Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Verslag toezicht wettelijke hackbevoegdheid politie 2020

Heeft de politie zich aan de regels gehouden bij het toepassen van de bevoegdheid tot binnendringen in een geautomatiseerd werk?

Inhoudsopgave

Voorwoord

Dit is het tweede verslag waarin de Inspectie Justitie en Veiligheid (hierna: de Inspectie) rapporteert over de inzet van de bevoegdheid door de politie om een geautomatiseerd werk dat in gebruik is bij een verdachte, heimelijk en op afstand binnen te dringen en hier onderzoek in te doen. Deze wettelijke hackbevoegdheid is geïntroduceerd met de inwerkingtreding van de Wet Computercriminaliteit III (Wet CCIII) op 1 maart 2019. De behoefte aan deze bevoegdheid ontstond door de toegenomen digitalisering van vele criminaliteitsvormen, waarbij andere opsporingsbevoegdheden vaak ontoereikend bleken te zijn. Bij het toepassen van de hackbevoegdheid maakt de politie inbreuk op de persoonlijke levenssfeer van de verdachte en mogelijk van derden. Toezicht is van belang om vast te stellen of de politie hierbij wet- en regelgeving juist toepast en naleeft zodat kan worden vertrouwd op een zorgvuldige en rechtmatige toepassing van deze bevoegdheid door de politie.

De Inspectie rapporteert in dit verslag over de inzet van de hackbevoegdheid door de politie in de periode 1 januari 2020 tot en met 31 december 2020. In 2020 is het eerste verslag gepubliceerd over de periode 1 maart 2019 tot en met 31 december 2019.[1]

Ondanks beperkingen door coronamaatregelen is de politie in 2020 verder gegaan met de doorontwikkeling van de hierbij gehanteerde werkprocessen in deze juridisch en technisch complexe omgeving.

De Inspectie wil met haar verslag bijdragen aan het lerend vermogen van de politie. Daarnaast kunnen de bevindingen van de Inspectie als input dienen voor de evaluatie van de effectiviteit van de Wet CCIII die momenteel wordt uitgevoerd. Het uitblijven van verbetering, waardoor voor het tweede opvolgende jaar dezelfde bevindingen moeten worden geconstateerd, beschouw ik als een risico. Het is zaak dat de politie uit onze verslagen lessen trekt en zelf tot verbeteringen komt. De Inspectie hoopt, evenals in 2019 en 2020, ook in 2021 van de politie een constructieve en open houding te ervaren bij de uitoefening van het toezicht op deze belangrijke bevoegdheid.

H.C.D. Korvinus
Inspecteur-generaal Inspectie Justitie en Veiligheid

[1] https://www.inspectie-jenv.nl/Publicaties/rapporten/2020/08/20/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019.

Samenvatting

Sinds 1 maart 2019 mag de politie apparaten hacken die in gebruik zijn bij een verdachte. De introductie van deze bevoegdheid heeft maatschappelijk tot veel discussie geleid, waarbij bleek dat er spanning bestaat tussen enerzijds het belang van veilige samenleving en anderzijds het recht op privacy. Hierbij werd gesteld dat de politie de hackbevoegdheid nodig heeft voor het bestrijden van de steeds meer gedigitaliseerde criminaliteit. Tegelijkertijd was er bezorgdheid dat de politie te pas en te onpas binnendringt in systemen en op grote schaal de privacy van burgers schendt. Daarnaast zouden veiligheidsrisico's kunnen ontstaan als de politie kwetsbaarheden laat bestaan, in plaats van deze bij de producent te melden. Ook werd opgemerkt dat een hack door de politie kan leiden tot nevenschade, bijvoorbeeld aan de digitale infrastructuur.

Om een rechtmatig en zorgvuldige inzet van de hackbevoegdheid te waarborgen, mag de politie deze alleen toepassen binnen strikte voorwaarden die in wet- en regelgeving zijn vastgelegd. Zo mag de politie pas binnendringen in een apparaat na toetsing door de rechter-commissaris en uitsluitend op bevel van de officier van justitie. Ook voor wat betreft de uitvoering door de politie zijn allerlei eisen gesteld, bijvoorbeeld aan de logging en de wijze waarop het bewijs wordt vastgelegd. De Inspectie ziet toe of de politie zich aan de regels houdt.

Dit is het tweede jaar dat de Inspectie Justitie en Veiligheid verslag doet over het toezicht op de hackbevoegdheid van de politie. De bevoegdheid is in 2020 op bevel van de officier van justitie in 14 zaken ingezet. Gelet op deze betrokkenheid van de officier van justitie en dit aantal zaken, is van een ongecontroleerde inzet op grote schaal geen sprake. Evenmin is in 2020 iets gebleken van nevenschade, of van veiligheidsrisico's door het in stand houden van kwetsbaarheden. Dit neemt niet weg dat de uitvoering van de hackbevoegdheid door de politie volgens de Inspectie voor het tweede jaar op rij niet geheel voldoet aan het rechtskader. De logging is net als in 2019 incompleet en ook beschikt de politie nog steeds niet over een goed functionerend intern kwaliteitssysteem. In haar eerste verslag heeft de Inspectie laten meewegen dat de bevoegdheid nieuw was en dat het betreffende team van de politie zich nog in een opbouwfase bevond. De Inspectie had verwacht dat in 2020 meer verbetering zichtbaar zou zijn, het uitblijven hiervan baart de Inspectie zorgen. Daarnaast is in 2020 in bijna alle zaken gebruik gemaakt van commerciële software waarbij de leverancier toegang heeft zonder dat de politie dit kan beperken en controleren. De Inspectie concludeert dat hierdoor risico's niet kunnen worden uitgesloten voor wat betreft de betrouwbaarheid van met de hackbevoegdheid verkregen bewijs en de privacy van de betrokkenen. In 2021 continueert de Inspectie haar toezicht dan ook met dezelfde diepgang en aanpak, met een focus op de inmiddels voor de tweede keer gesignaleerde tekortkomingen.

1 Aanleiding en aanpak onderzoek

1.1 Aanleiding en doelstelling

Op 1 maart 2019 is de Wet Computercriminaliteit III (Wet CCIII) in werking getreden. De Wet CCIII introduceert de bevoegdheid voor de politie om een geautomatiseerd werk (bijvoorbeeld een laptop of een smartphone) dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen.[2] In de volksmond wordt deze bevoegdheid de 'hackbevoegdheid' genoemd. De bevoegdheid mag uitsluitend worden ingezet in geval van verdenking van een ernstig of specifiek aangewezen misdrijf, georganiseerde criminaliteit of aanwijzingen van een terroristisch misdrijf.[3]

De wetgever hecht grote waarde aan een rechtmatige en zorgvuldige inzet van deze bevoegdheid en heeft daarom voorzien in een stelsel van maatregelen van controle en toezicht. Als onderdeel van dat stelsel is een belangrijke rol weggelegd voor de Inspectie. De Inspectie is op grond van de Politiewet 2012 als rijksinspectie belast met het toezicht op de kwaliteit van de taakuitvoering door de politie. Het toezicht door de Inspectie op de uitvoering van het bevel en de naleving van de wet- en regelgeving rond de toepassing van de bevoegdheid door de politie is verder verankerd in het Wetboek van Strafvordering en het besluit onderzoek in een geautomatiseerd werk (hierna: Bogw of het Besluit).[4]

Voor de toepassing van de bevoegdheid voor het onderzoek in een geautomatiseerd werk is het van belang dat de politie dat doet binnen de daarvoor gestelde wettelijke regels en voorschriften. Het toezicht door de Inspectie op de naleving van deze regels en voorschriften heeft mede tot doel om risico's te signaleren en om de politie aan te zetten tot verbetering.

Het eerste verslag van de Inspectie over de bevindingen van het toezicht op de toepassing van de hackbevoegdheid is vorig jaar gepubliceerd.[5] Dat verslag betrof de periode 1 maart 2019 tot en met 31 december 2019.

1.2 Afbakening

Het toezicht van de Inspectie is gericht op het functioneren van het wettelijk systeem rond het toepassen van de hackbevoegdheid door de politie.[6] Toepassing van deze bevoegdheid door de politie moet plaatsvinden binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris. De

[2] Daar waar in dit verslag de 'bevoegdheid' of 'hackbevoegdheid' wordt genoemd, wordt gedoeld op de bevoegdheid om een geautomatiseerd werk dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen.
[3] Zie artikel 126nba, 126uba en 126zpa Wetboek van Strafvordering.
[4] Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in artt. 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Stb. 2018, 340.
[5] https://www.rijksoverheid.nl/documenten/rapporten/2020/08/20/tk-bijlage-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019.
[6] Zie Nota van Toelichting bij het Besluit onderzoek in een geautomatiseerd werk dat op 9 oktober 2018 in het Staatsblad is gepubliceerd (Stb. 2018, nr. 340), p 23.

toetsing en oordeelsvorming door de officier van justitie en de rechter-commissaris valt buiten de reikwijdte van het toezicht door de Inspectie.[7]

Het systeemtoezicht heeft ook betrekking op de inzet van de bevoegdheid in gevallen die niet leiden tot een strafvervolging. [8] [9]

De uitvoering van de hackbevoegdheid door de politie is centraal belegd bij één technisch team: het Digital Intrusion Team (DIGIT) van de Landelijke Eenheid van de Nationale Politie. Naast politieambtenaren kunnen opsporingsambtenaren van de Koninklijke marechaussee en opsporingsambtenaren van de bijzondere opsporingsdiensten onderdeel vormen van dit team. In 2020 heeft dit team in 14 zaken bevel gekregen voor toepassing van de wettelijke hackbevoegdheid.[10] De Inspectie heeft toezicht gehouden op al deze inzetten.

In 2020 heeft DIGIT daarnaast uitvoering gegeven aan bevelen vanuit het buitenland, op basis van de regelgeving aldaar op twee geautomatiseerde werken die zich daar bevonden. De politie heeft hier niet gehandeld op basis van de hackbevoegdheid vanuit de Wet CCIII. Deze zaken vallen daarom buiten de reikwijdte van dit toezicht door de Inspectie.

In het Wetboek van Strafvordering is aangegeven dat bij de toepassing van de hackbevoegdheid al dan niet gebruik kan worden gemaakt van een technisch hulpmiddel.[11] Een technisch hulpmiddel is een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel. De minister van JenV heeft de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) tot 1 maart 2022 aangewezen als keuringsdienst voor het uitvoeren van keuringen van technische hulpmiddelen voor het uitoefenen van de hackbevoegdheid. De Inspectie houdt tevens toezicht op de naleving van de regels en procedures voor de keuring en inzet van technische hulpmiddelen.

In 2020 is in de media veel aandacht geweest voor het EncroChat onderzoek. Zowel de politie als het Openbaar Ministerie hebben aangegeven dat in dit onderzoek geen sprake is geweest van de inzet van de hackbevoegdheid door Nederlandse opsporingsambtenaren. Ook deze zaak valt daarom buiten de reikwijdte van dit toezicht door de Inspectie.

De Inspectie rapporteert in dit verslag over het handelen van de politie in de periode 1 januari 2020 tot en met 31 december 2020.

---

[7] Tweede Kamer, vergaderjaar 2017-2018, 34 372 nr.27 p.13. "De uitkomst van de oordeelsvorming van de officier van justitie of de rechter-commissaris over de proportionaliteit van het inzetten van de bevoegdheid in een specifieke zaak valt buiten deze toetsing. Het oordeel over dergelijke beslissingen is vooraleerst voorbehouden aan de rechter ter terechtzitting en – op grond van diens bevoegdheid uit hoofde van artikel 122 van de Wet op de rechterlijke organisatie – de procureur-generaal bij de Hoge Raad."

[8] Systeemtoezicht is een benadering van de onder toezicht staande waarbij in het toezicht gebruik wordt gemaakt van de eigen activiteiten van deze onder toezicht staande die gericht zijn op het systematisch vergroten van de eigen kwaliteit en regelnaleving. Het betreft al het toezicht waarbij de opzet, reikwijdte en werking van (kwaliteits)systemen en (bedrijfs)processen bij organisaties worden vastgesteld.

[9] *Kamerstukken II* 2016-2017, 34 372, nr. 6, p. 81-83.

[10] Artikel 126nba/126uba/126zpa Wetboek van Strafvordering.

[11] Artikel 126nba/126uba/126zpa lid 1 Wetboek van Strafvordering.

1.3 Onderzoeksaanpak

De Inspectie heeft per inzet van de hackbevoegdheid door DIGIT de aanpak gereconstrueerd op basis van beschikbare logging, documentatie en gesprekken met de teamleiding van DIGIT en leden van het technisch team. Daarnaast heeft de Inspectie onderzoek verricht naar diverse zaak-overstijgende aspecten, zoals de logging en de beveiliging van de technische infrastructuur van DIGIT.

Ook is de Inspectie nagegaan of de keuringsdienst de eisen uit het wettelijk kader heeft nageleefd bij het keuren van technische hulpmiddelen. Deze keuringen zijn uitgevoerd door TNO als aangewezen keuringsdienst omdat de keuringsdienst van de Landelijke Eenheid van de politie in 2020 niet beschikte over voldoende capaciteit en expertise.

Ook is de Inspectie nagegaan of de keuringsdienst de eisen uit het wettelijk kader heeft nageleefd bij het keuren van technische hulpmiddelen.

De Inspectie heeft zich bij de beoordeling van de inzet van de hackbevoegdheid gebaseerd op het toepasselijke rechtskader:

- Wetboek van Strafvordering;
- Het Besluit onderzoek in een geautomatiseerd werk (Bogw), inclusief de nota van toelichting;[4]
- Regeling kwalificaties opsporingsambtenaren technisch team;[12]
- Regeling eisen keuringsdienst technisch hulpmiddel;[13]
- Memorie van Toelichting bij de Wet CCIII;[14]
- Nota naar aanleiding van het verslag van 8 november 2016;[15]
- Verslag van de plenaire vergadering van de Eerste Kamer van 19 juni 2018;[16]
- Verslag van het schriftelijk overleg van 6 december 2018;[17]
- Beantwoording van Kamervragen van 24 juli 2019;[18]
- Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv;[19]
- Besluit bewaren en vernietigen niet-gevoegde stukken.[20]

Aspecten voor het toezicht

In het rechtskader zijn regels opgenomen over het binnendringen en doen van onderzoek in een geautomatiseerd werk. Essentie van deze regels is enerzijds te waarborgen dat het tijdens het onderzoek vergaarde bewijs betrouwbaar, integer en herleidbaar is. En anderzijds in het belang van de privacy van de betrokkenen het voorkomen van onbevoegde kennisname van deze gegevens. Het toezicht door de Inspectie heeft betrekking op de volgende aspecten:

- de voorbereidende activiteiten zoals het opstellen van een haalbaarheidsonderzoek en testen van het plan van aanpak;

[12] Deze regeling is op 27 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10910).
[13] Deze regeling is op 27 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10713).
[14] *Kamerstukken II* 2015-2016, 34 372, nr. 3.
[15] *Kamerstukken II* 2016-2017, 34 372, nr. 6.
[16] *Kamerstukken EK* 2017-2018, 34e vergadering.
[17] *Kamerstukken II* 2016-2017, 34 372, nr. 29.
[18] Kamerstuk 2019D31667 d.d. 26 juli 2019.
[19] Deze regeling is op 26 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10277).
[20] https://wetten.overheid.nl/BWBR0010975/2017-01-01.

- de organisatorische en personele aspecten waaronder het aanwijzen van opsporingsambtenaren, het instellen van een technisch team, vereiste screening, expertise en opleidingsniveaus;
- het keuringsproces en de uitgevoerde keuringen van technische hulpmiddelen door de keuringsdienst;
- het handelen van het technisch team binnen de kaders van het afgegeven bevel door de officier van justitie, inclusief het treffen van eventuele aanvullende waarborgen en verantwoording daarover;
- de inzet (registratie, plaatsing, gebruik en verwijderen) van een technisch hulpmiddel door het technisch team;
- de vastlegging van gegevens over de toegang tot het technisch hulpmiddel, het functioneren van de technische infrastructuur en over de handelingen die worden verricht ter uitvoering van een bevel (logging) teneinde onregelmatigheden te kunnen vaststellen die van invloed zijn op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens op een technische infrastructuur;
- de beveiliging van de logging (inzetlogging, systeemlogging en authenticatie en autorisatielogging);
- de beveiliging van de ter uitvoering van een bevel vergaarde gegevens die als bewijslast in een rechtszaak gebruikt kunnen worden (bewijslogging);
- de controle van logbestanden op onregelmatigheden en het melden van onregelmatigheden;
- de overdracht van de gegevens aan het tactisch team dat is belast met het opsporingsonderzoeken de selectie, bewaring en vernietiging van deze gegevens door het technisch team;
- de inzet van commerciële binnendringsoftware;
- het gebruik en het melden van onbekende kwetsbaarheden (zero-days)[21] voor het binnendringen waarvan aannemelijk is dat die nog niet bekend zijn bij de producent.

Relatie met het toezicht van de Procureur-Generaal van de Hoge Raad en de Autoriteit Persoonsgegevens

De Inspectie kan in aanraking komen met mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie. Indien dit zich voordoet, kan de Inspectie de procureur-generaal bij de Hoge Raad (PG-HR) informeren.[22] De PG-HR is in 2019 gestart met het thematisch toezicht naar de rechtmatigheid en zorgvuldigheid van het uitoefenen van strafvorderlijke bevoegdheden door het OM op het gebied van de Wet CCIII, en met name het bevelen van onderzoek in een geautomatiseerd werk als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 Wetboek van Strafvordering. De Inspectie heeft in 2020 geen melding gedaan van mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie.

[21] Een onbekende kwetsbaarheid is een zwakke plek in de hard- of software waarvan de producent of fabrikant niet op de hoogte is.
[22] *Kamerstukken II* 2016-2017, 34 372, nr. 6. p. 83.

Indien de Inspectie ziet dat de politie regels schendt rond de bescherming van persoonsgegevens, kan zij de Autoriteit Persoonsgegevens (AP) informeren.[23] De Inspectie heeft in 2020 geen dergelijke melding gedaan bij de AP.

[23] *Kamerstukken II* 2016-2017, 34 372, nr. 6. p. 83.

2 Bevindingen

Dit hoofdstuk beschrijft de bevindingen van het uitgevoerde toezicht door de Inspectie op de toepassing van de hackbevoegdheid door het technisch team van de politie in 2020. Tevens wordt in dit hoofdstuk ingegaan op bevindingen over de keuring van technische hulpmiddelen en op de keuringsdienst die deze keuringen heeft uitgevoerd.

Allereerst wordt met behulp van enkele statistieken in paragraaf 2.1 inzicht gegeven in de toepassing van de hackbevoegdheid gedurende de periode waarop het onderzoek betrekking heeft. Daarna zijn de voornaamste bevindingen in een vijftal paragrafen op onderwerp bij elkaar gebracht. De Inspectie heeft alle eerdergenoemde aandachtsgebieden betrokken in haar toezicht en rapporteert in dit hoofdstuk over haar belangrijkste bevindingen.

2.1 Toepassing hackbevoegdheid politie 2020 in aantallen

De Inspectie heeft toezicht gehouden op alle zaken waarin de bevoegdheid tot het binnendringen en het doen van onderzoek in een geautomatiseerd werk door de politie is ingezet. Onderstaande tabel geeft inzicht in het aantal zaken waarin deze bevoegdheid in 2020 is ingezet. Daarnaast geeft de tabel ook inzicht in het aantal keren dat commerciële binnendringsoftware is ingezet en het aantal keren dat door de politie aangetroffen onbekende kwetsbaarheden zijn ingezet. Tevens is in de tabel opgenomen het aantal technische hulpmiddelen dat aangeboden is aan de keuringsdienst en is goedgekeurd.

Onderwerp	**Aantal**
Totaal aantal zaken waarin DIGIT in 2020 uitvoering heeft gegeven aan de wettelijke hackbevoegdheid	14[24]
Aantal van deze zaken waarin bevel is gegeven voor de inzet van een vooraf goedgekeurd technisch hulpmiddel	*1*
Aantal van deze zaken waarin bevel is gegeven voor de inzet van een niet vooraf gekeurd technisch hulpmiddel	*11*
Aantal van deze zaken waarin bevel is gegeven voor het verrichten van onderzoekshandelingen zonder technisch hulpmiddel[25]	*3*
Aantal van deze zaken waarin commerciële binnendringsoftware is ingezet	*10*
Aantal van deze zaken waarin door de politie aangetroffen onbekende kwetsbaarheden zijn gebruikt	*0*
Aantal ter keuring aangeboden technische hulpmiddelen	3[26]
Aantal van deze technische hulpmiddelen die zijn goedgekeurd	*2*

[24] Per zaak kunnen meerdere bevelen voor de inzet van de hackbevoegdheid zijn afgegeven, waaronder eventuele verlengingen. In een van deze zaken is de eerste inzet reeds gestart in 2019.
[25] In één zaak kunnen zowel bevelen afgegeven zijn voor het verrichten van onderzoekshandelingen met als zonder technisch hulpmiddel.
[26] Sommige technische hulpmiddelen zijn meerdere keren aangeboden. In totaal zijn in 2020 zes keuringen uitgevoerd.

2.2 Verrichte handelingen versus reikwijdte bevelen

Het door de officier van justitie afgegeven bevel vormt het kader waarbinnen de politie uitvoering aan deze bijzondere bevoegdheid mag geven. In het bevel vermeldt de officier van justitie onder andere een aanduiding van het geautomatiseerde werk, de periode van uitvoering en de doelen van het onderzoek inclusief eventuele beperkende voorwaarden. De Inspectie heeft onderzocht in hoeverre de politie in 2020 heeft gehandeld binnen de reikwijdte van de door de officier van justitie afgegeven bevelen.

De Inspectie heeft geen aanwijzingen dat de politie in 2020 de hackbevoegdheid heeft ingezet buiten de in de bevelen aangegeven periodes en onderzoeksdoelen. Tevens heeft de Inspectie geen aanwijzingen dat het technisch team van de politie in 2020 onderzoekshandelingen heeft verricht in een geautomatiseerd werk van een verdachte, zonder dat de officier van justitie een bevel voor toepassing van de hackbevoegdheid had afgegeven voor de betreffende verdachte.

De Inspectie heeft echter wel vastgesteld dat in 2020 de politie vier keer binnengedrongen is in een geautomatiseerd werk waarvan het unieke kenmerk niet correspondeerde met het kenmerk dat was opgenomen in het bevel. De politie heeft twee van deze vier afwijkingen direct gesignaleerd en als onregelmatigheid gemeld aan de officier van justitie. De Inspectie heeft vastgesteld dat de politie in deze twee gevallen geen onderzoekshandelingen heeft verricht. In de twee andere situaties heeft de Inspectie na afronding van de inzet door de politie geconstateerd dat de politie op een verkeerd geautomatiseerd werk is binnengedrongen. In deze situaties heeft de politie onderzoekshandelingen verricht en gegevens vastgelegd. De Inspectie heeft de politie hiervan op de hoogte gebracht. Door het hanteren van het verkeerde kenmerk van het geautomatiseerde werk heeft de politie in deze situaties ten aanzien van dit aspect buiten de reikwijdte van het afgegeven bevel gehandeld, waardoor de verkregen gegevens mogelijk niet gebruikt kunnen worden in de betreffende strafzaak.[27] De Inspectie merkt hierbij op dat uit de vastgelegde gegevens is gebleken dat beide geautomatiseerde werken wel in gebruik waren bij de desbetreffende verdachten.

De Inspectie heeft geen aanwijzingen dat de politie in 2020 nevenschade heeft veroorzaakt bij de toepassing van de hackbevoegdheid.

Beperkingen t.a.v. locatiebepaling

Mobiele geautomatiseerde werken kunnen tijdens het onderzoek wisselen van locatie en de grens overgaan. Voor het doen van onderzoek in het buitenland is toestemming vereist.[28] Daarnaast geldt dat de politie bepaalde onderzoekshandelingen volgens het bevel uitsluitend op bepaalde locaties mag toepassen. In de logging wordt de locatie van het geautomatiseerde werk niet automatisch en doorlopend vastgelegd. Ook uit de verslaglegging van het technisch team kon de Inspectie niet altijd vaststellen op welke locatie en in welk land een

[27] Dit is een beslissing van de officier van justitie en valt derhalve buiten de reikwijdte van dit toezicht door de Inspectie.
[28] Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv. Gepubliceerd in Staatscourant nr. 10277, 26 februari 2019.

geautomatiseerd werk zich bevond terwijl de politie onderzoek deed.[29] De Inspectie kan hierdoor voor enkele onderzoekshandelingen niet bepalen of de politie hier toestemming voor had.

2.3 Logging en andere verslaglegging

Het Besluit schrijft voor dat elektronische verslaglegging plaatsvindt over de uitvoering van een bevel, ook wel logging genoemd. Het uitgangspunt voor deze logging is dat vastlegging doorlopend en automatisch plaatsvindt.[30] Volgens de toelichting bij het Besluit moeten bijvoorbeeld verrichte handelingen worden vastgelegd door het registreren van beeldschermopnames en toetsaanslagen van de opsporingsambtenaren van het technisch team. Ook het vastleggen van gebruikte scripts, de communicatie tussen de technische infrastructuur en het geautomatiseerd werk wordt in dat kader genoemd.[31]

De logging is in de eerste plaats van belang voor het uitvoeren van de interne controle door de politie van de verrichte handelingen en de controle op het functioneren van de technische infrastructuur.[32] [33] Op basis van deze logging moet vastgesteld kunnen worden of gegevens die kunnen dienen als bewijs in een strafzaak, betrouwbaar en integer zijn.

Ook moet aan de hand van deze logging verantwoording afgelegd kunnen worden als, in een strafzaak of in het kader van het toezicht door de Inspectie, twijfels ontstaan over de verrichte handelingen en/of de betrouwbaarheid van het hiermee vergaarde bewijs.[34] [35] Gelet op deze belangen moet de logging beveiligd zijn tegen wijziging en onbevoegde kennisname.[36]

De Inspectie stelt vast dat in 2020:

- de logging van verrichte handelingen ter uitvoering van een bevel onvolledig is voor alle zaken waarin in 2020 onderzoekshandelingen zijn verricht. Dit is mede veroorzaakt door het in heel 2020 niet goed functioneren van de voorziening voor het registreren van beeldschermopnames. Daarnaast heeft het technisch team niet alle handelingen uitgevoerd via systemen waarvan beeldschermopnames en toetsaanslagen worden vastgelegd. Ook kan op basis van de logbestanden niet worden vastgesteld in hoeverre verwijdering van de in 2020 ingezette technisch hulpmiddelen daadwerkelijk volledig heeft plaatsgevonden;[37]

[29] Mogelijk heeft het tactisch team andere instrumenten ingezet om de locatie van het geautomatiseerd werk te bepalen, zonder dat dit in de verslaglegging van het technisch team is vermeld.
[30] Art. 5 lid 1 Bogw.
[31] Nota van toelichting Bogw, paragraaf 3.4 p. 17.
[32] Nota van toelichting, paragraaf 3.4 p.18. "*De logging is ten eerste en vooral bedoeld voor de interne controle van de tijdens de uitvoering van het bevel verrichte handelingen en het functioneren van de technische infrastructuur.*"
[33] Nota van Toelichting, paragraaf 3.4 p.18. In dat kader is tevens aangegeven dat voor het functioneren van de technische infrastructuur de systeemlogging gebruikt wordt voor het signaleren, onderzoeken en verhelpen van problemen met betrekking tot de betrouwbaarheid, integriteit en beschikbaarheid van de technische infrastructuur.
[34] Bogw, Nota van Toelichting I, hoofdstuk 4, artikel 6 pagina 36. Vaststelling van onregelmatigheden.
[35] *Kamerstukken II* 2016/17, 34 372, nr.6, p.69 en p.80. De logging is ook van belang mocht er sprake zijn van het optreden van schade en een mogelijke schadeclaim door betrokkene en in gevallen waarin twijfel ontstaat over de wijze waarop de gegevens zijn verkregen of over de betrouwbaarheid van de verkregen gegevens, bijvoorbeeld op grond van een verweer van de verdachte of diens raadsman.
[36] Nota van toelichting Bogw, paragraaf 3.4 p. 18.
[37] Art. 26 Bogw schrijft een procedure voor die moet worden gevolgd indien een technisch hulpmiddel niet (volledig) kan worden verwijderd.

- niet door de politie is uitgewerkt hoe per zaak invulling wordt gegeven aan de vereiste doorlopende en automatische vastlegging van gegevens in logbestanden. Deze uitwerking is van belang voor de politie om te kunnen komen tot het treffen van passende maatregelen voor de betrouwbaarheid en de integriteit van de logbestanden en het effectief uitvoeren van de eigen interne controle;
- de politie geen structurele controle heeft uitgevoerd op een juiste en volledige registratie in logging en andere verslaglegging.

Door het technisch team verzamelde gegevens die kunnen dienen als bewijs in een strafzaak, moeten vastgelegd worden op een technische infrastructuur.[38] De Inspectie constateert dat de politie nog niet bepaald heeft wat de reikwijdte van de technische infrastructuur is, waardoor de Inspectie niet met zekerheid kan vaststellen of al deze bewijslogging wel op de juiste plek en op betrouwbare wijze is vastgelegd.

Om de betrouwbaarheid, integriteit en herleidbaar van de bewijslogging te borgen, heeft de wetgever eisen gesteld aan deze technische infrastructuur en gegevens die daarin vastgelegd worden. De bewijslogging mag niet inhoudelijk worden bewerkt en moet beveiligd worden tegen wijziging en kennisneming door onbevoegden.[39] De politie moet maatregelen treffen om aan deze eisen te voldoen. De Inspectie heeft geconstateerd dat de politie onvolledig zicht en grip heeft op de gehele keten van opslag, transport en verwerking van deze gegevens. De politie kan hierdoor onvoldoende komen tot het identificeren van te treffen passende beheersmaatregelen, de implementatie van deze maatregelen en een eigen controle op naleving daarvan.

De Inspectie constateert dat de politie het grootste deel van de bewijslogging heeft vastgelegd in een speciaal hiervoor ontwikkelde voorziening. Op basis van de netwerkarchitectuur en waarnemingen in de praktijk, is het naar mening van de Inspectie aannemelijk dat in 2020 de toegang tot deze voorziening beperkt is geweest tot medewerkers van DIGIT. De Inspectie heeft geen aanwijzingen dat eenmaal hierin vastgelegde gegevens gewijzigd kunnen worden en zijn.

Naast de elektronische logging vormt ook de verantwoording in processen-verbaal en de verslaglegging in het journaal door de opsporingsambtenaren een belangrijke waarborg voor de controleerbaarheid van de uitvoering van een bevel.

De Inspectie stelt vast dat in 2020 deze verantwoording onvolledig is en soms ontbreekt. Voor de wel aanwezige processen-verbaal geldt dat hieruit niet kan worden opgemaakt welke onderzoekshandelingen door wie op welk moment zijn uitgevoerd. In enkele gevallen kan dit ook niet worden vastgesteld op basis van het journaal en de aanwezige logging.

In de zaken waarin het technisch team in 2020 onderzoekshandelingen heeft verricht, heeft het bewijslogging overgedragen aan het tactisch team dat is belast met het uitvoeren van het operationele onderzoek. Uit de verslaglegging blijkt niet

[38] Art. 28 Bogw.
[39] Zie o.a. Nota van toelichting Bogw, artikelsgewijze toelichting bij art. 28, p. 48.

altijd welke gegevens zijn overgedragen. Tevens blijkt niet altijd of overgedragen gegevens afkomstig zijn uit de hiervoor ingerichte centrale voorziening.

2.4 Binnendringsoftware en technische hulpmiddelen

In 2020 is in 10 zaken commerciële software gebruikt om in een geautomatiseerd werk binnen te dringen. Deze binnendringsoftware maakt gebruik van kwetsbaarheden in software op het apparaat van de verdachte.[40] Aan de inzet van deze commerciële binnendringsoftware zijn strenge voorwaarden verbonden, waaronder:

- Een product of licentie wordt ingekocht per zaak waarbij hergebruik na het onderzoek niet mogelijk is omdat het softwarepakket wordt verwijderd of de licentie is verbruikt.[41]
- De leverancier is gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en levert niet aan dubieuze regimes.[42] [43] [44]
- Het functioneren van de software wordt gecontroleerd in een testomgeving.[45]

Zoals vermeld in het Verslag van de Inspectie over 2019 is volgens de daartoe vastgestelde procedure screening van de betreffende leverancier bij de AIVD aangevraagd. In die procedure is opgenomen dat als de AIVD binnen vier weken geen bericht geeft, er vanuit gegaan wordt dat er geen nadelige gegevens zijn gevonden. De teamleiding van DIGIT heeft de Inspectie JenV aangegeven dat er geen bericht van de AIVD is ontvangen, waaruit afgeleid wordt dat er voor de AIVD geen belemmeringen bestaan voor deze leverancier.

De politie kan niet aantonen dat elke inzet van de binnendringsoftware vooraf op een zo representatief mogelijke testomgeving is gecontroleerd. Dit is onder meer van belang met het oog op het voorkomen van schade van derden.[46]

De Inspectie heeft vastgesteld dat hergebruik van de licenties voor de binnendringsoftware mogelijk is en in de praktijk ook plaatsvindt. De Inspectie heeft vastgesteld dat achteraf in elke zaak ten minste één licentie is ingekocht. Uit de parlementaire behandeling blijkt dat de eis tot de aanschaf van licenties in een zaak is bedoeld voor het zo min mogelijk stimuleren van de markt voor onbekende

---

[40] Tevens kan handmatig worden binnengedrongen door bijvoorbeeld gebruik te maken van verkregen inloggegevens. Zie de Memorie van Toelichting bij de Wet CCIII (*Kamerstukken II* 2015-2016, 34 372, nr. 3.), p.34.

[41] Nota van toelichting Bogw, paragraaf 3.3 p.15 en p.16 vermeldt dat "*na het onderzoek het softwarepakket is verwijderd of is de licentie verbruikt waardoor hergebruik niet meer mogelijk is. Wanneer in een toekomstige zaak het gebruik van binnendringsoftware van derden wederom is aangewezen, zal eerst de bruikbaarheid van de minder ingrijpende middelen worden beoordeeld en het daarvoor benodigde gehele toetsings- en beslissingsmodel doorlopen, voordat kan worden overgegaan tot een (hernieuwde) aanschaf van een softwarepakket of van een nieuwe licentie.*"

[42] Tweede Kamer, vergaderjaar 2017-2018, Kamerstuk 34 372 nr. 27 p.7 en Regeerakkoord 2017-2021 "Vertrouwen in de toekomst" p.3.

[43] Tweede Kamer, vergaderjaar 2018-2019, Kamerstuk 35 257 nr. 3 p. 20. "*Ook in het Regeerakkoord is afgesproken dat de AIVD leveranciers screent en dat geen hacksoftware gekocht wordt van bedrijven die zakendoen met «dubieuze regimes», oftewel regimes waartegen vanuit de EU of de VN repressieve sancties bestaan.*"

[44] In de beantwoording op 24 juli 2019 van Kamervragen over een media bericht over WhatsApp geeft de Minister van Justitie en Veiligheid aan dat "*de politie een toets uitvoert voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.*" Kenmerk 2647151.

[45] Nota van toelichting bij het Bogw, paragraaf 3.5, p. 20.

[46] Nota van toelichting bij het Bogw, paragraaf 3.5, p. 20.

kwetsbaarheden en de daaraan verbonden negatieve gevolgen voor de veiligheid van het internet.[47] De Inspectie signaleert dat in de praktijk het voorgeschreven licentiemodel juist leidt tot extra kosten voor de politie en daarmee mogelijk tot een extra stimulans voor deze markt.

Na het binnendringen voert het technisch team onderzoek uit in het apparaat. Bij het verrichten van onderzoekshandelingen wordt al dan niet gebruik gemaakt van een technisch hulpmiddel.[48] Volgens het Bogw is een *technisch hulpmiddel* waarmee na het binnendringen in het geautomatiseerde werk onderzoek kan worden gedaan 'een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel'.[49] [50] In de toelichting bij het Bogw is beschreven dat het uitgangspunt is dat bij het verrichten van onderzoekshandelingen met een technisch hulpmiddel gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel.[51] De Inspectie stelt vast dat in 2020 in 11 zaken bevel is gegeven voor de inzet van een niet vooraf gekeurd technisch hulpmiddel. De Inspectie JenV stelt vast dat hiermee niet is tegemoetgekomen aan dit uitgangspunt.

Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.[52] Het gebruik van een goedgekeurd technisch hulpmiddel biedt daarmee waarborgen dat bewijs op een betrouwbare, integere en herleidbare manier is vergaard.

In het besluit is gespecificeerd aan welke eisen een technisch hulpmiddel moet voldoen om te worden goedgekeurd. [53] Hierbij is niet aangegeven dat deze eisen vervallen als een technisch hulpmiddel zich naar zijn aard verzet tegen keuren. Eind 2020 heeft het Openbaar Ministerie (OM) bepaald dat de aard van het in 2020 in tien zaken gebruikte technisch hulpmiddel zich verzet tegen keuring. Als keuring van een hulpmiddel op aangeven van de officier van justitie geheel achterwege blijft of als onderzoekshandelingen worden verricht zonder gebruik van een technisch hulpmiddel dan vermeldt de officier in de processtukken welke aanvullende (procedurele) waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen.[54] Het technisch team heeft in 2020 nog niet aangegeven welke waarborgen in de betreffende zaken getroffen zijn. Op basis van de beschikbare logging en andere verslaglegging kan door de Inspectie niet afgeleid worden dat het technisch team waarborgen getroffen heeft die aanvullend zijn op de standaard in het Besluit voorgeschreven maatregelen. Het is echter ook denkbaar dat de officier van justitie

[47] Zie *Kamerstukken I 2016/17, 34 372, E,* p. 4 en p. 11 en *Kamerstukken I 2016/17, 34 372, D (MvA I),* p. 20-22.
[48] Artt. 126nba, 126uba, 126zpa eerste lid, Wetboek van Strafvordering.
[49] Art. 1 sub g Bogw.
[50] In de nota van toelichting paragraaf 3.6. p.21, Bogw wordt een voorbeeld van een technisch hulpmiddel aangedragen van op maat gemaakte software, zoals een script dat is geschreven door een technisch team en semi-handmatig wordt ingezet.
[51] Bogw artikel 14 eerste lid en artikelsgewijze toelichting op het besluit, artikel 14 pagina 40.
[52] Bogw Nota van Toelichting paragraaf 3.5 pagina 19.
[53] Hoofdstuk 5 Bogw.
[54] Art.21, vierde en vijfde lid, Bogw en artikelsgewijze toelichting artikel 21, p.45.

besluit aanvullende waarborgen te treffen buiten de inzet van het technisch team, die buiten het toezicht van de Inspectie vallen. Op basis van de toelichting bij het wettelijk kader, vindt de Inspectie het moment van de daadwerkelijke uitvoering van de hackbevoegdheid het meest voor de hand liggende moment voor het treffen van aanvullende waarborgen, omdat achteraf repareren mogelijk niet in alle gevallen nog zinvol is omdat de inzet dan al heeft plaatsgevonden.[55]

De Inspectie stelt daarnaast vast dat dit technisch hulpmiddel aantoonbaar niet voldoet aan de technische eisen uit het Besluit.[56] De leverancier van het technisch hulpmiddel heeft zelfstandig en op elk moment toegang tot het middel. De leverancier kan daarmee mogelijk ook toegang verkrijgen tot de bewijslogging die met dit middel is verkregen. Werkzaamheden die de leverancier uitvoert, kunnen, mogelijk zelfs tijdens uitvoering van een bevel, gevolgen hebben voor de werking en functionaliteit van het technisch hulpmiddel.[57] De politie kan de toegang door de leverancier niet beperken en beschikt niet over mogelijkheden om controle uit te voeren van de toegang en uitgevoerde werkzaamheden door de leverancier. De Inspectie merkt hierbij op dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor deze commerciële software die mogelijk gebruik maakt van onbekende kwetsbaarheden. De politie stelt dat er geen alternatief voorhanden is dat dezelfde functionaliteit biedt zonder deze nadelen.

Het betreffende middel is een 'black box' voor de politie, waarbij voor hen onbekend is wat er technisch precies gebeurt. Bepaalde functionaliteit kan niet worden uitgezet, waardoor het gebruik van dit middel zou kunnen conflicteren met de eis dat het technisch hulpmiddel uitsluitend gegevens ten behoeve van de in het bevel vermelde functionaliteit detecteert en registreert.

De Inspectie stelt vast dat in het technisch hulpmiddel sprake is van vastlegging van gegevens die kunnen dienen als bewijs in een strafzaak. Het Besluit stelt dat dergelijke gegevens vastgelegd moeten worden op een technische infrastructuur en formuleert eisen waaraan een dergelijke technische infrastructuur moet voldoen. De politie heeft in 2020 echter nog geen antwoord geformuleerd of de componenten van dit technisch hulpmiddel waarop vastlegging plaatsvindt onderdeel vormen van de technische infrastructuur. Bij vastlegging van gegevens op een technische infrastructuur volgt dat onder andere de logische toegang beperkt wordt en dat bij een selectie van gegevens gebruik gemaakt wordt van een forensische kopie. Bij de inzet en het gebruik van dit technisch hulpmiddel zijn dergelijke maatregelen in 2020 niet door de politie getroffen.

Zienswijze definitie technisch hulpmiddel

In 2020 heeft DIGIT samen met het Openbaar Ministerie een definitie uitgewerkt van een technisch hulpmiddel. Volgens deze definitie is sprake van een technisch hulpmiddel indien het middel zelfstandig functioneert en buiten de invloedssfeer van de opsporingsambtenaar van het technisch team de drie componenten (detectie, registratie en transport) uitvoert waarmee onderzoekshandelingen ter uitvoering van een bevel worden verricht. Van handmatige uitvoering van

[55] Zie de voorbeelden van aanvullende waarborgen op pagina 45 van de Nota van Toelichting bij het Bogw.
[56] Hoofdstuk 5 Bogw.
[57] Zie art. 10 tweede lid Bogw.

onderzoekshandelingen is volgens deze definitie sprake indien op een of meerdere componenten (detectie, registratie en/of transport) een noodzakelijke betrokkenheid wordt vereist van de uitvoerder. Deze definitie sluit volgens de Inspectie niet aan bij de huidige definitie uit het Besluit en de uitwerking in de nota van toelichting, waar wordt aangegeven dat een script dat semi-handmatig wordt ingezet, na gebruik als technisch hulpmiddel moet worden gekeurd.[58] Keuring biedt als voordeel dat risico's op misbruik door derden worden beperkt en dat specificaties van technische hulpmiddelen niet worden prijsgegeven. Dit is van groot belang voor de afscherming van gevoelige opsporingsmethoden.[59]

Indien onderzoekshandelingen plaatsvinden met software die niet is aangemerkt als technisch hulpmiddel, moeten procedurele waarborgen getroffen worden om de betrouwbaarheid, integriteit en herleidbaarheid van de bewijslogging te garanderen.[60] Deze procedurele waarborgen zullen naar mening van de Inspectie veelal minder zekerheid bieden dan de technische maatregelen waarvan de betrouwbare werking middels keuring is vastgesteld.

Melden onbekende kwetsbaarheden

Het Wetboek van Strafvordering omschrijft een onbekende kwetsbaarheid in een geautomatiseerd werk als een kwetsbaarheid die kan worden gebruikt om binnen te dringen in dat geautomatiseerde werk en waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent.[61] Indien de politie een dergelijke onbekende kwetsbaarheid aantreft, moet ze deze onbekende kwetsbaarheden bekend maken aan de producent.[62] De Inspectie heeft op basis van de logging en de verslaglegging in het journaal en de processen-verbaal geen aanwijzingen dat het technisch team in 2020 onbekende kwetsbaarheden heeft aangetroffen die zijn gebruikt om binnen te dringen in een geautomatiseerd werk. De politie en de Inspectie hebben geen kennis over de kwetsbaarheden waarvan de commerciële binnendringsoftware gebruik maakt.

2.5 Interne processen

Voor het borgen van de kwaliteit van de taakuitvoering, vindt de Inspectie het van belang dat de politie uitwerkt hoe wettelijke begrippen in de praktijk worden ingevuld en dat ze beschikt over goed functionerende interne processen. Voorbeelden zijn het inrichten van interne controlemechanismen en het uitwerken van procedures. Voor het borgen van de betrouwbaarheid en integriteit van logging (inclusief bewijslogging) is het daarnaast van belang dat de politie komt tot een aantoonbaar en controleerbaar passend beveiligingsniveau. Mede naar aanleiding van haar bevindingen over 2019, is de Inspectie nagegaan wat de politie in 2020 op dit gebied heeft bereikt.

[58] Nota van toelichting bij het Bogw, p.21.
[59] Memorie van toelichting Wet CCIII, p.110.
[60] Art. 21 lid 5 Bogw.
[61] Volgens de definitie van art. 126ffa lid 4 Sv.
[62] Art. 126ffa Sv en *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 9: "*Uitgangspunt is dat een kwetsbaarheid of lek in de beveiliging van software, dat door politie en justitie wordt aangetroffen, wordt gemeld bij de leverancier met het oog op het beëindigen of dichten daarvan.*"

De Inspectie stelt vast dat interne processen veelal nog niet voldoen aan de wettelijke vereisten. De Inspectie stelt vast dat de politie voor de toepassing van de hackbevoegdheid in 2020:

- niet alle in het wettelijk kader beschreven documenten[63] heeft opgesteld en vastgesteld;
- niet beschikte over een goed functionerend intern kwaliteitssysteem (inclusief interne controle) om de kwaliteit van de inzet van deze bevoegdheid tijdens alle fasen van de uitvoering te borgen en eventuele onregelmatigheden en tekortkomingen hierin tijdig te identificeren en te verhelpen;
- in ten minste twee zaken de hackbevoegdheid heeft laten toepassen door drie opsporingsambtenaren die niet als lid of als deelnemer in de betreffende zaak zijn aangewezen.[64] De betreffende opsporingsambtenaren waren wel in dienst bij DIGIT;
- haar werkwijze voor het toepassen van deze bevoegdheid heeft gedocumenteerd. De beoogde werkwijze was gedurende 2020 nog aan verandering onderhevig. Een deel van de procesbeschrijvingen, werkinstructies en afspraken is opgesteld en aangepast in de laatste maanden van 2020. De Inspectie heeft voor haar toezicht gedurende 2020 daardoor nog geen gebruik kunnen maken van de resultaten hiervan.

De Inspectie stelt vast dat de aangewezen leden van het technisch team voldoen aan de technische opleidingsvereisten en screeningsniveaus.[65]

Beheersing van beveiligingsrisico's

DIGIT heeft in 2020 de eerste stappen gezet om te komen tot een aantoonbaar en controleerbaar passend beveiligingsniveau. Zo is gestart met het periodiek uitvoeren van een self-assessment op door de politie voorgeschreven beveiligingsmaatregelen. De beheersing van beveiligingsrisico's is van belang voor het waarborgen van de betrouwbaarheid en integriteit van de logging en de technische infrastructuur.[66]

DIGIT is gestart met het nagaan of haar processen en systemen voldoen aan de door de politie gestelde beveiligingseisen. De politie heeft in 2020 nog geen compleet en samenhangend pakket van door DIGIT te treffen beveiligingsmaatregelen vastgesteld en geen structurele en controleerbare verantwoording afgelegd over het functioneren van getroffen beveiligingsmaatregelen. De Inspectie heeft hierdoor in 2020 voor haar toezicht nog niet kunnen steunen op de resultaten van dit traject.

[63] Zoals (definitieve versies van) aanwijzingsbesluiten, haalbaarheidsonderzoeken, plannen van aanpak, resultaten van testen in een proefopstelling en processen-verbaal.
[64] Hoofdstuk 3 Bogw.
[65] Regeling kwalificaties opsporingsambtenaren technisch team, deze regeling is op 27 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10910).
[66] Inclusief het structureel intern toezien en rapporteren over het functioneren van getroffen beveiligingsmaatregelen.

Documentatie

De Inspectie stelt vast dat een aantal onderwerpen in 2020 nog niet of niet volledig door de politie zijn gedocumenteerd:

- De politie heeft niet uitgewerkt welke gebeurtenissen zij als 'onregelmatigheden' ziet. Dit is van belang omdat de logging zodanig ingericht moet zijn dat aan de hand daarvan vastgesteld kan worden of deze onregelmatigheden hebben plaatsgevonden en daarover te kunnen rapporteren.[67] Een uitwerking op welke wijze, door wie en wanneer het monitoren op onregelmatigheden vanuit een interne verantwoordelijkheid plaatsvindt, is niet aangetroffen.
- DIGIT heeft nog niet uitgewerkt hoe verwijdering, vernietiging en naleving van bewaartermijnen van vastgelegde gegevens in de praktijk moet worden uitgevoerd en wat dit betekent voor gegevens die op diverse plaatsen zijn vastgelegd;[68] [69]
- Een uitwerking hoe het technisch team gegevens kan selecteren op basis van een forensische kopie is niet voorhanden;[70]
- Binnen DIGIT is geen proces geïmplementeerd voor de registratie van toegang, uitgifte en inname van technische hulpmiddelen;[71]
- Ontwerpdocumentatie en keuzes op basis waarvan gekomen is tot de huidige technische inrichting zijn veelal niet volledig gedocumenteerd.

Functiescheiding tussen technisch team en tactisch team

Om het risico van tunnelvisie te beperken moet gedurende het opsporingsonderzoek sprake zijn van een strikte taakverdeling en functiescheiding tussen het technisch en tactisch team.[72] De samenwerking moet dusdanig plaatsvinden dat het tactisch team geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel of eigenstandig de werking van de software te beïnvloeden.[73] Volgens het journaal van het technisch team is dit technisch hulpmiddel in enkele zaken op verzoek van een lid van het tactisch team verwijderd van een geautomatiseerd werk van de verdachte. De inspectie heeft geen aanwijzingen dat leden van een tactisch team toegang hebben tot technische hulpmiddelen en de technische infrastructuur.

[67] Nota van toelichting Bogw, artikelsgewijze toelichting op art. 6, p. 36.
[68] Nota van toelichting Bogw, H4, p. 22.
[69] In 2020 heeft de politie van de officier van justitie geen bevel van ontvangen tot vernietiging of verwijdering van gegevens.
[70] Nota van toelichting Bogw, artikelsgewijze toelichting op art. 21, p. 45.
[71] Dit is voorgeschreven in artikel 22 Bogw en komt overeen met het proces voor 'klassieke' technische hulpmiddelen dat is beschreven in het Besluit technische hulpmiddelen strafvordering, dit besluit is op 7 november 2006 in het Staatsblad gepubliceerd (Stb. 2006, nr. 524).
[72] Vanwege de functiescheiding wordt het onderzoek in een geautomatiseerd werk uitgevoerd door speciaal daarvoor opgeleide opsporingsambtenaren die niet betrokken zijn bij het betreffende opsporingsonderzoek. Tweede Kamer, vergaderjaar 2016-2017, 34 372 nr.6, p.28.
[73] Nota van toelichting Bogw p. 36 en Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 6 p.40 en p.59.

2.6 Keuring en keuringsdienst

Indien onderzoekshandelingen worden verricht met een technisch hulpmiddel is het uitgangspunt dat een vooraf goedgekeurd technisch hulpmiddel wordt ingezet.[74] De beoordeling of een technisch hulpmiddel voldoet aan de eisen wordt uitgevoerd door een keuringsdienst. De Inspectie heeft vastgesteld dat TNO gedurende het verslagjaar 2020 door de Minister van Justitie en Veiligheid aangewezen is als keuringsdienst.[75] De organisatie, de medewerkers en de beschikbare middelen van deze aangewezen keuringsdienst moeten voldoen aan regels.[76] De Inspectie stelt vast dat TNO in 2020 hieraan heeft voldaan.

De wijze van keuring is op hoofdlijnen vastgelegd in een door de Minister goedgekeurd keuringsprotocol.[77] De Inspectie heeft vastgesteld dat door de keuringsdienst voor elk goedgekeurd technisch hulpmiddel testactiviteiten heeft uitgewerkt die aansluiten op het keuringsprotocol. Deze activiteiten en de resultaten zijn gestructureerd en controleerbaar vastgelegd in een voor dit doel ontwikkelde voorziening.

In 2020 zijn zes keuringen uitgevoerd van drie verschillende technische hulpmiddelen. Twee van deze technische hulpmiddelen zijn door de keuringsdienst goedgekeurd.[78] De Inspectie stelt vast dat de keuringdienst per goedgekeurd technisch hulpmiddel het doorlopen keuringstraject navolgbaar heeft vastgelegd. Het keuringsdossier is gestructureerd en goed toegankelijk. Verantwoording over de uitgevoerde testactiviteiten, bijbehorende uitkomsten en afwegingen zijn op een controleerbare wijze vastgelegd. Hieruit is voor de Inspectie in voldoende mate af te leiden in hoeverre het betreffende technische hulpmiddel voldoet aan de hieraan gestelde technische eisen[79] en is navolgbaar hoe en op basis waarvan de keuringsdienst tot goedkeuring is gekomen. Het keuringsrapport van de goedgekeurde technische hulpmiddelen voldoet aan de daaraan gestelde eisen.[80]

[74] Nota van toelichting bij het Bogw, artikelsgewijze toelichting bij art. 14, p. 60.
[75] Aanwijzingsbesluit TNO als keuringsdienst van het Ministerie van Justitie en Veiligheid, dit besluit is op 20 maart 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 15022).
[76] Regeling eisen keuringsdienst technisch hulpmiddel, deze regeling is op 27 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10713).
[77] Dit keuringsprotocol is niet extern gepubliceerd.
[78] In 2020 zijn geen onderzoekshandelingen verricht met deze goedgekeurde technische hulpmiddelen.
[79] Hoofdstuk 5 Bogw.
[80] Art. 18 Bogw.

3 Conclusie en aanbeveling

Het rechtskader benadrukt het belang van de betrouwbaarheid van het bewijs en de bescherming van de persoonlijke levenssfeer van de verdachte en derden. De Inspectie concludeert dat bij de toepassing van de hackbevoegdheid in 2020 risico's niet kunnen worden uitgesloten voor wat betreft de betrouwbaarheid van het door DIGIT verkregen bewijs en de privacy van de betrokkenen. Net als in 2019 wordt dit mede veroorzaakt door onvolledige logging en ongecontroleerde toegang door de leverancier van de commerciële software. De Inspectie heeft op basis van de wel aanwezige logging en overige beschikbare informatie geen aanwijzingen dat de politie in 2020 de hackbevoegdheid heeft ingezet buiten de in de bevelen aangegeven periodes en onderzoeksdoelen.

De politie heeft in 2020 een traject voor professionalisering van interne processen ingezet. De Inspectie concludeert dat de over 2019 geconstateerde tekortkomingen in 2020 echter nog niet zijn verholpen. De Inspectie had verwacht dat in 2020 meer verbetering zichtbaar zou zijn, het uitblijven hiervan baart de Inspectie zorgen.

De conclusie van de Inspectie is gebaseerd op de volgende deelconclusies:

Leverancier commerciële software heeft toegang tot vastgelegde gegevens
In 2020 heeft de politie in 14 zaken bevel gekregen voor het toepassen van de hackbevoegdheid. In tien van deze zaken heeft de politie commerciële software ingezet voor het binnendringen en het doen van onderzoek. De Inspectie concludeert, net als in 2019, dat deze software gebruik maakt van servers die worden beheerd door de leverancier. De leverancier heeft altijd toegang tot de software, inclusief de hiermee vastgelegde gegevens. Werkzaamheden die de leverancier uitvoert kunnen gedurende de uitvoering van een bevel gevolgen hebben voor de werking en functionaliteit van deze software. De politie heeft geen zicht op de technische werking van deze software en kan de toegang door de leverancier niet technisch beperken en controleren. De Inspectie merkt hierbij op dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor deze commerciële software die mogelijk gebruik maakt van onbekende kwetsbaarheden. De politie stelt dat er geen alternatief voorhanden is dat dezelfde functionaliteit biedt zonder deze nadelen.

Logging en andere verslaglegging incompleet
Net als in 2019 heeft de politie in 2020 de doorlopende en automatische vastlegging van gegevens in logbestanden niet op orde: de logging van verrichte handelingen is onvolledig voor alle zaken waarin de politie in 2020 onderzoekshandelingen heeft verricht. Ook de handmatige vastlegging is niet compleet. De Inspectie kan door deze hiaten niet uitsluiten dat onregelmatigheden hebben plaatsgevonden, zonder dat deze zijn gesignaleerd. Tevens kon de Inspectie door het ontbreken van locatiegegevens van enkele onderzoekshandelingen niet bepalen of de politie hier toestemming voor had. Logging vindt op verschillende manieren plaats, waarbij sprake is van overlap. Door

de wel aanwezige logging te combineren, kon de Inspectie uiteindelijk toch de uitgevoerde handelingen grotendeels reconstrueren. De Inspectie heeft op basis hiervan geen aanwijzingen dat de politie in 2020 de hackbevoegdheid heeft ingezet buiten de in de bevelen aangegeven periodes en onderzoeksdoelen.

Kwaliteitssysteem niet op orde
Voor toepassing van de hackbevoegdheid beschikte de politie, evenals in 2019, niet over een goed functionerend intern kwaliteitssysteem. Met een dergelijk systeem, inclusief interne controle, kan de politie de kwaliteit van de inzet van de bevoegdheid tijdens alle fasen van de uitvoering borgen en eventuele onregelmatigheden en tekortkomingen hierin zelf tijdig identificeren en verhelpen. De Inspectie concludeert dat de politie hierdoor soms fouten en hiaten in de verslaglegging niet heeft opgemerkt en onvoldoende toeziet op de kwaliteit van documenten. Tevens heeft de Inspectie de politie er twee keer op moeten wijzen dat zij niet zelf gesignaleerd heeft dat zij is binnengedrongen in een geautomatiseerd werk waarvan het unieke kenmerk niet correspondeerde met het kenmerk dat was opgenomen in het bevel. Door het hanteren van het verkeerde kenmerk van het geautomatiseerde werk heeft de politie in deze situaties ten aanzien van dit aspect buiten de reikwijdte van het afgegeven bevel gehandeld, waardoor de verkregen gegevens mogelijk niet gebruikt kunnen worden in de betreffende strafzaak.[81] De Inspectie merkt hierbij op dat uit de vastgelegde gegevens is gebleken dat beide geautomatiseerde werken wel in gebruik waren bij de desbetreffende verdachten.

De Inspectie stelt vast dat DIGIT in 2020 is gestart met een traject om te komen tot een aantoonbaar en controleerbaar passend beveiligingsniveau. Zo is gestart met het periodiek uitvoeren van een self-assessment op door de politie voorgeschreven beveiligingsmaatregelen. De beheersing van beveiligingsrisico's middels het identificeren, implementeren en het uitvoeren van eigen controles op naleving is voor de politie van belang om de betrouwbaarheid en integriteit van de logging en de vastgelegde gegevens te kunnen waarborgen. De Inspectie heeft voor haar toezicht in 2020 nog geen gebruik kunnen maken van de resultaten van dit traject.

Aanbeveling

De politie heeft de hackbevoegdheid sinds maart 2019 ontwikkelgericht ingezet en verder vormgegeven. In de achterliggende periode heeft de politie praktijkervaring opgebouwd en een traject voor verdere professionalisering ingezet. De Inspectie beveelt de politie aan om opvolging te geven aan de door de Inspectie gerapporteerde afwijkingen zodat verbeteringen uit dit traject zichtbaar worden in de praktijk.

[81] Dit is in eerste instantie een beslissing van de officier van justitie en valt derhalve buiten de reikwijdte van dit toezicht door de Inspectie.

Bijlage: Afkortingen

Afkorting	**Betekenis**
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AP	Autoriteit Persoonsgegevens
Bogw	Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in artt. 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Stb. 2018, 340.
CCIII	Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III)
DIGIT	Digital Intrusion Team (onderdeel van de Landelijke Eenheid van de Nationale Politie). Het technisch team dat is belast met de uitoefening van de hackbevoegdheid maakt deel uit van DIGIT.
OM	Openbaar Ministerie
PG-HR	Procureur-generaal bij de Hoge Raad der Nederlanden
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek

Inspectie Justitie en Veiligheid
Toezicht, omdat rechtvaardigheid en veiligheid
niet vanzelfsprekend zijn.

Dit is een uitgave van:
Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag
Contactformulier | www.inspectie-jenv.nl

Juni 2021