurtenissen in kaart gebracht die voor monitoring in aanmerking komen.

De NCTV heeft een korte eigen verkenning uitgevoerd waaruit bleek dat de potentiële schade groot was, vanwege de ruime toegang die de analist had tot staatsgeheime informatie.

Er wordt onderzoek uitgevoerd door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), door de ADR en door het OM.
Het is een bewuste keuze van de Nationaal Coördinator om na de korte eigen verkenning zelf geen onderzoek uit te (laten) voeren. De Nationaal Coördinator heeft aangegeven dat de NCTV de ADR niet voor de voeten wil lopen en vertrouwt erop dat de AIVD signaleert of er vergelijkbare casussen zijn.

Bij de NCTV loopt een verbetertraject
De NCTV wil een nieuwe governance-structuur opzetten met een afdeling Risk & Compliance en de invulling van de rol van de CISO als belangrijke onderdelen. De focus ligt in eerste instantie op het opstellen van nieuwe opzet (documentatie). Nieuw beleid en onderliggende stukken zijn vastgesteld. Dit bestaat onder andere uit strategisch en tactisch IB-beleid, beleid voor risicobeheer en informatiebeveiligingsregels.

De risico-bereidheid is vastgesteld op 'risico-avers'. Verdere uitwerking in informatiebeveiligingsproducten volgt volgens geïnterviewden in de eerst helft van 2024 en implementatie in de tweede helft van 2024.

Er is een nieuwe set maatregelen bepaald. Nieuwe risicoanalyses kunnen aanvullende maatregelen aan het licht brengen (bijv. voor USB-sticks of printen vanaf Stg. Net). De NCTV geeft aan de risicomanagement-methodiek MASKeR te gebruiken op advies van het NCSC. De *Kwetsbaarheidsanalyse spionage* (van de AIVD) wordt niet toegepast.

Het Stg.-net mag door de NCTV weer worden gebruikt voor de verwerking van staatsgeheime informatie
De SG heeft het Stg.-net van de NCTV geaccrediteerd voor verwerking van gerubriceerde informatie t/m Staatsgeheim Geheim. Het betreft een tijdelijke toestemming (Interim Approval to Operate) die geldig is van 8 april 2024 t/m 8 april 2025. Hieraan zijn voorwaarden verbonden: het actueel houden van het maatregelenplan, het implementeren van de voorgestelde maatregelen, het monitoren van de voortgang en de afhandeling van de uitkomsten uit het risicomanagementproces.

Het staatsgeheime digitale archiefsysteem kan volgens NCTV weer gebruikt worden nadat nieuwe werkprocessen zijn beschreven, risico's zijn beoordeeld en nieuwe maatregelen zijn getroffen (compartimentering en een striktere toepassing van de toegangsrechten van gebruikers).

NCTV brengt registratie van USB-sticks op orde
NCTV werkt aan de verbetering van de registratie van USB-sticks door in kaart te brengen welke USB-sticks zijn uitgegeven, op voorraad liggen, zijn vermist of vernietigd.

Gedeeld beeld over verantwoordelijkheden van NCTV en BVA
NCTV en BVA geven aan inmiddels een gedeeld beeld te hebben over ieders rol en verantwoordelijkheden op het gebied van

integrale beveiliging waarbij het helder is over welke onderwerpen afstemming nodig is en wie welke verantwoordelijkheid heeft in processen zoals accreditatie en het aanwijzen van vertrouwensfuncties.

Wat te doen?

NCTV

- Stel vast dat het aspect insider threat met de gekozen aanpak voor risicoanalyse voldoende wordt meegenomen.
- Waarborg dat de casus maximaal wordt benut om ervan te leren.

Politie

- Zorg dat maatregelen die zijn/worden ingevoerd rondom de inzet van tolken breed bekend worden.

7. Verantwoording

7.1 Afbakening

Het object van onderzoek is het beveiligingsproces van staatsgeheime informatie bij de NCTV en vertrouwelijke informatie bij de politie. Het onderzoek is gericht op de processen die van toepassing zijn op de casus (de verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie) en systemen die een rol spelen in de casus.

Tijdens het vooronderzoek zijn meer details bekend geworden over de casus bij de NCTV en de politie. Dat heeft geleid tot de volgende afbakening

Afbakening	NCTV	Politie
Functies die bij het onderzoek worden betrokken	Nationaal Coördinator, leden van het MT NCTV CISO, BVC, Hoofd Bedrijfsvoering, Hoofd Informatiebeveiliging a.i. Manager en medewerkers van Afdeling Analyse Nationale Veiligheid Beheerders van IT-voorzieningen	Lid Korpsleiding, Concern Security Officer, CISO, CIO, directeur Informatievoorziening, [redacted] adviseur screening, [redacted] [redacted]
	BVA JenV	Cluster CTER: [redacted] Beheerders IT-voorzieningen
Systemen	Het staatsgeheime digitale archiefsysteem Het staatsgeheime digitale documentatiemanagement systeem	Het tapsysteem Summ-IT Het opnamesysteem
Aard van de Informatie	Informatie die is gerubriceerd als Staatsgeheim (conform VIRBI 2013).	Informatie die binnen CTER wordt behandeld als vertrouwelijk.

Inzoomen op personen

Met de opdrachtgever is overeengekomen dat er geen sprake is van een persoonsgericht onderzoek of integriteitsonderzoek. Bij de beantwoording van de onderzoeksvragen is, waar dat zinvol was, ingezoomd op de persoon die bij de NCTV in dienst was als analist en bij de politie werd ingehuurd als tolk/vertaler. De tweede persoon in de casus is niet betrokken in het onderzoek.

Toetsen van de inrichting van de PDCA-cyclus maar niet de werking

In dit onderzoek is 1-10-2023 als peildatum gehanteerd bij het in beeld brengen van de inrichting (de opzet en het bestaan) van de PDCA-cyclus voor de beveiliging van staatsgeheime of vertrouwelijke informatie. De bevindingen in dit rapport geven de stand van zaken weer op deze peildatum tenzij anders aangegeven.

Over het toetsen van de werking van de PDCA-cyclus is afgestemd tussen de opdrachtgever en de ADR op 4-4-2024. Na documentanalyse (bij NCTV en politie), interviews (bij NCTV en deels bij politie) en waarnemingen (bij NCTV) was het beeld van de ADR dat het toetsen van de werking van de PDCA-cyclus over de periode 1-10-2022 – 1-10-2023 niet mogelijk was. De reden hiervoor is het ontbreken van onderdelen van de opzet en/of het van de PDCA-cyclus (actuele set beveiligingsmaatregelen, aantoonbare implementatie van maatregelen, ingerichte interne controle en toezicht). Op basis daarvan heeft de opdrachtgever besloten het toetsen van de werking achterwege te laten.

7.2 Gehanteerde onderzoeksvragen

In het onderzoek zijn de volgende drie onderzoeksvragenvragen gehanteerd:

1. Op welke wijze hebben de NCTV en politie ingeregeld dat bijzondere informatie in de in deze casus gebruikte processen en systemen wordt behandeld conform de voorschriften van het VIRBI 2013 of de Rubriceringsregeling Politie 2015?
2. Welke bevindingen hebben wij bij de invulling van de relevante maatregelen in relatie tot deze casus?
3. Welke maatregelen kunnen waar nodig ter aanvulling of verbetering worden getroffen in de in deze casus gebruikte processen en systemen?

Op verzoek van de opdrachtgever zijn daarbij aanvullend drie elementen in het onderzoek meegenomen:

A. De berichtgeving over eerdere signalen en de opvolging daarvan.
B. De (on)wenselijkheid van samenloop van functies.
C. De maatregelen in geval van mogelijk misbruik.

7.3 Uitgevoerde werkzaamheden

Vooronderzoek

Na goedkeuring van de opdrachtbevestiging op 5 december 2023 is gestart met een vooronderzoek. Het vooronderzoek had drie doelen: duidelijkheid krijgen over de casus, samenstellen van een referentiekader en opstellen van een auditontwerp.
Tijdens het vooronderzoek is door de NCTV en de politie informatie opgeleverd over de casus en zijn enkele interviews gehouden.

Het concept referentiekader is op 31-1-2024 aan de opdrachtgever aangeboden voor een reactie. De opdrachtgever heeft het referentiekader besproken in de stuurgroep voor het onderzoek en het referentiekader voorgelegd aan BZK, NCTV, politie en het Openbaar Ministerie voor een reactie. Het referentiekader is op 4-4-2024 vastgesteld.

In de periode dat het concept referentiekader bij de opdrachtgever lag voor een reactie, is het onderzoek alvast van start gegaan. De op te leveren documentatie is afgestemd met NCTV en politie. Op basis van de door de ADR opgestelde lijst

met te interviewen functionarissen is een interviewplanning opgesteld voor interviews bij NCTV en politie.

Afstemming met OM
Op verzoek van het OM heeft het OM inzicht gekregen in de voor interviews geselecteerde medewerkers van de NCTV. Op basis daarvan is door het OM nagegaan of sprake was verstoring van het strafrechtelijk onderzoek door het onderzoek van de ADR. Dit heeft niet geleid tot wijzigingen in de voor interviews geselecteerde medewerkers van de NCTV.

Documentanalyse, interviews, analyse van feitenrelaas en waarnemingen
Om de onderzoeksvragen te kunnen beantwoorden zijn documenten geanalyseerd, zijn interviews gehouden met relevante functionarissen binnen beide onderzochte organisaties, is gebruik gemaakt van door beide organisaties opgestelde feitenrelazen en zijn bij beide organisaties waarnemingen gedaan.

Hoor wederhoor bevindingen
De resultaten van documentanalyse, interviews en waarnemingen zijn per organisatie samengevat en in mei 2024 (NCTV) en juni 2024 (politie) teruggelegd voor een reactie. Beide organisaties hebben een reactie gegeven op de bevindingen en over een deel van de bevindingen aanvullende informatie opgeleverd die door de ADR is verwerkt. NCTV en politie zijn geïnformeerd over de verwerking.

Hoor wederhoor concept rapport
De opdrachtgever en de ADR hebben in juli 2024 procesafspraken gemaakt over de oplevering van het concept-rapport en de wederhoor. Daarbij is afgesproken dat de opdrachtgever zes weken de tijd heeft om te reageren op het concept-rapport.

Het concept-rapport is op 30 augustus 2024 voor wederhoor opgeleverd aan de opdrachtgever. Op 14 oktober 2024 heeft de opdrachtgever gereageerd en de reacties van de NCTV, de politie, de BVA, het OM en de AIVD opgeleverd aan de ADR. Daarna heeft de ADR afgestemd met de NCTV, de politie, de BVA en de AIVD over de gemaakte opmerkingen. Over de reactie van het OM was geen verdere afstemming nodig.

Op 7 november 2024 heeft de ADR de versie "Concept na wederhoor" van het rapport opgeleverd aan de opdrachtgever. Bij het rapport is een overzicht opgeleverd van de verwerking van de opmerkingen van de NCTV, de politie, de BVA, het OM en de AIVD. Bij opmerkingen die niet zijn verwerkt, is aangegeven waarom deze niet zijn verwerkt.

Op 19 november 2024 hebben de NCTV, de politie en de AIVD aangegeven welke onderdelen in het rapport volgens hen niet geschikt zijn voor openbaarmaking. De ADR heeft op basis van deze reactie het volgende aangepast:

- namen van onderzochte systemen bij NCTV en politie;
- namen van de beleidsinterventieteams bij de politie;
- details over de samenstelling van de CTER-leiding.

Overige voorstellen van de politie en de AIVD voor het schrappen of aanpassen van passages in het rapport, zijn niet overgenomen.
Op verzoek van het OM is de tekst verduidelijkt over het in 2021 door de NRC gehouden interview met de NCTV.

Het definitieve rapport is op 29 november 2024 opgeleverd. De rubricering van het rapport is bij oplevering Stg. Geheim.

Afstemming met de opdrachtgever
Tijdens het onderzoek is het verloop op een aantal momenten besproken in een overleg tussen opdrachtgever en ADR.

7.4 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

7.5 Verspreiding van het rapport

De opdrachtgever, de pSG van JenV, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid en de uitzonderingsgronden voor het niet openbaar maken.

Ondertekening

Den Haag, 29-11-2024

w.g.

Projectleider
Auditdienst Rijk