

Vergaderjaar 2022–2023

29 628

Politie

Nr. 1124

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 oktober 2022

Op 29 september jl. heeft de vaste commissie voor Justitie en Veiligheid van uw Kamer verzocht om in een brief in te gaan op het tapsysteem van de politie, refererend aan het artikel in NRC «Opsporing komt in gevaar door disfunctioneren tapkamer politie». Hierbij kom ik aan dit verzoek tegemoet en bericht ik u over het tapsysteem en het kentekenvolgsysteem.

Ik merk dat er veel vragen zijn over diverse facetten rondom de tapkamer en interceptie. Ik ga in deze brief in op de invoering van het nieuwe tapsysteem en andere systemen op dit terrein, het proces van verwerving van het nieuwe tapsysteem en de impact hiervan op de operatie. Het lid Van Nispen van de SP-fractie vroeg mij daarnaast om specifiek in te gaan op de mogelijke veiligheidsrisico's die worden gelopen bij de huidige stand van de invoering van het nieuwe systeem. Hierop kan ik aangeven dat de korpsleiding van de politie mij heeft laten weten dat er bij de politie geen gevallen bekend zijn waarbij de veiligheid van politiecollega's of te beschermen personen in het geding is gekomen door storingen in het tapsysteem of het systeem waarin ANPR-informatie wordt verrijkt (i-trechter). Ook laat de politie mij weten dat er geen gevallen bekend zijn waarbij opsporingsonderzoeken schade hebben opgelopen vanwege storingen in deze systemen.

Implementatie nieuw tapsysteem

In eerdere brieven¹ heeft mijn ambtsvoorganger uw Kamer geïnformeerd over de aanschaf van het nieuwe tapsysteem. Het huidige systeem draait vanaf 2011.

Vanwege contractuele verplichtingen worden geen mededelingen gedaan over de naam van de leverancier van het huidige tapsysteem. Dit systeem werkt tot op de dag van vandaag, maar software en hardware zijn verouderd. Daarom is vanaf 2015 gestart met de verwerving van een

¹ Kamerstuk 29 628, nr. 920, Kamerstuk 29 628, nr. 890 en Kamerstuk 30 517, nr. 31.

nieuw tapsysteem. De aanbesteding is zeer zorgvuldig uitgevoerd en heeft enige tijd geduurd. Ten tijde van de start met de werving was er veel aandacht in de media en vanuit de Kamer voor het tapsysteem in verband met zorgen over de werking van het tapsysteem en beschikbaarheid van taps. Mede daardoor kostte de aanbesteding veel (doorloop)tijd. In 2016 zijn aanpassingen in het verwervingsproces doorgevoerd nadat de Tweede Kamer vragen had gesteld over het ingezette gesloten proces. Daarop is gekozen voor een open en een gesloten fase in het proces van de aanbesteding. De politie heeft bij de aanbesteding de Europese aanbestedingsregels in acht genomen. Dit maakte onder andere dat inschrijving ook voor partijen buiten Nederland openstond. Ik kan geen uitspraken doen over de bij de aanbesteding betrokken partijen en ook niet aangeven of er Nederlandse alternatieven bij de aanbesteding waren. Voorafgaand aan de aanbesteding is overwogen of de politie zelf een tapsysteem kon bouwen, waardoor zij ook zelf de volledige regie zou hebben op de toegang tot het systeem. Dit idee is snel verworpen omdat zelf bouwen van een tapsysteem zeer complex is, er goede alternatieven in de markt beschikbaar zijn, regie en toegangsvereisten meegenomen kunnen worden bij verwerving en de benodigde specifieke IV-expertise en -capaciteit van de politie begrensd is.

Bij brief van 1 juli 2019² is aan uw Kamer gemeld dat na een zorgvuldig traject conform Europese aanbestedingsregels de politie de opdracht gegund heeft aan het bedrijf Cyber Intelligence Ltd, dochterbedrijf van Elbit Systems uit Israël. Daarna bleek dat na de gunning Elbit Systems, het moederbedrijf van de leverancier, vanwege de overname van de firma IMI (eind 2018) door PAX werd aangemerkt als clustermunitieproducent. Voor Cyber Intelligence Ltd zelf geldt dat overigens niet.

In de brief van 1 juli 2019 aan uw Kamer is toen ook aangegeven dat de implementatie, en vervolgens de uitrol, tijd kost, omdat het complexe en gevoelige technologie betreft en de opsporing ondertussen door moet blijven gaan. De implementatie van een nieuw tapsysteem is een grote operatie waarbij het gaat om maatwerk. Systemen van een dergelijke omvang en complexiteit kennen dit soort doorlooptijden. Niet alleen worden alle technische omgevingen ingericht conform state of the art informatiebeveiliging, ook de koppelingen met de providers moeten worden ingericht, het moet voldoen aan de Nederlandse wet- en regelgeving, die bijvoorbeeld een geheimhoudersfilter nodig maakt. Het nieuwe tapsysteem beschikt over een uitbreidbare architectuur gericht op de toekomst, maakt het mogelijk om tapgegevens sneller en efficiënter te delen binnen de politie en voldoet tevens aan hogere veiligheidseisen.

Na gunning van de aanbesteding in 2019, volgde een periode van een jaar van specificatie in detail van het nieuwe systeem. Daarbij was in die periode de benodigde inzet van specialistische politiemedewerkers schaars en niet altijd (tijdig) beschikbaar voor de implementatie. Na aankoop bleek ook dat een nieuwe versie van het systeem beschikbaar kwam. Gelet op de meerwaarde die dat bood heeft de politie bewust gekozen voor deze versie, daarbij acceptierend dat dit tot vertraging in het implementatieproces zou leiden. In 2020 is gestart met de bouw van het nieuwe systeem, tijdens de Corona-pandemie, wat met grote regelmaat beperkingen met zich meebracht in samenwerkingsmogelijkheden en eveneens de invoering vertraagde. In 2020³ heeft mijn ambtsvoorganger gemeld dat vanwege de complexiteit van het gehele project de implementatie tot ten minste 2022 zal gaan duren. Als huidige planning kan ik melden dat de implementatie gefaseerd zal plaatsvinden vanaf eind dit

² Kamerstuk 29 628, nr. 890.

³ Kamerstuk 29 628, nr. 948.

jaar. Dan verwacht de politie de productieomgeving klaar te hebben. Daarna volgt een zorgvuldige stapsgewijze implementatie die naar verwachting nog heel 2023 zal vergen.

De stapsgewijze overgang verloopt via een migratiestrategie. Tijdens de migratie worden lopende taps per onderzoek overgezet naar het nieuwe systeem. Hiervoor wordt een natuurlijk moment gebruikt, namelijk het zetten van een tap binnen een onderzoek of het verlengen hiervan. In 2023 worden op deze wijze alle taplijnen naar het nieuwe systeem overgezet en zal uiteindelijk aan het einde van 2023 het huidige tapsysteem niet meer in gebruik zijn. Hierna wordt het oude systeem gearchiveerd en zal het worden uitgezet en afgevoerd.

Met deze stapsgewijze aanpak worden gefaseerd gebruikers toegevoegd. Omdat de werkbaarheid voor rechercheurs en de integriteit van de gegevens voorop staat kiest de politie niet voor een big bang voor de circa 10.000 gebruikers van verschillende organisaties die uiteindelijk van dit systeem gebruik zullen maken. Op dit moment vinden diverse tests plaats. Testen met de eindgebruikers zijn thans in voorbereiding, daarna zijn testen in de praktijk voorzien. Ik hecht eraan te benadrukken dat het huidige systeem operationeel blijft totdat het nieuwe systeem volledig is geïmplementeerd. Ook 2023 zal nog in het teken staan van verdere uitrol. Voor 2023 is ook de oude leverancier gecontracteerd zodat zowel het oude als het nieuwe systeem beschikbaar is tijdens de overgang.

Hierna zal ik ingaan op de beveiliging en technische en personele aspecten die in het krantenartikel zijn genoemd.

Beveiliging

In mijn brief van 16 februari jl.⁴ heb ik de beveiligingsmaatregelen toegelicht op het huidige en het nieuwe tapsysteem. Met betrekking tot het tapsysteem zijn afspraken gemaakt en beheersmaatregelen genomen zodat de leverancier geen toegang heeft tot gevoelige locaties en ICT-systemen. Dit is ook het geval tijdens de implementatie van het tapsysteem. In het contract met de leverancier zijn diverse eisen opgenomen over de logging. Verder voert de politie periodiek pentesten uit, onder meer op veiligheid en ongewenst netwerkverkeer en «achterdeurtjes».

Technische aspecten

In het NRC-artikel worden storingsmeldingen genoemd en zorgen geuit over de betrouwbaarheid van het huidige systeem, verlies van data en de veiligheid die daarmee samenhangt. Het huidige systeem dateert uit 2011 en functioneert, maar is end-of-life. Dit is de reden voor vervanging.

Elk ICT-systeem heeft te maken met verstoringen of verminderde beschikbaarheid op bepaalde functionaliteit. Het huidige tapsysteem heeft geregeld storingen van wisselende impact. Het systeem wordt continu gemonitord op werking en continuïteit. In de afgelopen drie maanden is het huidige tapsysteem drie keer niet beschikbaar geweest door een «prio1-storing». Daarnaast is er drie keer gepland onderhoud aan het systeem gepleegd. Gepland onderhoud wordt tijdig aan de opsporings-teams gemeld zodat het team dit gegeven kan betrekken in haar onderzoek. Bij dataverlies wordt proces-verbaal opgemaakt dat gevoegd kan worden in een strafdossier.

⁴ Kamerstuk 29 628, nr. 1069.

Prio1-storingen zijn storingen waarbij (delen van) systemen onbeschikbaar zijn.

De politie registreert meer soorten storingen, namelijk prio's 1 t/m 4. Dat zijn er in aantallen meer. Bij kleinere dan prio1-storingen is er geen verminderde beschikbaarheid van het systeem, maar is er tijdelijk minder functionaliteit beschikbaar, bijvoorbeeld sprekerherkenning, problemen met een enkele taplijn of een printknopje doet het even niet. Deze storingen komen vaker voor en zijn vervelend, maar zorgen dus niet voor systeemuitval en in de regel ook niet voor dataverlies. Niet-prio1 storingsmeldingen worden gewogen en geprioriteerd op basis van de ernst daarvan (impact en urgentie).

Dataverlies door prio1-storingen is naar verhouding gering. Behalve dat het verlies gering is, is het verlies ook bekend. En in een onderzoek is nooit alle mogelijke data beschikbaar: zo worden bijvoorbeeld niet alle telefoons getapt en wordt niet alles geobserveerd. Rechercheurs werken met de gegevens die er zijn. Wanneer dataverlies voorkomt wordt dit ook vastgelegd in een proces-verbaal en bekend gemaakt aan het opsporingsteam.

Daarbij benadruk ik dat tappen een belangrijk middel in de opsporing is, maar slechts een van de hulpmiddelen in een onderzoek. Dit geldt ook voor automatische kentekenplaatherkenning.

In het krantenartikel wordt gesteld dat het kentekensysteem niet goed werkte ten tijde van de gevonden wapens in een auto bij het huis van de Belgische Minister van Justitie en tijdens Prinsjesdag. Hierover kan ik aangeven dat er geen sprake was van een storing in de automatische kentekenplaatherkenning (ANPR). Het systeem waarin ANPR-informatie wordt verrijkt (i-trechter) kende wel een verstoring. Deze storing was bekend en heeft zoals hiervoor aangegeven niet tot problemen geleid voor de veiligheid. Naast dat er dan wordt gewerkt aan een oplossing, wordt de operatie in kennis gesteld zodat daar eventueel passende maatregelen genomen kunnen worden.

Bij een storing op de i-trechter is de data van ANPR gewoon beschikbaar en kan deze gebruikt worden (eventueel ook achteraf) voor analyse. Als de i-trechter stoort, dan wordt dit gemeld aan de opsporings- en bewakingsdiensten en het operationele centrum. Deze diensten zijn in staat met deze kennis andere middelen in te zetten waardoor de opsporing of de beveiliging gewaarborgd blijft.

Een ander systeem dat genoemd wordt in het artikel in NRC betreft Replay. Replay is ontwikkeld vanaf 2003 en werd ingezet om IP-data te analyseren op basis van de toenmalige standaard voor de aanlevering van telecomgegevens door aanbieders. Het toenmalige tapsysteem kon dat toen nog niet. Replay is enkele jaren geleden al operationeel uitgefaseerd omdat telecomaandbieders zijn overgegaan op een andere standaard en deze functionaliteit in het huidige systeem is opgenomen. Voor cold cases blijft Replay beschikbaar omdat de politie beschikt over een eeuwigdurende licentie. Overigens is Replay weliswaar in Nederland ontwikkeld, maar inmiddels is de ontwikkeling op deze software gestopt en bovendien is al enige tijd onderdeel van een Amerikaanse firma die zich vooral richt op cybersecurity.

Over het Replay systeem is eerder niet gecommuniceerd aan de Tweede Kamer. De politie volgt de reguliere verwervings- en aanbestedingsprocedures en die worden niet standaard gecommuniceerd aan de Tweede Kamer. Sinds 2019 is de politie aangesloten op het stelsel van het Adviescollege ICT-toetsing voor projecten met een ICT-component van meer dan 5 miljoen euro. Via deze toetsing wordt de Kamer geïnformeerd.

Alle andere bijzonderheden, bijvoorbeeld bij hoog risico, meldt de politie via reguliere rapportages. Op basis van de rapportages van politie kan mijn ministerie besluiten de Kamer te informeren. Daarbij wordt terughoudend omgegaan met het publiek maken van de gebruikte systemen met het oog op veiligheidsrisico's.

Personele aspecten

In het krantenartikel wordt ook gerefereerd aan slechte verhoudingen bij de afdeling interceptie en sensing. Ik betreur deze situatie.

De korpsleiding laat mij weten dat er veel speelt binnen de afdeling en er ook diverse signalen zijn ontvangen over de werking van de systemen. In relatie tot de totale verbeteringen binnen de Landelijk Eenheid wordt ook bij deze afdeling ingezet op goed leiderschap en medewerkerschap. De interne verhoudingen zijn onderkend, bespreekbaar gemaakt en er wordt gewerkt aan een afdelingsbrede veranderaanpak, vooruitlopend en in lijn met de veranderingen zoals voorgesteld door de commissie Schneiders.

Dit past naadloos in de transitie van de Landelijke Eenheid om meer focus te richten op de uitvoering van specialistische taken. De leiding van de Landelijke Eenheid neemt de zorgen van medewerkers serieus en bespreekt deze in alle openheid met teams waar dit aan de orde is. Dit geldt ook voor de afdeling interceptie en sensing.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius