

35 925 VI Vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2022

Nr. 146 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 10 mei 2022

Op grond van artikel 8 van het Besluit verstrekking gegevens telecommunicatie wordt de werking van het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) jaarlijks gecontroleerd aan de hand van audits¹. Met deze brief bied ik u conform het tweede lid van dit artikel een verslag aan van drie van deze audits. Het betreft audits die zijn uitgevoerd naar het beheer van het informatiepunt in de periode 2018-2020 en het gebruik van het informatiepunt door de opsporingsdiensten in 2019.

Aanleiding

Het Centraal Informatiepunt Onderzoek Telecommunicatie zorgt ervoor dat opsporings-, inlichtingen- en veiligheidsdiensten snel kunnen achterhalen wie de gebruiker is van een bepaald telefoonnummer, e-mailadres of IP-adres. Zo kan bijvoorbeeld worden onderzocht met wie een verdachte heeft gesproken in de aanloop naar een misdrijf of wie verantwoordelijk is voor het verspreiden van illegaal materiaal op het internet. Het informatiepunt is ondergebracht bij de Justitiële Informatiedienst en werkt als doorgeefluik tussen de telecomaانبieders en de bevragende dienst. Aanbieders stellen dagelijks bepaalde klantgegevens ter beschikking die – mits wordt voldaan aan de wettelijke voorwaarden – via het informatiesysteem van het informatiepunt kunnen worden doorgeleid aan een bevragende dienst.² Het informatiepunt heeft zelf geen inzage in of toegang tot de gegevens van telecomaانبieders of de bevragingen van de voorgenoemde diensten.

Het opvragen van gegevens via het CIOT-informatiesysteem geschiedt op basis van wettelijke bevoegdheden, zoals die in het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten. Ook gelden voor het informatiesysteem voorschriften die zijn vastgelegd in het Besluit verstrekking gegevens telecommunicatie (het Besluit). Het doel van de audits is om vast te stellen of dit Besluit goed wordt uitgevoerd door de opsporingsdiensten, de telecomaانبieders en de beheerders van het informatiepunt.

Met deze brief ontvangt u het verslag van de volgende audits:

1. Het onderzoek van de Auditdienst Rijk naar het beheer van het informatiepunt in 2018, 2019 en 2020
2. Het onderzoek van de Auditdienst Rijk naar het gebruik van het informatiepunt door de FIOD, ISZW en KMar in 2019
3. Het onderzoek van de Concernaudit Politie naar het gebruik van het informatiepunt door de politie in 2019

¹ Raadpleegbaar via www.tweedekamer.nl

² In het Besluit verstrekking gegevens telecommunicatie is vastgelegd welke klantgegevens door aanbieders beschikbaar worden gesteld. Het gaat o.a. om de naam, adres, type aansluiting, e-mailadres, telefoonnummer en IP-adres van de klant. Nadrukkelijk worden er geen gegevens verstrekt over de inhoud van het telecommunicatieverkeer, noch metadata over het verkeer of locatiegegevens anders dan het geregistreerde adres van de klant.

U treft de resultaten van deze audits aan als bijlage bij deze brief³. Conform de afspraken in de ministerraad, zijn de rapporten van de Auditdienst Rijk tevens openbaar gemaakt op de website van de rijksoverheid.

In een brief van 15 december 2020 is uw Kamer geïnformeerd over de inhaalslag die momenteel wordt uitgevoerd met betrekking tot de audits.⁴ Met deze brief bied ik u de eerste rapporten in het kader van deze inhaalslag aan. Ook de audits naar de politie en de (bijzondere) opsporingsdiensten over de periode 2020 zijn inmiddels voltooid en zullen na bespreking met de Commissie van Advies van het informatiepunt met uw Kamer worden gedeeld. Verder worden op dit moment met de Auditdienst Rijk afspraken gemaakt over de resterende aanbiedersaudit en de jaarlijkse audits met betrekking tot 2021.

Belangrijkste bevindingen

Audit beheer 2018-2020

De Auditdienst Rijk heeft aan de hand van een normenkader onderzoek gedaan naar het beheer van het CIOT-informatiesysteem door het informatiepunt in de jaren 2018, 2019 en 2020.

Op basis van dit onderzoek en met inachtneming van de aanbevelingen van de auditdienst ben ik van mening dat de beheersmaatregelen bij het informatiepunt toereikend zijn om de risico's op inbreuken op beveiliging of integriteit van de informatie-uitwisseling te beperken.

Uit het onderzoek is gebleken dat het informatiepunt voor de jaren in de scope van het onderzoek verbetering laat zien zowel in het vastleggen en formaliseren van maatregelen als het aantoonbaar voldoen aan de beheersnormen. Onder meer wordt daarbij verwezen naar een in 2019 opgesteld en geformaliseerd logbeleid en de tijdig met securityupdates bijgewerkte servers. Ook is in de onderzochte periode een procedure vastgelegd waarin per gegevenssoort bewaartermijnen worden geformaliseerd en de bewaartermijn van bevragingen is teruggebracht van vijf naar drie jaar conform het Besluit.

Wel zijn mogelijkheden voor verbetering aangekaart voor het versterken van de interne procesbeheersing, alsook op het gebied van versleuteling en het accountbeheer. Het informatiepunt heeft mij in reactie op de bevindingen laten weten de aanbevelingen over te nemen en dat waar nodig reeds verbeteracties zijn ingezet. Enkele bevindingen wil ik nader toelichten:

De auditdienst heeft in haar rapportage mogelijkheden voor verbeteringen aangekaart voor het definitief vastleggen van documentatie en het inrichten van controle en monitoring, o.a. op interne accounts en de analyse van de logging. Het informatiepunt neemt de aanbeveling van de auditdienst over en zal de documentatie met betrekking tot interne accounts actualiseren.

Voor wat betreft de versleuteling van gegevens wordt geconstateerd dat verbindingen naar het informatiepunt worden versleuteld, maar dat dit in één geval niet gebeurt conform de richtlijn van het Nationaal Cyber Security Centrum. Inmiddels is de aanbeveling van de auditdienst opgevolgd door ook deze server conform de richtlijn te configureren. Verder stelde de auditdienst vast dat de

³ Raadpleegbaar via www.tweedekamer.nl

⁴ Kamerstuk 35 570 VI, nr. 90

server die het klantenbestand ontvangt van de telecomaanhouders is ingesteld om niet-versleutelde verbindingen te kunnen ontvangen. Het informatiepunt laat weten dat inmiddels een wijziging heeft plaatsgevonden waarmee dit niet langer mogelijk is. Hierbij wordt benadrukt dat het klantenbestand reeds voorafgaand aan verzending door de telecomaanhouders wordt versleuteld, en dat het versleutelen van de verbinding een extra schil van bescherming vormt.

Afsluitend stelt de auditdienst vast dat gegevens in de interne databases en de CIOT-applicatieserver niet worden versleuteld. Hierbij wordt opgemerkt dat deze gegevens worden opgeslagen in de beveiligde omgeving van het informatiepunt – een afgeschermd omgeving voor de verwerking van vertrouwelijke gegevens. Het informatiepunt neemt desondanks de aanbeveling over om een risicoanalyse uit te voeren over de noodzaak van encryptie voor deze gegevens.

Voorts heeft de auditdienst vastgesteld dat er in 2020 zes accounts voorkwamen in de omgeving van het informatiepunt met beheerdersrechten die niet terug te vinden waren in de meest recente autorisatiematrix, waarmee de toestemming voor deze rechten wordt vastgesteld. Het betreft de accounts van twee medewerkers en vier serviceaccounts voor geautomatiseerde beheerstaken. Het informatiepunt laat weten dat voor één van de accounts nadien is gebleken dat het een voormalige beheerder van het CIOT-informatiesysteem betreft die is overgestapt op een nieuwe functie binnen het informatiepunt. Deze medewerker voert op verzoek en met instemming van de organisatieleiding incidenteel nog beheerstaken uit en beschikt daarom om legitieme redenen om beheerdersrechten. De andere vijf accounts waren ten tijde van de audit reeds uitgeschakeld en niet toegankelijk, maar kwamen nog voor in de gebruikerslijst. Conform de aanbeveling van de auditdienst zijn de beheerdersrechten voor deze accounts ingetrokken.

Audit FIOD, ISZW en KMar 2019

In het kader van het onderzoek naar de goede uitvoering van het Besluit door de gebruikers van het CIOT-informatiesysteem heeft de Auditdienst Rijk onderzoek uitgevoerd bij de bijzondere opsporingsdiensten FIOD, ISZW en KMar. Het doel van dit onderzoek was om inzicht te verkrijgen in de rechtmatigheid van de bevestigingen van het CIOT-informatiesysteem.

In het onderzoek wordt geconstateerd dat bij 73 van de 75 onderzochte bevestigingen de rechtmatigheid kon worden vastgesteld op basis van een onderliggende vordering met een geldige grondslag. Bij één van de overige bevestiging kon de rechtmatigheid niet worden aangetoond omdat de onderliggende vordering niet kon worden gevonden vanwege de verhuizing van de betrokken afdeling. Verder is geconstateerd dat gebruikers van het CIOT-informatiesysteem niet altijd zijn aangewezen door het bevoegd gezag in de eigen organisatie, en dat door een procedurefout bij één partij 17 bevestigingen foutief in het informatiesysteem zijn geregistreerd. Afsluitend is geconstateerd dat de onderzochte diensten allen periodieke controles uitvoeren over hun bevestigingen, maar dat niet in alle gevallen sprake is van rapportage daarover aan het bevoegd gezag of het informatiepunt.

De FIOD, ISZW en KMar hebben mij laten weten zich in de bevindingen te herkennen en de verbeteringen door te voeren. Op basis van dit onderzoek en de toegezegde opvolging van de bevindingen ga ik ervan uit dat de onderzochte diensten de juiste maatregelen hebben ingezet om de rechtmatigheid van bevestigingen te waarborgen.

Audit Nationale Politie 2019

Voorts heeft de Concernaudit Politie een onderzoek uitgevoerd naar de mate waarin in 2019 door de politie is voldaan aan wet- en regelgeving en afspraken verbonden aan de uitvoering van de bevraging van de klantgegevens van telecom- en internetbedrijven via het informatiepunt. De politie gebruikt deze informatie voor opsporingshandelingen en, zoals ik uw Kamer reeds heb geïnformeerd,⁵ in 2019 nog bij noodhulpverlening door de 112-meldkamers en in uitzonderlijke gevallen ten behoeve van haar taken in het kader van de Wet verplichte geestelijke gezondheidszorg.

Uit de auditrapportage blijkt dat de politie op een groot aantal punten voldoet aan geldende wet- en regelgeving en de vastgelegde afspraken met het informatiepunt. Wel zijn afwijkingen geconstateerd met betrekking tot het controleren van de opsporingsbevoegdheid, de bewaartermijn van spoedbevragingen en de inzet van het informatiepunt ten behoeve van noodhulpverlening.

Blijkens het auditonderzoek was in 2019 nog sprake van een werkwijze waarbij de aanwijzing van medewerkers van de politie met toegang tot het CIOT-informatiesysteem jaarlijks achteraf werd bekrachtigd door de korpschef. Eveneens zijn in twee gevallen bevragingen geconstateerd waarbij de opsporingsbevoegdheid van de betrokken gebruiker was verlopen. Het gaat hierbij vermoedelijk om administratieve tekortkomingen. Deze situatie is geadresseerd door invoering van een nieuwe landelijke procedure, op grond waarvan de aanwijzingen van nieuwe gebruikers op voorhand geschiedt en een eenduidige controle is ingericht op de opsporingsbevoegdheid. Deze nieuwe procedure is op 19 mei 2020 in werking getreden.

Verder is geconstateerd dat de documentatie voor spoedbevragingen van het CIOT-informatiesysteem, die namens de regionale eenheden worden uitgevoerd door de afdeling Interceptie en Sensing van de Landelijke Eenheid, in veel gevallen niet kon worden teruggevonden. In het huidige onderzoek zijn zes deelwaarnemingen aan het licht gekomen waarbij documentatie ontbreekt. De politie heeft mij laten weten de aanbeveling van de Concernaudit over te nemen om zorg te dragen voor adequate dossiervorming en monitoring op deze bevragingen.

In eerdere verslagen van audits is uw Kamer geïnformeerd over de bevraging van het CIOT-informatiesysteem door de 112-meldkamers ten behoeve van de noodhulpverlening en de Wet verplichte geestelijke gezondheidszorg. Hierover kan ik u melden dat de beschikbaarheid van de benodigde gegevens voor de 112-meldkamers inmiddels is gerealiseerd. Hiermee zijn de naam, adres, woonplaats en postcode van bellers direct zichtbaar voor de meldkamer en komt de bevraging van deze gegevens via het informatiepunt te vervallen.

Voorts is de wetswijziging die gaat voorzien in een specifieke wettelijke grondslag voor bevragingen van het CIOT-informatiesysteem in het kader van de Wet verplichte geestelijke gezondheidszorg in voorbereiding. Ik verwacht deze spoedig in procedure te kunnen brengen. Hierbij zijn ook de ministeries van Economische Zaken en Klimaat en van Volksgezondheid, Welzijn en Sport betrokken.

Publicatie jaarcijfers

⁵ Kamerstuk 35 570 VI, nr. 90.

Het Centraal Informatiepunt Onderzoek Telecommunicatie publiceert, conform de wettelijke verplichting, jaarlijks cijfers over het aantal afgehandelde informatieverzoeken. Dit gebeurt door publicatie van een rapport van de cijfers via de website www.rijksoverheid.nl. Sinds 2015 worden deze cijfers met het verschijnen van het jaarverslag van het Ministerie van Justitie en Veiligheid gepubliceerd.

Ik blijf met de beheerder en de bevrogende diensten van het CIOT-informatiesysteem in gesprek om te borgen dat de in de audits geconstateerde verbetermogelijkheden tijdig en volledig worden opgepakt.

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