Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2317

Vragen van het lid **Van Dam** (CDA) aan de Minister van Justitie en Veiligheid over *het bericht «OM Eist 45 maanden cel tegen corrupte aspirant-agent»* (ingezonden 7 maart 2019).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 17 april 2019) Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 2093

Vraag 1
Kent u het artikel «OM Eist 45 maanden cel tegen corrupte aspirant-agent»?[1]

Antwoord 1
Ja.

Vraag 2 en 3
Kunt u uitleggen tot welke informatie aspirant-agenten toegang hebben? Verschilt dit per eenheid of is de informatietoegankelijkheid voor (aspirant-) agenten gestandaardiseerd?
Hoe kan het dat een aspirant-agent toegang had tot vertrouwelijke informatie uit lopende opsporingsonderzoeken?

Antwoord 2 en 3
Politiemedewerkers en dus ook aspiranten worden pas geautoriseerd voor politiesystemen wanneer de screening is afgerond. Deze screening betreft het betrouwbaarheids- en geschiktheidsonderzoek bij de aanstelling. Op 21 maart 2019 heb ik uw Kamer een wetsvoorstel aangeboden in verband met het verruimen van dit onderzoek. Aspirant-agenten voeren tijdens hun opleiding ook politietaken uit en hebben daarvoor toegang tot de informatie die zij op basis van hun rol nodig hebben. Het gaat daarbij om gebiedsgebonden politiezorg (GGP).
Het autorisatiebeleid is een aantal jaren geleden vernieuwd en geldt voor de gehele politieorganisatie. Met dit autorisatiebeleid is gekozen voor role based access, een systeem waarbij medewerkers bij het aanloggen op basis van hun functie en rollen toegang krijgen tot applicaties en gegevens. Door een koppeling met het personeelssysteem kan gezorgd worden dat de autorisaties op basis van profielen (rollen) ieder moment worden toebedeeld op basis van

[1] De Volkskrant, 5 maart 2019, https://www.volkskrant.nl/nieuws-achtergrond/om-eist-45-maanden-cel-tegen-corrupte-aspirant-agent~ba290b9d/

ah-tk-20182019-2317
ISSN 0921 - 7398
's-Gravenhage 2019

de meest actuele informatie. Deze functionaliteit zal ook bij ieder nieuw politie-informatiesysteem van toepassing zijn. Ook hanteert de politie sinds januari 2016 het vierogen-principe, waarbij de aanvraag voor een autorisatie boven een bepaald niveau door een extra leidinggevende wordt getoetst. Naast deze technische voorzieningen heeft de politie ook allerlei sociale voorzieningen getroffen op het gebied van integriteit en opleiding. Het blijft belangrijk om medewerkers van de politie weerbaarder te maken en te houden, bijvoorbeeld door bewustwordingsmaatregelen. De afdeling VIK heeft een Toolkit Preventie geïntroduceerd met daarin verschillende middelen die helpen bij het met elkaar praten over, en leren van, dilemma's, integriteitsrisico's en best practices in het dagelijks werk. In januari 2019 heb ik de Kamer een brief gestuurd over deze activiteiten van de afdeling VIK.[2] Daarnaast gaan teamchefs en Operationeel Experts naar een leiderschapstraining en heeft de politie de theatervoorstelling «Rauw» ontwikkeld. De voorstelling is een belangrijk element in de bewustwordingscampagne hoe om te gaan met onder meer politie-informatie

Vraag 4
Hoe wordt gemonitord wie, wanneer, welke informatie uit lopende opsporingsonderzoeken bekijkt? Wordt dat überhaupt gemonitord? Verschilt dat per politie-informatiesysteem?

Antwoord 4
Van het gebruik van systemen worden *log-files* bijgehouden, dit gebeurt veelal in afzonderlijke systemen. Zo kan achteraf worden bekeken wie toegang heeft gehad tot welke informatie. Als daar aanleiding voor is kan in opdracht van het bevoegde gezag binnen de politie, de betreffende *logging* door een interne afdeling (Veiligheid Integriteit en Klachten, VIK) nader worden bekeken. De politie voegt de afzonderlijke logging-systemen samen in één nieuw systeem waarmee centraal kan worden bijgehouden wie welke informatie heeft geraadpleegd. De interne auditafdeling monitort of het logging-systeem aanwezig is en functioneert.
Binnen één politie-eenheid vindt een pilot plaats om atypisch gebruik van informatie te detecteren en zo mogelijk ongeoorloofd raadplegen van informatie te signaleren. Daarover heb ik u in november 2018 geïnformeerd in het halfjaarbericht Politie.[3] De pilot richt zich op de ontwikkeling van het logging-model en de governance daaromtrent, evenals op proactiever signaleren. Afwijkend gedrag van gebruikersaccounts kan zo vroegtijdig worden opgepikt.
Proactief signaleren van atypisch gebruik van informatie heeft tevens een preventieve werking. Door in een vroeg stadium met medewerkers in gesprek te gaan kan een misverstand uit de weg worden geruimd, een probleem worden opgelost, misbruik worden voorkomen en gedrag tijdig worden aangepast.
Signalen van (mogelijk) ongeoorloofd raadplegen van informatie tijdens de pilot worden opgevolgd.
Op basis van de uitkomsten en ervaringen van de pilot kan voor alle politie-informatiesystemen met gevoelige informatie een betrouwbaar en effectief systeem worden geïmplementeerd om misbruik en oneigenlijk gebruik (near) real time op te kunnen sporen. In dit traject is ook de ondernemingsraad betrokken.

Vraag 5
Is het waar dat er momenteel (meerdere) nieuwe politie-informatiesystemen in aanbouw zijn? Zo ja, welke? Hoe wordt bij die nieuwe informatiesystemen geborgd dat vertrouwelijke informatie uit opsporingsonderzoeken niet zomaar te raadplegen is?

Antwoord 5
In het ICT-vernieuwingsprogramma Vernieuwend Registreren worden de operationele systemen vernieuwd om daarmee de ondersteuning van de werkprocessen van de politie gebruiksvriendelijker te maken. Hierover heb ik

[2] Kamerstuk 28 844, nr. 166
[3] Kamerstuk 29 628, nr. 825

de Kamer in september 2018 een brief gestuurd met daarin de aanpak van deze vernieuwing.[4] Inmiddels is gestart met de proces «Afhandeling van winkeldiefstal». Ook zullen functionaliteiten van legacy-systemen, waaronder BVH en Summ-IT, worden vervangen dan wel volledig worden vernieuwd binnen het programma Vernieuwend Registreren.
Om zicht te houden op het gebruik van de systemen worden alle systemen aangesloten op de Logging as a Service (LaaS) omgeving. De wijze van logging wordt daarmee geüniformeerd.
De politie hanteert het privacy en security by design-principe. Dat betekent dat bij de aanschaf/ontwikkeling van elke nieuwe applicatie of nieuw systeem er al tijdens het ontwerp wordt nagedacht over de bescherming van de informatie daarin. Voor het laatste deel van deze vraag betreffende autoriseren verwijs ik u naar het antwoord op vraag 2 en 3.

[4] Kamerstuk 29 628, nr. 787