Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

Aanhangsel van de Handelingen

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

660

Vragen van het lid **Gerkens** (SP) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie over *een medewerker van de Politieacademie die buiten functie is gesteld.* (Ingezonden 30 september 2009)

1
Is het bericht waar dat een 33-jarige medewerker van de Academie Politie Amsterdam-Amstelland buiten functie is gesteld vanwege het ongeoorloofd toegang verschaffen tot digitale systemen?[1] Wat was hiervan de exacte reden?

2
Tot welke systemen had de medewerker toegang?

3
Hoe vaak heeft de medewerker de systemen onrechtmatig gebruikt? Met welk doel?

4
Om wat voor gegevens ging het? Waarvoor heeft de medewerker de gegevens gebruikt?

5
Hoe is de politie achter het misbruik van de systemen gekomen?

6
Kunt u uitsluiten dat de systemen vaker onrechtmatig gebruikt worden door medewerkers? Zo nee, hoeveel gevallen zijn u bekend?

7
Hoe wordt misbruik van de systemen voorkomen? Waarom is het deze medewerker toch gelukt? Moet er volgens u een betere beveiliging van de systemen komen? Waarom wel/niet?

[1] Nu.nl, 29 september 2009: «Medewerker Amsterdamse politie buiten functie gesteld» http://www.nu.nl/algemeen/2091609/medewerker-politieacademie-buiten-functie-gesteld.html

Antwoord

Antwoord van minister **Ter Horst** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de minister van Justitie (ontvangen 16 november 2009)

1
Het is juist dat de politie Amsterdam-Amstelland een medewerker van de Academie Politie Amsterdam-Amstelland buiten functie heeft gesteld. Reden voor de buitenfunctiestelling is de verdenking dat betrokkene anders dan voor de uitoefening van de politietaak de politiële systemen heeft bevraagd én de verdenking dat betrokkene de aldus verkregen informatie anders dan voor de uitoefening van de politietaak heeft gebruikt. Dat levert een verdenking op van overtreding van artikel 272 (schending ambtsgeheim) van het Wetboek van Strafrecht.
Ter zake de overtreding van dit misdrijf wordt onder verantwoordelijkheid van de Officier van Justitie een opsporingsonderzoek ingesteld.
Artikel 84 lid 2 van het Besluit algemene rechtspositie politie bepaalt dat politieambtenaren buiten functie kunnen worden gesteld in afwachting van een eventuele schorsing.
Gedurende de buitenfunctiestelling worden geen werkzaamheden verricht en hebben dergelijke politieambtenaren van het korps Amsterdam-Amstelland geen toegang tot politiegebouwen en -systemen.

2
De toegang tot politiesystemen wordt verleend op basis van een geprotocolleerd autorisatieproces. Daarbij wordt aan de hand van nut en noodzaak voor het werk en vooraf gedefinieerde criteria bepaald of een medewerker toegang tot informatie krijgt. Gelet op de opgedragen werkzaamheden is betrokkene toegang verleend tot de volgende politiesystemen: X-pol. FIT, HKS, Papos en NSIS-List.
In het kader van een onderzoek door het College Bescherming Persoonsgegevens (CBP) naar de

KVR38351
2009Z17657
0910tkkvr660
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2009

invoering van de Wet politiegegevens (WPG) bij de infodesk van het korps is onlangs vastgesteld dat deze autorisatieprocedure de toets der kritiek goed kan doorstaan.

3
In het onderzoek wordt gekeken naar de bevragingen van de politiële systemen en het gebruik van de daardoor verkregen informatie. In het belang van het onderzoek kunnen daarover verder geen mededelingen worden gedaan.

4
Omdat de gedragingen van betrokkene onderwerp zijn van een lopend strafrechtelijk onderzoek kan in dit stadium slechts zeer beperkt antwoord gegeven worden. Het onjuist gebruik van informatie, waaronder ook wordt begrepen het anders dan voor de uitoefening van de opgedragen werkzaamheden bevragen van systemen, wordt als een ernstige schending van de integriteit opgevat. Dergelijke meldingen worden adequaat en voortvarend onderzocht.

5
Een melding van een derde is de directe aanleiding geweest dit onderzoek in te stellen.

6
Ongeoorloofd gebruik van de systemen kan nooit worden uitgesloten. Wel spant de politie Amsterdam-Amstelland zich in om dit zoveel mogelijk te voorkomen. Zie hiervoor verder de beantwoording van vraag 7. Het bevragen van de politiële systemen en/of het gebruik van politiële informatie anders dan voor de uitoefening van de functie heeft in het korps Amsterdam-Amstelland in 2007 16 maal tot een disciplinair besluit geleid, in 2008 4 maal en in 2009 tot op heden 5 maal.

7
De medewerker was regulier geautoriseerd voor de toegang tot het primaire informatiesysteem. Hij heeft in dat systeem informatie opgevraagd zonder dat er een dienstbelang mee gemoeid was. Vervolgens heeft hij deze informatie anders dan voor de uitoefening van de hem opgedragen taak gebruikt. Het korps stelt vanuit een integrale visie op beveiliging ieder jaar een werkplan op voor de verbetering van de beveiliging en het daaraan verbonden gedrag van de medewerkers.
Naast het bij vraag 2 genoemde autorisatieprotocol zijn ook andere maatregelen, in de loop van de tijd, aan het beveiligingsconcept toegevoegd.
a) Reeds vier jaar wordt een bewustwordingscampagne gevoerd. Hierin wordt onder de aandacht gebracht hoe om te gaan met informatie en op welke wijze de eigen verantwoordelijkheid ten aanzien van informatiebeveiliging wordt vormgegeven. Aan de hand van verschillende praktijkvoorbeelden worden de medewerkers geïnformeerd over dilemma's, eerdere misstappen van collega's, beslismomenten en risico's in de omgang met en het gebruik van informatie.
b) In het verlengde van bovengenoemde campagne is in 2007 een verkennend onderzoek verricht naar indicatoren voor lekken/misbruik van informatie binnen het korps. De beschreven indicatoren worden onder de aandacht gebracht van de leidinggevenden.
c) Alle korpsleden hebben een dilemmatraining integriteit gevolgd, waarbij het boek «Integriteit in teams» is uitgereikt. In dit boek is casuïstiek beschreven betreffende lekken en misbruik van politie-informatie, aan de hand van zaken die zich in de praktijk hebben voorgedaan.
d) Alle handelingen in de politie systemen worden gelogd waardoor achteraf is na te gaan welke handelingen zijn verricht. Medewerkers worden preventief gewezen op deze logging om te zorgen dat zij zich daardoor nog extra bewust zijn dat zij slechts zakelijk gebruik mogen maken van de opgeslagen informatie.
e) Het aanmoedigen van sociale controle op de werkplek die er op gericht is dat medewerkers elkaar aanspreken op het juiste gebruik van informatie en dilemma's daaromtrent voorleggen aan hun leidinggevende. In combinatie met de bewustwording wordt duidelijk gemaakt dat vrijwillige professionele toetsing een belangrijke bijdrage levert aan informatiebeveiliging.
f) Voorlichting aan nieuwe lichtingen politiemedewerkers over beveiliging van informatie, hun eigen verantwoordelijkheid en de noodzaak zich te conformeren aan de regels en normen op dit gebied.
g) Voor toegang tot politie-informatie en de daarbij behorende systemen is een opleidingseis van toepassing die zorgt dat medewerkers het middel op de juiste wijze kunnen toepassen.
De beveiligingsmaatregelen zijn zodanig ingericht dat de oordeelvorming van de medewerker een belangrijk aspect vormt bij het juist toepassen van de informatie. De brede toegang tot toezicht-, handhavings- en noodhulpinformatie is noodzakelijk om het werk naar behoren uit te kunnen voeren. De brede toegang is nodig om de volgende punten te voorkomen:
a. Gevaarzetting voor burgers en politiemedewerkers omdat cruciale informatie ontbreekt als opgetreden moet worden.
b. Irritatie bij burgers omdat telkens om dezelfde informatie wordt gevraagd of men (de politie) niet eens weet heeft van andere relevante incidenten.
c. Onoordeelkundig optreden van politiemedewerkers die niet of niet afdoende op de hoogte zijn van relevante informatie.
In de opsporingssystemen is specifieke informatie aanwezig die een gevoeliger karakter draagt. Daar is de afweging gemaakt, en de organisatorische mogelijkheid aanwezig, wel aanvullende maatregelen in te bouwen. De algemene toegang wordt beperkt tot de opgedragen onderzoek(en) en de daaraan verbonden informatie.