Bijlage I: Opzet en methodiek

Bij het toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

CTIVD nr. 70

[vastgesteld op 19 augustus 2020]

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 70

BIJLAGE I

Bij het toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD

Opzet en methodiek

Opzet van het onderzoek

In deze bijlage licht de CTIVD toe wat de opzet en methodiek is van het onderzoek naar het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD.

Het onderzoek beslaat de periode van 1 mei 2018, de datum van inwerkingtreding van de Wiv 2017, tot 1 november 2019.

De CTIVD geeft met dit onderzoek antwoord op onderstaande onderzoeksvragen:

- *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze uitvoering gegeven aan de hackbevoegdheid bij het verzamelen van bulkdatasets ('bulkhacks')?*
- *Hebben de AIVD en de MIVD in de onderzoeksperiode op rechtmatige wijze bulkdatasets uit de hackbevoegdheid verwerkt?*

Bij de eerste onderzoeksvraag richt het onderzoek zich op een aantal onderdelen bij de uitoefening van de hackbevoegdheid die nieuw zijn in de Wiv 2017. Hierbij zijn de volgende deelvragen te onderscheiden:

- Vond het verzamelen van bulkdatasets met de hackbevoegdheid in de onderzoeksperiode plaats op basis van een door de TIB rechtmatig bevonden verzoek tot toestemming?
- Zijn de technische risico's die zich bij de inzet van de hackbevoegdheid kunnen voordoen in de toestemmingsverzoeken in overeenstemming met de praktijk omschreven?
- Hebben de diensten aan de opruimverplichting voldaan?
- Hebben de diensten van de uitvoering van de hackbevoegdheid aantekening gehouden?

De tweede onderzoeksvraag is te preciseren aan de hand van de volgende deelvragen:

- Hoe gaan de AIVD en de MIVD om met de wettelijke eisen met betrekking tot de relevantiebeoordeling ex. artikel 27 Wiv 2017?
- In hoeverre geven de AIVD en de MIVD uitvoering aan procedurele waarborgen voor de verdere verwerking van bulkdatasets die via een hack zijn verzameld?

Afbakening van het onderzoek

De hiervoor genoemde onderzoeksvragen hebben betrekking op verschillende fases, namelijk enerzijds het verzamelen van bulkdatasets via de hackbevoegdheid (art. 45 Wiv 2017) en anderzijds de verdere verwerking van deze gegevens door de AIVD en de MIVD. Het onderzoek richt zich op het beleid, de werkinstructies en de praktijk (namelijk de in de onderzoeksperiode uitgevoerde bulkhackoperaties en de verdere verwerking van de daarmee verzamelde gegevens) van de diensten. Het gaat om elf door de TIB in de onderzoeksperiode goedgekeurde operaties, naast vier afgewezen operaties. Eén operatie is in de loop van de onderzoeksperiode goedgekeurd en later bij verlenging alsnog in de onderzoekersperiode afgekeurd. De CTIVD heeft deze operaties geïdentificeerd op basis van eigen onderzoek en door de beide diensten aangeleverde informatie. Nu het onderzoek zich richt op hackoperaties die een bulkdataset hebben opgeleverd, betekent dit dat niet alle uitgevoerde hackoperaties noch alle aanwezige bulkdatasets in het onderzoek zijn betrokken.

Verzamelen van gegevens

Voor wat betreft de onderzoeksvragen die gaan over de rechtmatigheid van de inzet van de hackbevoegdheid (verzamelfase) in de praktijk, heeft de CTIVD ervoor gekozen het onderzoek toe te spitsen op die onderdelen van artikel 45 Wiv 2017 die nieuw zijn. Het gaat specifiek om:

- De toestemming van de minister en voorafgaande rechtmatigheidstoetsing door de TIB (lid 3 jo. art. 32). In de Wiv 2017 vormt de toetsing van de TIB een belangrijke waarborg voor rechtmatige inzet. De TIB toetst de noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid van de inzet van de hackbevoegdheid.
- Het omschrijven van technische risico's in het verzoek om toestemming, waaronder het gebruik van onbekende kwetsbaarheden (lid 4). Daarbij wordt ook interne afweging en verslaglegging van risico's betrokken.
- De naleving van de opruimplicht na beëindiging van een operatie (lid 7).

Verder richt het onderzoek zich voor wat betreft de verwervingsfase op de wijze van opvolging van de aanbeveling uit rapport nr. 53 over het houden van aantekening van de uitoefening van de bevoegdheid (thans artikel 31 Wiv 2017), waaronder geautomatiseerde logging.[1] De rechtmatigheidstoetsing door de TIB als zodanig is geen onderdeel van dit onderzoek.

Verdere verwerking

Voor wat betreft de verdere verwerking van bulkdatasets uit de hackbevoegdheid ligt de nadruk op de (procedurele) waarborgen die gelden bij de toegankelijkheid van deze gegevens voor het inlichtingenproces. Het wettelijke aanknopingspunt vormt het vereiste van beoordelen op relevantie en de daarvoor geldende bewaartermijn (krachtens artikel 27 Wiv 2017). Ook heeft de CTIVD aandacht voor de wijze van uitvoering van de door de diensten gehanteerde waarborgen. Hierbij betrekt zij de wijze van opvolging van de door de ministers overgenomen aanbevelingen uit rapport nr. 55. In het huidige onderzoek is niet onderzocht op welke wijze de gegevens uit de bulkdatasets in het inlichtingenproces worden gebruikt. Ook is niet onderzocht in hoeverre de bulkdatasets werkelijke betekenis hebben voor de uitvoering van de onderzoeken van de diensten (en of de inbreuk op fundamentele rechten opweegt tegen het belang van de diensten). Deze vraag is verdisconteerd in de afwegingen en motivering van de vereisten van noodzakelijkheid en proportionaliteit in de verzoeken om toestemming en eventuele verlengingsaanvragen waarin de opbrengst voor het onderzoek moet worden gemotiveerd.

1 Toezichtsrapport van de CTIVD nr. 53 (gepubliceerd april 2017) over de inzet van de hackbevoegdheid door de AIVD en de MIVD, Kamerstukken II 2016/17, 29 924, nr. 149 (bijlage), beschikbaar op www.ctivd.nl.

Onderzoeksmethodiek

De CTIVD heeft een juridisch toetsingskader opgesteld om het beleid c.q. de werkinstructies en de praktijk van het verzamelen van bulkdatasets met inzet van de hackbevoegdheid en de waarborgen bij de verdere verwerking ervan te kunnen toetsen. Het kader is gebaseerd op de Wiv 2017 en de beleidsregels, de parlementaire geschiedenis, relevante jurisprudentie, eerdere toezichtsrapporten en door de ministers van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) en van Defensie in dat verband overgenomen aanbevelingen. Ook het interne beleid van beide diensten is bij het opstellen van het kader in aanmerking genomen. Het toetsingskader is opgenomen in Bijlage II bij het toezichtsrapport.

De CTIVD heeft dossieronderzoek verricht. Daarbij zijn beleidsdocumenten en werkinstructies beoordeeld. Ook is onderzocht welke waarborgen gelden bij de toegankelijkheid van deze verkregen bulkgegevens voor het inlichtingenproces. Het wettelijke aanknopingspunt vormt het vereiste van beoordelen op relevantie en de daarvoor geldende bewaartermijn (krachtens artikel 27 Wiv 2017). Daarnaast hanteren de diensten bepaalde waarborgen.

Verder zijn alle aanvragen tot toestemming en verlengingen van de in de onderzoeksperiode vallende bulkhackoperaties bekeken.

Tijdens het onderzoek zijn interviews met juristen, beleidsmedewerkers en operationele medewerkers van de beide diensten gehouden. Deze gesprekken zijn gevoerd om een beter beeld te krijgen van het handelen en het werkproces van de diensten en ter verificatie van de onderzoeksresultaten. Voor de bestudering van het verzamelen, ontsluiten en verder verwerken van de gegevens zijn ook gesprekken gevoerd met technische experts.

Verder heeft de CTIVD zelf technisch onderzoek gedaan in de systemen van de diensten. Daartoe maakte de cybersecurity-expert van de CTIVD deel uit van de onderzoeksgroep. De CTIVD heeft alle bulkhackoperaties in de onderzoeksperiode in de breedte (technisch) onderzocht en beoordeeld op het punt van het rechtmatig verzamelen van bulkdatasets, de beschrijving van technische risico's, de vastlegging van de uitvoering van de opruimverplichting (voor zover aan de orde) en de aanwezigheid van (geautomatiseerde) logging van de hackbevoegdheid. Daarnaast is door middel van een technische steekproef bij een aantal operaties een nadere verdieping in het onderzoek aangebracht. Hierbij is nader gekeken naar de kwaliteit en reikwijdte van de logging en de technische risico's van operaties. Dit levert op deze punten een representatief beeld op van de uitvoeringspraktijk van bulkhacks in de onderzoeksperiode.

Doorlooptijd

Op 11 september 2019 heeft de CTIVD aangekondigd een rechtmatigheidsonderzoek te verrichten naar de toepassing van de hackbevoegdheid bij het verzamelen van bulkdatasets door de AIVD en de MIVD.[2] Het onderzoek is met het opstellen van het concepttoezichtsrapport afgerond op 10 juni 2020. De ministers van BZK en van Defensie zijn in de gelegenheid gesteld te reageren op de in het concepttoezichtsrapport opgenomen bevindingen. De reacties van de ministers van BZK en Defensie zijn op 14 augustus 2020 ontvangen. Het toezichtsrapport is op 19 augustus 2020 vastgesteld.

2 Zie www.ctivd.nl.

Oranjestraat 15, 2514 JB Den Haag
Postbus 85556, 2508 CG Den Haag

T 070 315 58 20
E info@ctivd.nl | www.ctivd.nl