Ministerie van Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Bestuurlijke en Juridische Zaken

Schedeldoekshaven 100
2511 EX Den Haag
Postbus 20301
2500 EH Den Haag
www.justitie.nl

Ons kenmerk
5625692/09

Uw kenmerk
2009Z17067

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 3 november 2009
Onderwerp Beantwoording Kamervragen van het lid Gerkens (SP) over het CIOT-informatiesysteem

In antwoord op uw brief van 23 september 2009 deel ik mee, mede namens mijn ambtgenote van Binnenlandse Zaken en Koninkrijksrelaties, dat de schriftelijke vragen van het lid Gerkens (SP) van uw Kamer over het CIOT-informatiesysteem (ingezonden 23 september 2009) worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Minister van Justitie,

Antwoorden van de Minister van Justitie, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties op vragen van het lid Gerkens (SP) over het CIOT-informatiesysteem. (Ingezonden 23 september 2009, 7720)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Bestuurlijke en Juridische Zaken

Datum
3 november 2009

Ons kenmerk
5625692/09

1
Is het waar dat de Structured Query Language (SQL)-server van het informatiesysteem van het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) 250.000 vragen per maand krijgt, en dus zo'n 3.000.000 zoekopdrachten per jaar telt? 1)

Antwoord vraag 1
Het aantal vragen verschilt per maand. In 2008 bedroeg het totale aantal vragen iets meer dan 2,8 miljoen. Tot en met september van 2009 zijn 2.276.865 vragen gesteld.

2
Welke organisaties komen in aanmerking om gebruik te mogen maken van CIOT-
Informatiesysteem? 2) Hoe wordt dit bepaald en door wie? Welke wettelijke basis bestaat hiervoor?

Antwoord vraag 2
Op basis van het Besluit verstrekking gegevens telecommunicatie zijn opsporingsdiensten, de AIVD en de MIVD verplicht gebruik te maken van het CIOT informatiesysteem. Daarnaast kunnen een bevoegde autoriteit en een aanbieder gezamenlijk beslissen om gebruik te maken van het informatiepunt. In overleg met aanbieders en de alarmcentrales 112 is besloten de alarmcentrales toegang te verlenen tot het CIOT informatiesysteem in het geval van misbruik en levensbedreigende situaties.

3
Worden medewerkers van die instanties getoetst op integriteit voor zij inlogbevoegdheden krijgen? Zo nee, waarom niet? Zo ja, door wie wordt dit getoetst en hoe vaak? Vinden er periodiek hertoetsingen plaats van toegekende bevoegdheden? Zo nee, waarom niet?

Antwoord vraag 3
De leiding van een opsporings- of veiligheids- en inlichtingendienst draagt een medewerker voor om toegang te verkrijgen tot het CIOT-systeem. Dit gebeurt op basis van het Besluit verstrekking gegevens telecommunicatie. De medewerkers worden in het kader van het ambt dat zij bekleden getoetst op integriteit. De verantwoordelijkheid daarvoor ligt bij de respectievelijke opsporings- of inlichtingen- en veiligheidsdienst. Er vindt geen aanvullende integriteitstoets door het CIOT plaats. Ook de verantwoordelijkheid van de periodieke hertoetsing van de toegekende bevoegdheden ligt bij de opsporings- of veiligheids- en inlichtingendienst. Op basis van het Besluit algemene rechtspositie politie is een antecedentenonderzoek verplicht bij de aanstelling van aspiranten, bijzondere ambtenaren van politie en vrijwillige ambtenaren van politie. Voor de Bijzondere Opsporingsdiensten geldt in deze de Wet op de Bijzondere Opsporingsdiensten en het Besluit bekwaamheid en betrouwbaarheid opsporingsambtenaren bijzondere opsporingsdiensten. Bij de inlichtingen- en veiligheidsdiensten betreft het een

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Bestuurlijke en Juridische Zaken

Datum
3 november 2009

Ons kenmerk
5625692/09

veiligheidsscreening in de zin van de Wet Veiligheidsonderzoeken. Deze screening wordt elke vijf jaar herhaald.

4
Hoe is de verbinding naar CIOT-informatiesysteem beveiligd? Hoe is de site zelf beveiligd?

Antwoord vraag 4
De verbinding naar het CIOT-informatiesysteem is beveiligd met het HyperText Transfer Protocol Secure (https). De website van het CIOT-informatiesysteem is alleen te benaderen vanaf vaste werkplekken binnen het (interne) Politie/Justitie-netwerk. Dit wordt onder meer afgedwongen door middel van firewalls en routers. Verder kan opgemerkt worden dat het Politie/Justitie-netwerk aanvullende beveiligingsmaatregelen kent, waaronder extra encryptie op de (interne) verbindingen.
De website van het CIOT-informatiesysteem is beveiligd met beveiligingsmaatregelen die aan een externe audit zijn onderworpen. Het gaat hier om fysieke beveiligingsmaatregelen, autorisatie beveiligingsmaatregelen, antivirus beveiligingsmaatregelen en aanvullende netwerkmaatregelen.
Daarnaast organiseert het CIOT samen met de politie een gebruikerscursus waarin het gebruik van het systeem wordt uitgelegd, alsmede de borging van het bevragingsproces in de administratieve organisatie van de politie. Informatiebeveiliging en rechtmatigheid van bevragen staan hierbij centraal.

5
Komt het vaak voor dat wachtwoorden 'weggegeven' worden? Is hier toezicht op? Zo ja, hoe is dit georganiseerd? Zo nee, waarom niet?

Antwoord vraag 5
Nee, dat is voor zover bekend slechts in een enkel geval gebeurd. In de audit van 2008 is er sprake van één korps dat zich niet heeft gehouden aan de opgestelde veiligheidsmaatregelen. Correctieve maatregelen zijn getroffen en deze situatie bestaat niet meer. Overigens is het weggeven van wachtwoorden niet voldoende om toegang te krijgen tot het CIOT- informatiesysteem. Zo moet men fysiek toegang hebben tot de beveiligde werkplek en toegang hebben tot het account van de aangewezen opsporingsambtenaar.

6
Deelt u de mening dat de manier waarop de audit op onrechtmatige verzoeken op dit moment uitgevoerd wordt volstrekt ontoereikend is? Deelt u de mening dat juist de feitelijke zoekopdrachten onderwerp van onderzoek moeten zijn en niet of de bevragingen al dan niet aan een onderzoek gekoppeld zijn? Zo ja, bent u bereid de auditprocedure aan te passen? Zo nee, waarom niet?

Antwoord vraag 6
De audit richt zich op de rechtmatigheid van bevraging. Verder moet het korps in de audit aantonen dat de gestelde vragen rechtmatig waren op basis van dossiers. Zo moeten er, onder meer, processenverbaal van vordering en verstrekking aanwezig zijn. Ik deel de mening dat de feitelijke zoekopdrachten onderwerp van onderzoek moeten zijn, alsmede het bevragingsproces zoals dat is ingericht. Dit is nu ook steeds het geval.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Bestuurlijke en Juridische Zaken

Datum
3 november 2009

Ons kenmerk
5625692/09

7
Heeft u een schatting hoeveel van die 3.000.000 zoekopdrachten worden gebruikt voor zaken die niets met het onderzoek te maken hebben? Bent u bereid dit nader te onderzoeken? Zo nee, waarom niet?

Antwoord vraag 7
In de auditrapporten is slechts een geval vastgesteld waarbij een zoekopdracht niet gerelateerd kon worden aan een onderzoek. Het betrof de audit over 2008. In dat jaar kon in een geval geen dossier getoond worden waardoor er geen relatie gelegd kon worden tussen de bevraging en een onderzoek. De bevindingen uit het auditrapport hebben geleid tot het uitzetten van verbeteracties door politie en justitie. De huidige audits zijn voldoende en ik acht een nader onderzoek daarom niet nodig.

1) Hackblog.nl
http://www.hackblog.nl/89-ciot-cis-de-telefoongids-overheid.html
2) Ministerie van Justitie, Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)
http://www.justitie.nl/onderwerpen/opsporing_en_handhaving/ciot/