Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Verslag toezicht wettelijke hackbevoegdheid politie 2019

Verslag van het toezicht door de Inspectie Justitie en Veiligheid op de toepassing door de politie van de bevoegdheid op basis van de Wet Computercriminaliteit III om in een geautomatiseerd werk binnen te dringen en onderzoek te doen.

Inhoudsopgave

Voorwoord

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 zoals een laptop of een smartphone dat in gebruik is bij een verdachte, heimelijk en op afstand binnen te dringen en hier onderzoek in te doen. De Inspectie Justitie en Veiligheid (Inspectie JenV) is de toezichthouder op de taakuitvoering door de politie. Vanuit die rol houdt zij toezicht op de toepassing door de politie van de bevoegdheid op basis van de Wet CCIII om in een geautomatiseerd werk binnen te dringen en onderzoek te doen.

De Inspectie JenV rapporteert jaarlijks aan de minister van Justitie en Veiligheid over de bevindingen van haar toezicht op de inzet van deze hackbevoegdheid door de politie. Dit is haar eerste verslag. De Inspectie rapporteert in dit verslag over de periode 1 maart 2019 (de datum van inwerkingtreding van de wet) tot en met 31 december 2019.

De politie heeft de praktische uitoefening van de nieuwe hackbevoegdheid gedurende 2019 doorontwikkeld. De Inspectie houdt daar in haar toezicht rekening mee. Wel dient de politie deze bevoegdheid altijd binnen de wettelijke kaders uit te voeren. In de uitoefening van het toezicht op de hackbevoegdheid heeft de Inspectie van de politie een constructieve en open houding ervaren.

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 na twee jaar na invoering hiervan wordt uitgevoerd.

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

1 Inleiding

1.1 Wettelijk kader toezicht

De Wet Computercriminaliteit III

De toegenomen digitalisering van de maatschappij drukt een groot stempel op de aard van vele criminaliteitsvormen. De bestaande opsporingsbevoegdheden bleken niet afdoende in de bestrijding van ernstige (computer)criminaliteit. Met de Wet Computercriminaliteit III (CCIII) wordt beoogd bij te dragen aan een effectieve aanpak van criminaliteit en aan een veilig digitaal domein.

De Wet CCIII introduceert de bevoegdheid om een geautomatiseerd werk (een apparaat zoals een laptop of een smartphone) dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen.[1] 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.[2]

Het onderzoek in een geautomatiseerd werk bestaat uit verschillende fasen. De eerste fase betreft het op afstand heimelijk binnendringen in een apparaat.[3] De tweede fase betreft het – al dan niet met een technisch hulpmiddel – verrichten van bepaalde onderzoekshandelingen waarmee gegevens kunnen worden vastgelegd die kunnen dienen als bewijs in een strafzaak.

Toezicht door de Inspectie Justitie en Veiligheid

De Inspectie JenV houdt toezicht op het functioneren van het wettelijk systeem rond het toepassen van de hackbevoegdheid door de politie.[4] Toepassing van deze bevoegdheid vindt plaats binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris. De oordeelsvorming door de officier van justitie en de rechter-commissaris valt buiten de reikwijdte van het toezicht door de Inspectie JenV.

---

[1] Daar waar in dit verslag de ‘bevoegdheid’ of ‘hackbevoegdheid’ wordt genoemd, wordt gedoeld op de bevoegdheid om een geautomatiseerd werk (een apparaat zoals 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] Zie artikel 126nba, 126uba en 126zpa Wetboek van Strafvordering.
[3] In dit verslag is ter bevordering van de leesbaarheid het begrip ‘geautomatiseerd werk’ op diverse plaatsen vervangen door ‘apparaat’.
[4] 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.

Het toezicht van de Inspectie JenV is niet beperkt tot toezicht achteraf. De Inspectie JenV kan zich te allen tijde vergewissen van een juiste uitvoering van het bevel van de officier van justitie. De Inspectie JenV kan, in het kader van het systeemtoezicht, toezicht houden tijdens de uitvoering van het bevel.[5] Het toezicht heeft ook betrekking op de inzet van de bevoegdheid in gevallen die niet leiden tot een strafvervolging.[6]

De Inspectie JenV houdt tevens toezicht op de naleving van de regels en procedures voor de keuring en inzet van software waarmee op apparaten gegevens worden verzameld en de vastlegging van gegevens op een beveiligde technische infrastructuur.[7]

Indien de Inspectie tijdens de uitoefening van het toezicht in aanraking komt met mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie of in aanraking komt met mogelijke schendingen van de regels rond de bescherming van persoonsgegevens kan de Inspectie JenV de procureur-generaal bij de Hoge Raad (PG-HR) respectievelijk de Autoriteit Persoonsgegevens (AP) informeren.[8]

De Inspectie JenV rapporteert jaarlijks over de uitkomsten van haar toezicht op de naleving van de in het Wetboek van Strafvordering en het Besluit onderzoek in een geautomatiseerd werk[9] (Bogw) opgenomen normen. Indien daaruit structurele problemen blijken, dan kunnen die voor de Inspectie JenV aanleiding zijn de politie te verzoeken een verbeterplan op te stellen. Daarnaast kunnen de bevindingen in het verslag aanleiding geven om het toezicht op onderdelen te intensiveren.[10]

De Inspectie JenV rapporteert in dit verslag over de periode 1 maart 2019 (de datum van inwerkingtreding van de wet) tot en met 31 december 2019. In de volgende verslagen zal ze telkens over het hele kalenderjaar rapporteren.

1.2 Leeswijzer

In het verslag zijn in hoofdstuk 2 de toezichtactiviteiten op hoofdlijnen beschreven die de Inspectie heeft uitgevoerd. In bijlage 1 zijn deze nader verantwoord. In hoofdstuk 3 formuleert de Inspectie haar conclusie en de belangrijkste bevindingen waarop die conclusie is gebaseerd. In bijlage 2 zijn de detailbevindingen van het toezicht door de Inspectie JenV opgenomen.

[5] Eerste Kamer, 2017-2018, 34 372, nr. 27, verslag van een schriftelijk overleg, p. 13.
[6] *Kamerstukken II* 2016-2017, 34 372, nr. 6, p. 81-83.
[7] Eerste Kamer, 2017-2018, 34 372 G, nadere memorie van antwoord, ontvangen 4 mei 2018, p. 14.
[8] *Kamerstukken II* 2016-2017, 34 372, nr. 6. p. 83.
[9] Het besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).
[10] Eerste Kamer, 2017-2018, 34 372 G, nadere memorie van antwoord, ontvangen 4 mei 2018, p. 20.

2 Uitgevoerde toezichtactiviteiten

De hackbevoegdheid is centraal belegd bij één team: het Digital Intrusion Team (DIGIT) van de Landelijke Eenheid van de Nationale Politie. In 2019 heeft dit technisch team de hackbevoegdheid in acht zaken toegepast. Een bevel wordt afgegeven per verdachte per apparaat (bijvoorbeeld een laptop of telefoon) of groep van apparaten (bijvoorbeeld een aantal computers in hetzelfde netwerk). In deze acht zaken hebben officieren van justitie in totaal zeventien bevelen afgegeven voor het inzetten van de hackbevoegdheid. De Inspectie JenV heeft toezicht gehouden op alle acht inzetten. Ze heeft per inzet de toedracht gereconstrueerd op basis van beschikbare logging, documentatie en gesprekken met de teamleiding van DIGIT en leden van het technisch team. Tevens heeft de Inspectie JenV 'live' meegekeken tijdens de uitvoering van een onderzoek door het technisch team.

Daarnaast heeft de Inspectie JenV – over de diverse inzetten heen – kennis genomen van generieke aspecten zoals de beveiliging van de technische infrastructuur en de procesmatige inrichting van informatiebeveiliging van DIGIT. Omdat de politie de implementatie van deze aspecten in 2019 nog niet had voltooid, heeft de Inspectie JenV zich in 2019 gericht op de beoordeling op zaakniveau en nog geen inhoudelijke beoordeling uitgevoerd op de effectiviteit van deze generieke aspecten.

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. In 2019 is nog geen technisch hulpmiddel goedgekeurd. De Inspectie JenV heeft in 2019 nog geen toezicht uitgevoerd op de door de keuringsdienst uitgevoerde keuringsprocedure. Wel heeft de Inspectie in 2019 gesproken met zowel TNO als met de keuringsdienst van de Landelijke Eenheid om inzicht te verkrijgen in het keuringsproces.

Zie bijlage 1 voor een nadere verantwoording van de uitgevoerde toezichtactiviteiten door de Inspectie JenV.

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

3 Conclusie

De Inspectie JenV komt op basis van haar bevindingen tot de volgende conclusie.

De Inspectie JenV stelt vast dat de politie in het eerste jaar van de nieuwe hackbevoegdheid op een professionele wijze invulling heeft gegeven aan de ontwikkeling van de organisatie en de daarvoor benodigde middelen.

De Inspectie JenV concludeert dat de politie bij de toepassing van de hackbevoegdheid heeft voldaan aan de wettelijke eisen, met uitzondering van de eis tot het doorlopend vastleggen van gegevens in logbestanden, doordat in alle zaken de logging niet compleet is. De Inspectie heeft geen aanwijzing dat hierdoor onregelmatigheden onopgemerkt zijn gebleven die van invloed waren op de betrouwbaarheid en integriteit van de vastgelegde gegevens of dat er buiten de reikwijdte van het bevel is gehandeld. Wel heeft het de mogelijkheden tot interne controle door de politie en de toezichthoudende taak van de Inspectie bemoeilijkt.

Daarnaast constateert de Inspectie JenV dat verbeteringen nodig zijn bij de inzet van technische hulpmiddelen, bij het testen van uit te voeren handelingen en bij het aantoonbaar beheersen van beveiligingsrisico's. Hiermee kan worden voorkomen dat later in een strafprocedure discussie ontstaat over de betrouwbaarheid en integriteit van het bewijs.

De Inspectie JenV realiseert zich daarbij dat het technisch team van de politie zich in de opbouwbase bevindt en dat de bevoegdheid nieuw is. De Inspectie heeft gezien dat de politie in de voorbereiding en inrichting van de organisatie en werkprocessen, en bij het verwerven van de middelen, veel inspanning heeft verricht om de nieuwe bevoegdheid professioneel en binnen de wettelijke kaders te kunnen uitvoeren. Er is in korte tijd voorzien in nieuwe huisvesting en apparatuur. In een gespannen IT-markt is de politie erin geslaagd om deskundigen te werven om een start te kunnen maken met het inzetten van de bevoegdheid.

De conclusie van de Inspectie JenV is gebaseerd op de volgende belangrijkste bevindingen:

1. De Inspectie JenV heeft bij de uitoefening van de bevoegdheid door het technisch team van de politie in 2019 geen handelingen geïdentificeerd die buiten de grens vallen van de bevelen van de officier van justitie en de machtigingen van de rechter-commissaris. De initiële termijn van vier weken bleek vaak niet toereikend vanwege een langere doorlooptijd van het proces van verkennen, binnendringen en onderzoeken. De Inspectie JenV stelt vast dat in deze gevallen het technisch team pas is doorgegaan met het inzetten van de bevoegdheid nadat een verlenging van het bevel van de officier van justitie en toestemming van de rechter-commissaris was ontvangen. Hiermee heeft de politie gehandeld binnen de wettelijke kaders.

2. In het wettelijk kader is aangegeven dat gedurende de uitvoering van een bevel doorlopend en automatisch gegevens worden vastgelegd in logbestanden over de handelingen die worden verricht ter uitvoering van een bevel, de toegang tot een technisch hulpmiddel, de gegevens die al dan niet met een technisch hulpmiddel op de technische infrastructuur worden vastgelegd ter uitvoering van een bevel, en het functioneren van de technische infrastructuur. Hierbij is aangegeven dat gegevens over de handelingen die worden verricht ter uitvoering van een bevel die naar hun aard niet automatisch kunnen worden vastgelegd, handmatig worden vastgelegd door een opsporingsambtenaar van het technisch team.[12] De logging is in alle acht zaken niet geheel in overeenstemming met deze wettelijke bepalingen uitgevoerd. In alle acht zaken is de logging van uitgevoerde handelingen niet volledig. Dit heeft de mogelijkheden tot interne controle door de politie en de toezichthoudende taak van de Inspectie bemoeilijkt. Daardoor heeft de Inspectie JenV niet kunnen vaststellen of zich gedurende de uitvoering van de bevelen een onregelmatigheid heeft voorgedaan, die van invloed is op de betrouwbaarheid van de met de onderzoekshandelingen verkregen gegevens.

   Hierbij merkt de Inspectie JenV op dat zij op basis van de wel aanwezige logging en overige beschikbare informatie de uitgevoerde handelingen grotendeels heeft kunnen reconstrueren. Daaruit blijkt dat er geen aanwijzing is dat het technisch team tijdens de inzet van de hackbevoegdheid heeft gehandeld buiten de reikwijdte of periode van de door de officier van justitie afgegeven bevelen.

3. De wet biedt de officier van justitie de mogelijkheid het onderzoek in een geautomatiseerd werk handmatig of met een technisch hulpmiddel te laten verrichten.[13] In zes van de acht zaken is door de officier van justitie in 2019 bevolen dat onderzoekshandelingen met een technisch hulpmiddel verricht worden. In diverse parlementaire stukken is beschreven dat het uitgangspunt is dat bij het inzetten van een technisch hulpmiddel gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel.[14] De Inspectie JenV stelt vast dat in geen van deze zes zaken onderzoek is uitgevoerd met een vooraf goedgekeurd technisch hulpmiddel. De Inspectie JenV stelt vast dat in 2019

[12] Artikel 5 Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).
[13] Artikel 126nba/126uba/126zpa lid 1 Wetboek van Strafvordering.
[14] Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2018-2019, 34 372, nr. 29, p.7,13, de Memorie van Toelichting bij de Wet CCIII (*Kamerstukken II* 2015-2016, 34 372, nr. 3.) en de toelichting bij het Bogw (Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340)). Dit uitgangspunt kan ook worden afgeleid uit de tekst van artikel 21 Bogw.

niet is tegemoetgekomen aan het uitgangspunt dat in diverse parlementaire stukken is beschreven.

4. Indien een ingezet technisch hulpmiddel niet vooraf is gekeurd, moet dit na afloop van het gebruik worden gekeurd tenzij de aard van het technisch hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet.[15] In 2019 heeft de politie voor zes zaken bevel gekregen voor het verrichten van onderzoekshandelingen met een technisch hulpmiddel. Slechts voor één zaak is het in die zaak ingezette technisch hulpmiddel – na afloop van het gebruik – ter keuring aangeboden, de overige technische hulpmiddelen zijn in 2019 niet ter keuring aangeboden. Overigens is in het wettelijk kader geen termijn gesteld waarbinnen het technisch hulpmiddel achteraf ter keuring moet worden aangeboden, zodat de politie keuring achteraf geruime tijd achterwege kan laten.

   Voor de enige zaak waar het technisch hulpmiddel in 2019 wel achteraf ter keuring is aangeboden, heeft de keuringsdienst geoordeeld dat deze software niet voldoet aan de eisen zoals vastgelegd in het wettelijk kader. Dit betekent dat dit technisch hulpmiddel is afgekeurd. In 2019 is dus geen van de ingezette technische hulpmiddelen goedgekeurd.

5. In 2019 heeft de officier van justitie in twee zaken bevolen dat het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt zonder een technisch hulpmiddel, dus handmatig. In een van deze zaken heeft de politie een zelf ontwikkeld script ingezet. Gelet op de functionaliteit van het script is de Inspectie van mening dat dit script valt onder de definitie van een technisch hulpmiddel. Zowel in haar haalbaarheidsonderzoek als in haar plannen van aanpak beschouwt de politie de hiermee verrichte onderzoekshandelingen echter als handmatig. Hieruit blijkt dat een verschil van inzicht over de interpretatie van deze definitie bestaat. De politie werkt samen met het Openbaar Ministerie aan een nadere uitwerking van deze definitie, de Inspectie houdt de vinger aan de pols om na te gaan of deze uitwerking past binnen het wettelijk kader.

6. Omdat het technisch team in 2019 in geen van de zaken, waarbij de officier van justitie in het bevel had aangegeven dat van een technisch hulpmiddel gebruik moest worden gemaakt, de uitgevoerde onderzoekshandelingen heeft uitgevoerd met een goedgekeurd technisch hulpmiddel, zijn op grond van het wettelijk kader voor elk van deze zes zaken aanvullende waarborgen vereist om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen.[16] Op basis van de analyse van de inzetlogging stelt de Inspectie vast dat geen vastlegging beschikbaar is van door het technisch team getroffen waarborgen die aanvullend zijn op de standaard maatregelen die in (de toelichting bij) het wettelijk kader zijn beschreven. 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

[15] De Inspectie stelt vast dat in 2019 geen toepassing is gegeven aan artikel 21 lid 4 Bogw, op grond waarvan keuring of herkeuring na afloop van het gebruik achterwege blijven, indien de aard van het technisch hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet. Overigens is in het Bogw geen termijn gesteld waarbinnen de officier moet besluiten of al dan niet toepassing is gegeven aan artikel 21 lid 4 Bogw.

[16] Tenzij de ingezette technische hulpmiddelen alsnog worden goedgekeurd.

heeft plaatsgevonden.[17] Het is echter ook denkbaar dat de officier van justitie besluit aanvullende waarborgen te treffen buiten de inzet van het technisch team, die buiten het toezicht van de Inspectie JenV vallen. Bijvoorbeeld door een review op de toegepaste technieken te laten uitvoeren door een externe expert.

7. De politie heeft bij de toepassing van de hackbevoegdheid de uitgevoerde handelingen niet vooraf volledig getest. De Inspectie heeft vastgesteld dat, doordat de politie in een aantal zaken heeft nagelaten bepaalde handelingen volledig te testen, er in de uitvoering van die zaken technische problemen optraden, die vermijdbaar waren. Op basis van analyse van de beschikbare logging merkt de Inspectie hierbij op dat de opgetreden technische problemen geen negatieve gevolgen hebben gehad voor het onderzochte apparaat of systemen van derden.

8. In 2019 beschikte de politie niet over een intern kwaliteitssysteem om eventuele tekortkomingen in de toepassing van de hackbevoegdheid tijdig te identificeren en te verhelpen. Daardoor kan zij zelf niet aantonen dat de verwerking van de politiegegevens in overeenstemming wordt verricht met de wettelijke eisen en dat passende beveiligingsmaatregelen zijn getroffen. De Inspectie JenV vindt het, voor het toezicht op de beheersing van beveiligingsrisico's van DIGIT, van belang dat de politie een intern kwaliteitssysteem inricht.

9. In het Bogw wordt gesteld dat het technisch team maatregelen moet treffen om wijziging van de vastgelegde gegevens of kennisneming van de vastgelegde gegevens door onbevoegden te voorkomen. Tevens wordt gesteld dat het mogelijk moet zijn achteraf vast te stellen of wijziging of kennisneming hiervan heeft plaatsgevonden.[18] Vanuit de Wet politiegegevens (Wpg) geldt tevens de algemene eis tot het treffen van passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. De minister heeft daarnaast in een reactie op vragen van de vaste commissie aangegeven dat voor de beveiligde omgeving waar de onderzoeksgegevens worden weggeschreven, zwaardere fysieke en cryptografische beveiligingseisen gelden dan de gebruikelijke eisen voor de digitale infrastructuur van de politie.[19]

   De Inspectie JenV heeft vastgesteld dat de politie een breed scala aan beveiligingsmaatregelen heeft getroffen. De politie heeft echter nog geen integrale risicoanalyse uitgevoerd om te bepalen welke maatregelen passend zijn. Ook heeft de politie nog geen integrale toets uitgevoerd op de effectiviteit van de getroffen maatregelen.

10. In parlementaire stukken is aangegeven dat de technische infrastructuur waarop onderzoeksgegevens worden vastgelegd wordt beheerd door de politie en dat de servers van deze technische infrastructuur zich bevinden in Nederland.[20] De Inspectie JenV heeft zich door het technisch team laten informeren over de technische infrastructuur waarop onderzoeksgegevens worden vastgelegd. Met uitzondering van de commerciële binnendringsoftware,

[17] Zie de voorbeelden van aanvullende waarborgen op pagina 45 van de Nota van Toelichting bij het Bogw.
[18] Artikel 28 lid 3 Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).
[19] Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2018-2019, 34 372, nr. 29, p.11.
[20] Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2018-2019, 34 372, nr. 29, p.12.

heeft de Inspectie JenV gezien dat de technische infrastructuur waarop onderzoeksgegevens worden vastgelegd, wordt beheerd door de politie en dat de servers van deze technische infrastructuur zich op locatie van de politie in Nederland bevinden.

In bijlage 2 zijn de detailbevindingen van het toezicht door de Inspectie JenV opgenomen.

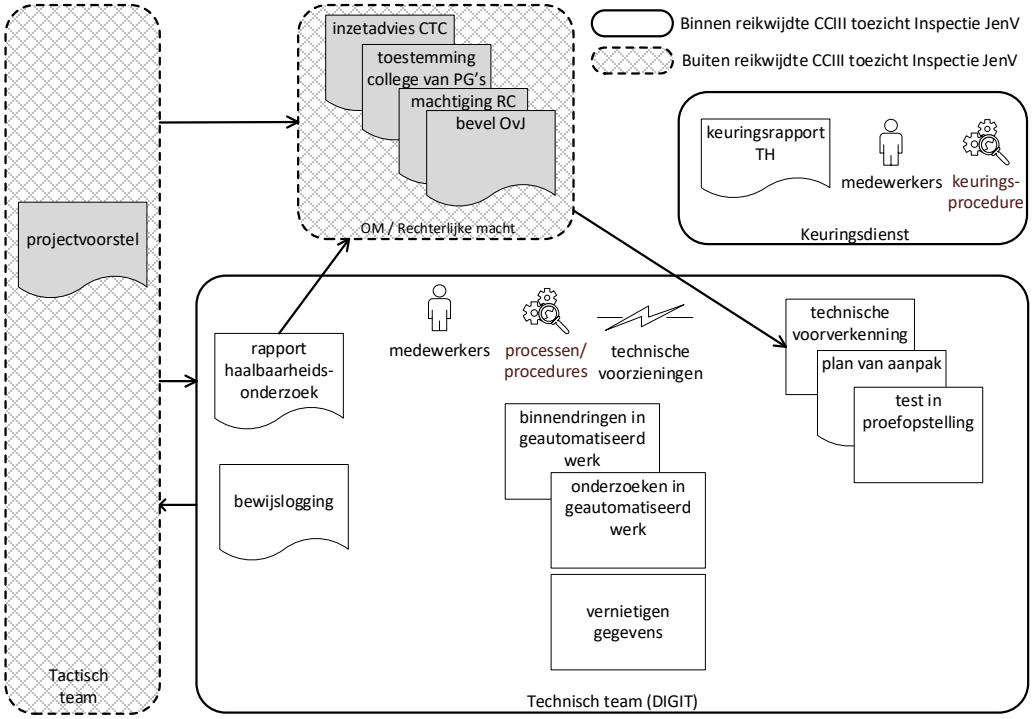
De Inspectie heeft vastgesteld dat de politie zich samen met andere hierbij betrokken partijen inspant om te gaan beschikken over goedgekeurde technische hulpmiddelen. Daarnaast blijkt uit het onderzoek van de Inspectie dat de teamleiding van DIGIT is gestart met het uitwerken van procesbeschrijvingen om aantoonbaar te werken binnen de wettelijke kaders en te verbeteren op de hierboven genoemde punten. Ook heeft de teamleiding van DIGIT aan de Inspectie JenV gemeld dat extra functies zijn en worden ingevuld om meer aandacht te kunnen geven aan een snelle en correcte administratieve verwerking van de inzetten (zoals het consistent volledig bijhouden van het journaal en het opstellen van de vereiste processen verbaal).

De Inspectie blijft de door de politie ingezette verbeteringen kritisch volgen en zet de in 2019 ingezette vorm van toezicht op de politie in 2020 voort door op elke inzet van de hackbevoegdheid toezicht te houden.

Bijlage Verantwoording toezichtactiviteiten

Reikwijdte toezicht Inspectie JenV

De Inspectie JenV heeft vanaf de inwerkingtreding van de Wet CCIII toezicht gehouden op de uitoefening van de bevoegdheid tot het binnendringen en onderzoeken in een geautomatiseerd werk (hierna: de bevoegdheid). Uitoefening van de bevoegdheid is belegd bij een technisch team van de politie, dat onderdeel uitmaakt van DIGIT. Het toezicht van de Inspectie JenV richt zich met name op toepassing van de hackbevoegdheid door het technisch team. Ook de randvoorwaarden zoals eisen ten aanzien van medewerkers, processen, procedures en technische voorzieningen vallen binnen de reikwijdte van het toezicht door de Inspectie JenV.



Afbeelding 1. *Reikwijdte toezicht.*

De reikwijdte van het toezicht is schematisch weergegeven in afbeelding 1 en hieronder toegelicht.

De voorbereiding van het onderzoek in een geautomatiseerd werk (een apparaat zoals een laptop of een smartphone) start met een projectvoorstel van een tactisch team aan de officier van justitie. Het projectvoorstel kan afkomstig zijn van tactische rechercheteams van de politie, van de Koninklijke Marechaussee (KMar) of van een bijzondere opsporingsdienst zoals de Fiscale inlichtingen- en opsporingsdienst (FIOD). Het projectvoorstel bevat onder meer een beschrijving van de verdachte, de verdenking, de noodzaak om de onderzoeksbevoegdheid toe te passen en de gewenste resultaten van de toepassing van de bevoegdheid.

Ter voorbereiding van het bevel stelt het technisch team, op basis van de intakegegevens en overige relevante gegevens, een rapport haalbaarheidsonderzoek op voor de officier van justitie. Hierin wordt het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt. In het rapport wordt onder meer opgenomen welke bevelen nodig zijn, en of en zo ja welke software van derden moet worden aangeschaft.

De officier van justitie gebruikt het rapport haalbaarheidsonderzoek voor het verkrijgen van toestemming voor de inzet van de opsporingsbevoegdheid van het College van procureurs-generaal (het College) en de machtiging van de rechter-commissaris. De rechter-commissaris toetst de rechtmatigheid van het bevel en de proportionaliteit en subsidiariteit van de inzet van de bevoegdheid. Het College laat zich bij zijn besluit adviseren door de Centrale Toetsingscommissie (CTC), een intern adviesorgaan van het Openbaar Ministerie (OM) dat is samengesteld uit leden van het OM en de politie. De oordeelsvorming door de officier van justitie en de rechter-commissaris valt buiten de reikwijdte van het toezicht door de Inspectie JenV.

In de toelichting bij het Bogw is beschreven dat het technisch team na afgifte van een bevel een technische verkenning uitvoert. Na een analyse hiervan wordt een plan van aanpak opgesteld. De gekozen aanpak wordt vervolgens getest in een proefopstelling voordat wordt gestart met het daadwerkelijk binnendringen en het uitvoeren van onderzoekshandelingen.

Om in een geautomatiseerd werk binnen te dringen kan het technisch team gebruik maken van binnendringsoftware die bijvoorbeeld gebruik maakt van kwetsbaarheden in software op het apparaat van de verdachte. Tevens kan handmatig worden binnengedrongen door bijvoorbeeld gebruik te maken van verkregen inloggegevens.[21] Na het binnendringen voert het technisch team onderzoek uit in het apparaat. 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. Een technisch hulpmiddel is een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel. Als bij het verrichten van onderzoekshandelingen gebruik wordt gemaakt van goedgekeurde software mag er vanuit worden gegaan dat aan de wettelijke eisen omtrent de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan. Een uitzondering op deze hoofdregel is mogelijk als het onderzoeksbelang dringend vordert dat gebruik wordt gemaakt van software die zich naar zijn aard niet leent voor voorafgaande

[21] Zie de Memorie van Toelichting bij de Wet CCIII (*Kamerstukken II* 2015-2016, 34 372, nr. 3.), p.34.

goedkeuring. In dat geval vermeldt de officier van justitie in het bevel dat gebruik wordt gemaakt van een niet gekeurd hulpmiddel. Na afloop vindt alsnog keuring plaats, tenzij de aard ervan zich naar het oordeel van de officier hiertegen verzet. In dat geval vermeldt de officier van justitie in de processtukken dat is afgezien van keuring en vermeldt hij welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en de herleidbaarheid van de vastgelegde gegevens te garanderen. In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven.

In het Bogw is aangegeven dat de minister een onderdeel van de Landelijke Eenheid aanwijst als keuringsdienst voor de keuring van technische hulpmiddelen. Tevens is aangegeven dat de minister een of meer andere organisaties kan aanwijzen als keuringsdienst. Omdat de Landelijke Eenheid niet beschikte over voldoende capaciteit en expertise, heeft de minister TNO tot 1 maart 2022 aangewezen als keuringsdienst voor het uitvoeren van keuringen van technische hulpmiddelen.[22] De Inspectie JenV houdt toezicht op de naleving van de regels en procedures omtrent de keuring van een technisch hulpmiddel. In de toelichting bij het Bogw is aangegeven dat de wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een apparaat, geen deel uitmaakt van het keuringsproces. In het geval binnendringsoftware door de politie wordt ingekocht (commerciële binnendringsoftware) wordt het functioneren hiervan in een testomgeving gecontroleerd.

Nadat onderzoek is verricht in het apparaat dat in gebruik is bij de verdachte, draagt het technisch team de verzamelde gegevens (bewijslogging) over aan het tactisch team. Deze gegevens moeten na afloop van de bewaartermijn worden vernietigd.

Gehanteerde normen

Voor de uitoefening van het toezicht heeft de Inspectie JenV gebruik gemaakt van normen en teksten uit de volgende en wet- en regelgeving en verslagen:

- Wetboek van Strafvordering;
- Bogw (inclusief de Nota van Toelichting);[23]
- Wet politiegegevens (Wpg);
- Regeling kwalificaties opsporingsambtenaren technisch team;[24]
- Regeling eisen keuringsdienst technisch hulpmiddel;[25]
- Memorie van Toelichting bij de Wet CCIII;[26]
- Nota naar aanleiding van het verslag van 8 november 2016;[27]
- Verslag van de plenaire vergadering van de Eerste Kamer van 19 juni 2018;[28]
- Verslag van het schriftelijk overleg van 6 december 2018;[29]
- Beantwoording van Kamervragen van 24 juli 2019.[30]

[22] Dit besluit op 20 maart 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 15022).
[23] Artikel 16 Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).
[24] Deze regeling is op 27 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10910).
[25] Deze regeling is op 27 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10713).
[26] *Kamerstukken II* 2015-2016, 34 372, nr. 3.
[27] *Kamerstukken II* 2016-2017, 34 372, nr. 6.
[28] *Kamerstukken EK* 2017-2018, 34e vergadering.
[29] *Kamerstukken II* 2016-2017, 34 372, nr. 29.
[30] Antwoord op vragen van het lid Verhoeven over het bericht 'WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone'.

Relatie met OM en PG-HR

Het toezicht op de inzet van de hackbevoegdheid dat de Inspectie JenV in het afgelopen jaar bij de politie heeft uitgevoerd, heeft duidelijk gemaakt dat er een nauwe verwevenheid is tussen de activiteiten die de politie in het kader van deze bevoegdheid heeft verricht en beslissingen van de officier van justitie in de onderzochte zaken. De oordeelsvorming door de officier van justitie valt buiten de reikwijdte van het toezicht door de Inspectie JenV. Indien naar het oordeel van de procureur-generaal bij de Hoge Raad (PG-HR) het OM bij de uitoefening van zijn taak de wettelijke voorschriften niet naar behoren handhaaft of uitvoert, kan hij de minister daarvan in kennis stellen.[31] De Inspectie JenV heeft in de afgelopen verslagperiode met de PG-HR afgestemd over bevindingen in haar onderzoek die betrekking hadden op het handelen van de officier van justitie, met inbegrip van het toezicht dat het OM uitoefent op de uitvoering van zijn bevelen door de politie. Door de PG-HR is een aanvang gemaakt met de uitvoering van 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.

[31] Artikel 122 Wet op de rechterlijke organisatie.

Bijlage Detailbevindingen

Onderstaande tabel a geeft inzicht in het aantal zaken waarin de bevoegdheid tot het binnendringen in een geautomatiseerd werk in 2019 is ingezet.

Tabel a. *Gegevens inzetten bevoegdheid van maart tot en met december 2019*

Onderwerp	Aantal
Zaken waarin de bevoegdheid is ingezet	8
Zaken waarin met de bevoegdheid verkregen gegevens als bewijs zijn ingebracht in een strafzaak	0[32]
Afgegeven initiële/aanvullende bevelen	17[33]
Bevelen voor inzet vooraf goedgekeurd technisch hulpmiddel	0
Bevelen voor inzet niet vooraf gekeurd technisch hulpmiddel	11
Bevelen voor onderzoekshandelingen zonder technisch hulpmiddel	6
Inzet commerciële binnendringsoftware (licenties)	7
Gebruikte onbekende kwetsbaarheden (niet via commerciële binnendringsoftware)	0

Voorbereiding onderzoek

Alle inzetten die het technisch team in 2019 heeft uitgevoerd zijn in lijn met de beschrijving van het proces uit de toelichting bij het Bogw gestart vanuit een aanvraag (projectvoorstel) van een tactisch team. Voor alle zaken heeft het technisch team een rapport haalbaarheidsonderzoek opgesteld dat is besproken tijdens een zitting van de CTC. Voor elk van de inzetten in 2019 heeft de officier van justitie een bevel afgegeven en heeft de rechter-commissaris een machtiging verleend.

In de toelichting bij het Bogw is beschreven dat het technisch team een plan van aanpak opstelt voor de uit te voeren binnendring- en onderzoekshandelingen. Deze aanpak wordt volgens de toelichting vervolgens getest in een proefopstelling. De Inspectie JenV stelt vast dat het technisch team voor een deel van de uitgevoerde binnendring- en onderzoekshandelingen geen plan van aanpak heeft opgesteld. In

[32] Omdat (nog) niet is overgegaan tot strafvervolging (omdat bijvoorbeeld ontlastend bewijs is gevonden) of omdat het met de hackbevoegdheid verkregen informatie (nog) niet in lopende strafzaken is ingebracht.
[33] Per zaak kan sprake zijn van meerdere verdachten en meerdere apparaten waarop de hackbevoegdheid is ingezet. Een bevel wordt afgegeven per verdachte voor per apparaat of groep apparaten.

de inzetdossiers heeft de Inspectie JenV geen verslaglegging aangetroffen van (resultaten van) testen in een proefopstelling. Het testen in een proefopstelling is onder meer van belang om het risico op verstoringen te beperken voor het apparaat waarop wordt binnengedrongen.

De Inspectie JenV heeft waargenomen dat tijdens de uitvoering van vier zaken technische problemen optraden. Naar mening van de Inspectie hadden deze problemen in de uitvoering voorkomen kunnen worden als, conform de beschrijving in de toelichting bij het Bogw, vooraf getest was in een proefopstelling. Hierbij merkt de Inspectie JenV op dat het realiseren van een proefopstelling die gelijk is aan het te onderzoeken geautomatiseerde werk niet in alle gevallen mogelijk is. Op basis van analyse van de beschikbare logging merkt de Inspectie hierbij op dat de opgetreden technische problemen geen negatieve gevolgen hebben gehad voor het onderzochte apparaat of systemen van derden.

Technische hulpmiddelen

In de wet is aangegeven dat de officier van justitie, indien het onderzoek dit dringend vordert, kan bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet.[34]

De wet biedt de officier van justitie de mogelijkheid het onderzoek in een geautomatiseerd werk handmatig of met een technisch hulpmiddel te laten verrichten.[35] In zes van de acht zaken is door de officier van justitie in 2019 bevolen dat onderzoekshandelingen met een technisch hulpmiddel verricht worden. In diverse parlementaire stukken is beschreven dat het uitgangspunt is dat bij het inzetten van een technisch hulpmiddel gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel.[36] De Inspectie JenV stelt vast dat in geen van deze zes zaken onderzoek is uitgevoerd met een vooraf goedgekeurd technisch hulpmiddel. De Inspectie JenV stelt vast dat in 2019 niet is tegemoetgekomen aan het uitgangspunt dat in diverse parlementaire stukken is beschreven.

Indien een ingezet technisch hulpmiddel niet vooraf gekeurd is, moet dit na afloop van het gebruik worden gekeurd tenzij de aard van het technisch hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet.[37] In 2019 heeft de politie voor zes zaken bevel gekregen voor het verrichten van onderzoekshandelingen met een technisch hulpmiddel. Slechts voor één zaak is het in die zaak ingezette technisch hulpmiddel – na afloop van het gebruik – ter keuring aangeboden, de overige technische hulpmiddelen zijn in 2019 niet ter keuring aangeboden. Overigens is in het Bogw geen termijn gesteld waarbinnen het technisch hulpmiddel achteraf ter keuring moet worden aangeboden, zodat de politie keuring achteraf geruime tijd achterwege kan laten.

[34] Artikel 126nba/126uba/126zpa lid 1 Wetboek van Strafvordering.
[35] Artikel 126nba/126uba/126zpa lid 1 Wetboek van Strafvordering.
[36] Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2018-2019, 34 372, nr. 29, p.7,13, de Memorie van Toelichting bij de Wet CCIII (*Kamerstukken II* 2015-2016, 34 372, nr. 3.) en de toelichting bij het Bogw (Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340)). Dit uitgangspunt kan ook worden afgeleid uit de tekst van artikel 21 Bogw.
[37] De Inspectie stelt vast dat in 2019 geen toepassing is gegeven aan artikel 21 lid 4 Bogw, op grond waarvan keuring of herkeuring na afloop van het gebruik achterwege blijven, indien de aard van het technisch hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet. Overigens is in het Bogw geen termijn gesteld waarbinnen de officier moet besluiten of al dan niet toepassing is gegeven aan artikel 21 lid 4 Bogw.

Voor de enige zaak waar het technisch hulpmiddel in 2019 wel achteraf ter keuring is aangeboden heeft de keuringsdienst geoordeeld dat deze software niet voldoet aan de eisen zoals vastgelegd in het Bogw. Dit betekent dat dit technisch hulpmiddel is afgekeurd. In 2019 is dus geen van de ingezette technische hulpmiddelen goedgekeurd.

In het Bogw is aangegeven[38] dat voor toegang tot technische hulpmiddelen een formeel proces gevolgd moet worden dat vergelijkbaar is met het proces voor de registratie, uitgifte en inname van 'klassieke' technische hulpmiddelen (zoals een microfoon en/of een videocamera).[39] Bij het technisch team is een dergelijk proces niet geïmplementeerd.

In 2019 heeft de officier van justitie in twee zaken bevolen dat het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt zonder een technisch hulpmiddel, dus handmatig. In een van deze zaken heeft de politie een zelf ontwikkeld script ingezet. Gelet op de functionaliteit van het script is de Inspectie van mening dat dit script valt onder de definitie van een technisch hulpmiddel. Zowel in haar haalbaarheidsonderzoek als in haar plannen van aanpak beschouwt de politie de hiermee verrichte onderzoekshandelingen echter als handmatig. Hieruit blijkt dat een verschil van inzicht over de interpretatie van deze definitie bestaat. De politie werkt samen met het Openbaar Ministerie aan een nadere uitwerking van deze definitie, de Inspectie houdt de vinger aan de pols om na te gaan of deze uitwerking past binnen het wettelijk kader.

Omdat het technisch team in 2019 in geen van de zaken, waarbij de officier van justitie in het bevel had aangegeven dat van een technisch hulpmiddel gebruik moest worden gemaakt, de uitgevoerde onderzoekshandelingen heeft uitgevoerd met een goedgekeurd technisch hulpmiddel, zijn op grond van het Bogw voor elk van deze zes zaken aanvullende waarborgen vereist om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen.[40] Op basis van de analyse van de inzetlogging stelt de Inspectie vast dat geen vastlegging beschikbaar is van door het technisch team getroffen waarborgen die aanvullend zijn op de standaard maatregelen die in (de toelichting bij) het wettelijk kader zijn beschreven. Op basis van de toelichting bij het Bogw, 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.[41] Het is echter ook denkbaar dat de officier van justitie besluit aanvullende waarborgen te treffen buiten de inzet van het technisch team, die buiten het toezicht van de Inspectie JenV vallen. Bijvoorbeeld door een review op de toegepaste technieken te laten uitvoeren door een externe expert.

Onbekende kwetsbaarheden en commerciële binnendringsoftware

Om in een geautomatiseerd werk binnen te dringen kan het technisch team binnendringsoftware inzetten die bijvoorbeeld gebruik maakt van kwetsbaarheden in software op het systeem van de verdachte. Soms bevat software onbekende kwetsbaarheden die nog niet bekend zijn bij de leverancier hiervan.[42] Indien het technisch team een dergelijke onbekende kwetsbaarheid ontdekt of inkoopt, geldt

[38] Artikel 22 Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).
[39] 'Besluit technische hulpmiddelen strafvordering, dit besluit is op 7 november 2006 in het Staatsblad gepubliceerd (Stb. 2006, nr. 524).
[40] Tenzij de ingezette technische hulpmiddelen alsnog worden goedgekeurd.
[41] Zie de voorbeelden van aanvullende waarborgen op pagina 45 van de Nota van Toelichting bij het Bogw.
[42] Zie de Memorie van Toelichting bij de Wet CCIII (*Kamerstukken II* 2015-2016, 34 372, nr. 3.), p.34.

dat deze in beginsel direct gemeld dient te worden bij de leverancier.[43] De Inspectie JenV stelt vast dat het technisch team in 2019 geen eigen ontwikkelde of ingekochte informatie over onbekende kwetsbaarheden heeft ingezet om een geautomatiseerd werk binnen te dringen.

Het technisch team kan ook binnendringsoftware inkopen bij een leverancier. In het Regeerakkoord 2017–2021 en in het Bogw is opgenomen dat deze zogenaamde commerciële binnendringsoftware van derden die mogelijk gebruik maakt van onbekende kwetsbaarheden alleen zal worden aangeschaft als daartoe in een specifieke zaak een noodzaak bestaat. Aan de inzet van deze commerciële binnendringsoftware zijn strenge voorwaarden verbonden:[44]

- Commerciële binnendringsoftware mag uitsluitend worden ingezet indien minder ingrijpende middelen niet toereikend zijn. Dit oordeel wordt gevormd door de officier van justitie en getoetst door de rechter-commissaris.
- Een product of licentie wordt pas ingekocht na centrale toetsing door het OM, waarbij hergebruik na het onderzoek niet mogelijk is omdat het softwarepakket wordt verwijderd of de licentie is verbruikt.
- De leverancier is gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en levert niet aan dubieuze regimes.
- Het functioneren van de software wordt gecontroleerd in een testomgeving.
- Opslag van de onderzoeksgegevens vindt plaats op de technische infrastructuur van de politie, zonder gebruik te maken van een server van de leverancier van de software.

In 2019 heeft het technisch team de beschikking gekregen over commerciële binnendringsoftware. Deze software is in 2019 ingezet in drie van de acht zaken. De Inspectie JenV heeft vastgesteld dat het technisch team deze commerciële binnendringsoftware heeft ingezet na toestemming van de officier van justitie en de rechter-commissaris en na centrale toetsing binnen het OM door de CTC. Volgens de daartoe vastgestelde procedure is 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.

Per apparaat waarop is binnengedrongen heeft het technisch team een zo goed mogelijk gelijkende testomgeving ingericht waarop de software op functioneren is getest. De in 2019 ingezette binnendringsoftware maakt voor het binnendringen en onderzoeken in het geautomatiseerde werk gebruik van servers van de leverancier. De server waarop de onderzoeksgegevens worden opgeslagen bevindt zich in het rekencentrum van de politie en wordt beheerd door de leverancier. De Inspectie JenV stelt vast dat op dit punt niet wordt voldaan aan tijdens de parlementaire behandeling geformuleerde toezeggingen.

De Inspectie JenV stelt vast dat commerciële binnendringsoftware doorgaans wordt geleverd met een eigen technisch hulpmiddel dat onlosmakelijk is verbonden met de binnendringsoftware. Daarmee is het in de praktijk zo dat binnendringsoftware en een technisch hulpmiddel voor het doen van onderzoek in één pakket van een

[43] Zie artikel 126ffa Wetboek van Strafvordering.
[44] Deze restricties zijn geformuleerd in het Bogw. De afspraak dat geen gebruik gemaakt mag worden van een server van de leverancier is genoemd in het Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2018-2019, 34 372, nr. 29, p.12.

commerciële leverancier worden afgenomen, waardoor ze niet los van elkaar kunnen worden beschouwd. De Inspectie voorziet dat keuring wordt bemoeilijkt doordat de leveranciers waarschijnlijk geen (volledige) inzage geven in de werking van deze software.

Uitvoering binnendring- en onderzoekshandelingen door technisch team

In de Wet CCIII is aangegeven dat de inzet van de bevoegdheid is beperkt tot de limitatief omschreven doelen.[45] Dit betreft het verrichten van bepaalde onderzoekshandelingen[46], waarvoor het nodig is dat op afstand heimelijk wordt binnengedrongen in het geautomatiseerde werk. Tevens is in de toelichting bij de wet aangegeven dat de bevoegdheid wordt toegepast in een zo beperkt mogelijk deel van een geautomatiseerd werk. Deze beperking dient in het bevel te worden omschreven en waarborgt dat de overheid geen onbegrensde toegang heeft tot gegevens die zijn opgeslagen in een geautomatiseerd werk. Wanneer tijdens het onderzoek blijkt dat de bevoegdheid in een ander deel van het geautomatiseerde werk moet worden toegepast, dan is daarvoor een aangepast bevel en uitdrukkelijke toestemming van de rechter-commissaris nodig.[47] Ten slotte is in de wet aangegeven dat de toepassing van de bevoegdheid is beperkt in tijd. Het bevel vermeldt het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven. De bevoegdheid mag slechts voor de duur van hoogstens vier weken worden toegepast en kan telkens voor een periode van ten hoogste vier weken worden verlengd.[48]

De Inspectie JenV heeft bij de uitoefening van de bevoegdheid door het technisch team in 2019 geen handelingen geïdentificeerd die buiten de grens vallen van de bevelen van de officier van justitie en de machtigingen van de rechter-commissaris. De initiële termijn van vier weken bleek vaak niet toereikend vanwege een langere doorlooptijd van het proces van verkennen, binnendringen en onderzoeken. De Inspectie JenV stelt vast dat in deze gevallen het technisch team pas is doorgegaan met het inzetten van de bevoegdheid nadat een verlenging van het bevel van de officier van justitie en toestemming van de rechter-commissaris was ontvangen. Hiermee heeft de politie gehandeld binnen de wettelijke kaders.

Op grond van het Bogw dient het technisch team zorg te dragen voor doorlopende en automatische vastlegging van in het Bogw gespecificeerde gegevens in logbestanden. In de toelichting bij het Bogw zijn de volgende aspecten beschreven die minimaal moeten worden vastgelegd:

- het beeldscherm en de toetsaanslagen van de uitvoerende opsporingsambtenaren;
- communicatie tussen de technische infrastructuur en het geautomatiseerde werk;
- gebruikte scripts en softwareversies.

Volgens het Bogw dient logging op zodanige wijze te geschieden dat zowel tijdens de uitvoering van het bevel als achteraf kan worden vastgesteld of zich gedurende de uitvoering van het bevel een onregelmatigheid heeft voorgedaan, die van invloed is op de betrouwbaarheid van de met de onderzoekshandelingen verkregen

[45] Artikel 126nba/126uba,126zpa lid 1 Wetboek van Strafvordering.
[46] Namelijk de vaststelling van kenmerken (zoals de identiteit of locatie, en de vastlegging daarvan), het opnemen/onderzoeken van vertrouwelijke communicatie, stelselmatige observatie, vastlegging van gegevens die in het geautomatiseerde werk zijn/worden opgeslagen en ontoegankelijkmaking van gegevens.
[47] *Kamerstukken II* 2015-2016, 34 372, nr. 3, p. 53.
[48] Artikel 126nba lid 3 Wetboek van Strafvordering.

gegevens.[49] Deze loggingplicht is ook van toepassing op de voorbereidende fase van het onderzoek: het binnendringen in een geautomatiseerd werk. Alle logging moet naar beveiligde omgevingen worden weggeschreven waar manipulatie niet meer mogelijk is.[50] Voor de Inspectie JenV is deze vastlegging een van de belangrijkste bronnen op basis waarvan zij beoordeelt in hoeverre is gewerkt binnen de grenzen van het wettelijk kader en het bevel.

De Inspectie JenV heeft tijdens haar onderzoek per zaak de beschikbare logging geanalyseerd en stelt op basis hiervan het volgende vast:

- In zeven van de acht zaken is nagelaten de toetsaanslagen vast te leggen van opsporingsambtenaren van het technisch team.
- In de zaak waarin wel toetsaanslagen in logbestanden zijn vastgelegd, waren niet van alle in het journaal beschreven handelingen toetsaanslagen beschikbaar.
- In drie zaken is nagelaten de beeldschermopnames vast te leggen van de uitgevoerde handelingen van de opsporingsambtenaren van het technisch team.
- In drie van de vijf zaken waarin wel beeldschermopnames zijn vastgelegd, zijn niet van alle in het journaal beschreven handelingen beeldschermopnames vastgelegd.
- In geen van de acht zaken was vastlegging beschikbaar van de integrale communicatie tussen de technische infrastructuur en het geautomatiseerde werk.
- In zeven zaken was de handmatige vastlegging (in het journaal) van niet automatisch gelogde relevante zaken niet compleet. In deze zaken zijn geen processen-verbaal opgesteld van de handelingen en gebeurtenissen waarvoor dit in het Bogw is voorgeschreven. Dit betreft de plaatsing van een technisch hulpmiddel, het verrichten van onderzoekshandelingen, de verwijdering van een technisch hulpmiddel en van het stopzetten van het transport van de gegevens.
- In een zaak zijn technische logging en beeldschermopnames handmatig in de beschermde opslag-omgeving geplaatst zonder dat hiervan verantwoording is afgelegd (in een proces-verbaal of in het journaal), ook zijn hiervan geen beeldschermopnames vastgelegd.
- In drie zaken is door het technisch team gebruik gemaakt van systemen die buiten het pand van de politie zijn gebruikt. In twee zaken is geen systeemlogging vastgelegd van deze systemen.
- In drie zaken is de logging uitsluitend opgeslagen binnen de omgeving van het gebruikte technisch hulpmiddel en niet binnen de beschermde opslag-omgeving.

De inzetlogging is ten eerste en vooral bedoeld voor de interne controle van de tijdens het onderzoek in een geautomatiseerd werk verrichte handelingen.[51] De Inspectie JenV stelt vast dat de politie achteraf nog geen analyse heeft uitgevoerd om (als onderdeel van een intern systeem voor kwaliteitsbewaking) na te gaan in hoeverre is voldaan aan de eisen uit het wettelijk kader. Interne periodieke controles worden niet structureel uitgevoerd. De Inspectie is van mening dat de realisatie van een intern kwaliteitssysteem belangrijk is om afwijkingen tijdig te identificeren en op te volgen.

[49] Artikel 6 lid 1 Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).
[50] Verslag van het schriftelijk overleg van 6 december 2018, *Kamerstukken II* 2016-2017, 34 372, nr. 29, p.11.
[51] Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2017-2018, 34 372, nr. 27, p.11.

Het ontbreken van volledige logging bemoeilijkt de Inspectie JenV in de uitoefening van haar toezichthoudende taak. Hierbij merkt de Inspectie JenV op dat zij op basis van de wél beschikbare logging de uitgevoerde handelingen grotendeels heeft kunnen reconstrueren en dat zij hierbij geen aanwijzing heeft dat hierdoor onregelmatigheden onopgemerkt zijn gebleven die van invloed waren op de betrouwbaarheid en integriteit van de vastgelegde gegevens of dat er buiten de reikwijdte van het bevel is gehandeld. Wel heeft het de mogelijkheden tot interne controle door de politie en de toezichthoudende taak van de Inspectie bemoeilijkt.

De Inspectie JenV stelt daarnaast vast dat van de acht in 2019 gestarte zaken slechts in één geval alle vereiste processen-verbaal zijn opgesteld. Veel van de handelingen waarvoor een proces-verbaal is vereist, hebben inmiddels enkele maanden geleden plaatsgevonden.

Technische infrastructuur

In parlementaire stukken is aangegeven dat de technische infrastructuur waarop onderzoeksgegevens worden vastgelegd wordt beheerd door de politie en dat de servers van deze technische infrastructuur zich bevinden in Nederland.[52] De Inspectie JenV heeft zich door het technisch team laten informeren over de technische infrastructuur waarop onderzoeksgegevens worden vastgelegd. Met uitzondering van de commerciële binnendringsoftware, heeft de Inspectie JenV gezien dat de technische infrastructuur waarop onderzoeksgegevens worden vastgelegd, wordt beheerd door de politie en dat de servers van deze technische infrastructuur zich op locatie van de politie in Nederland bevinden.

In het Bogw wordt gesteld dat het technisch team maatregelen moet treffen om wijziging van de vastgelegde gegevens of kennisneming van de vastgelegde gegevens door onbevoegden te voorkomen. Tevens wordt gesteld dat het mogelijk moet zijn achteraf vast te stellen of wijziging of kennisneming hiervan heeft plaatsgevonden.[53] Vanuit de Wet politiegegevens (Wpg) geldt tevens de algemene eis tot het treffen van passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. Dit heeft met name betrekking op de verwerking van de bijzondere categorieën van politiegegevens, op een zodanige manier dat de politiegegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. De minister heeft daarnaast in een reactie op vragen van de vaste commissie aangegeven dat voor de beveiligde omgeving waar de onderzoeksgegevens worden weggeschreven, zwaardere fysieke en cryptografische beveiligingseisen gelden dan de gebruikelijke eisen voor de digitale infrastructuur van de politie.[54] De Inspectie JenV heeft vastgesteld dat de politie een breed scala aan beveiligingsmaatregelen heeft getroffen. De politie heeft echter nog geen integrale risicoanalyse uitgevoerd om te bepalen welke maatregelen passend zijn. Ook heeft de politie nog geen integrale toets uitgevoerd op de effectiviteit van de getroffen maatregelen.

Met een goed functionerend kwaliteitssysteem zou de politie zelf kunnen aantonen dat de verwerking van de politiegegevens in overeenstemming met de Wpg wordt verricht[55] en dat de beveiliging van persoonsgegevens is gewaarborgd.[56] De politie heeft in 2019 een dergelijk kwaliteitssysteem nog niet ingericht.

---

[52] Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2018-2019, 34 372, nr. 29, p.12.
[53] Artikel 28 lid 3 Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).
[54] Verslag van het schriftelijk overleg van 7 mei 2018, *Kamerstukken II* 2018-2019, 34 372, nr. 29, p.11.
[55] Artikel 4a lid 1a Wet politiegegevens.

Verstrekking en vernietiging gegevens

Het technisch team van de politie mag uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking stellen aan het tactisch team. Indien gegevens worden geselecteerd of bewerkt, moet dit gebeuren op basis van een forensische kopie en moet hiervan een proces-verbaal worden opgemaakt.[57]

De Inspectie stelt vast dat het technisch team in drie zaken op verzamelde gegevens een technische vertaalslag heeft uitgevoerd alvorens deze over te dragen aan het tactisch team. De vertaalslag is gemaakt op een export van de bronbestanden die digitaal is ondertekend zodat de integriteit van het origineel kan worden gevalideerd; hiermee is voldaan aan de eis tot het gebruik van een forensische kopie. Van het maken van deze selectie is nog geen proces-verbaal opgemaakt, dit is echter wel een vereiste. De Inspectie JenV stelt vast dat de administratieve afhandeling door het technisch team op het punt van het opstellen van processen-verbaal over de zaken in 2019 achterloopt bij de uitvoering van de onderzoeken.

In de toelichting bij het Bogw is beschreven dat op grond van andere wettelijke bepalingen de volgende eisen gelden voor bewaartermijnen en vernietiging van verzamelde gegevens:

- Zodra de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek, worden deze verwijderd of gedurende een periode van maximaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10 Wpg. Na afloop van deze termijn worden de gegevens verwijderd.[58]
- Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en de notificatie, bedoeld in artikel 126bb Sv is verricht, doet de officier van justitie de processen-verbaal en andere voorwerpen vernietigen.[59]

Omdat geen van de zaken uit 2019 formeel is geëindigd, is nog niet bekend wanneer de gegevens vernietigd moeten zijn. De Inspectie JenV stelt vast dat de politie geen procedure heeft uitgewerkt voor het tijdig en juist vernietigen van gegevens die niet langer bewaard mogen worden.

Personele aspecten

Het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen is voorbehouden aan daartoe door hun werkgever aangewezen opsporingsambtenaren van de politie, de KMar, de bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren. Een aangewezen opsporingsambtenaar kan de bevoegdheid uitsluitend uitoefenen als hij heeft voldaan aan door de minister van JenV aangewezen kwalificaties[60] en door de korpschef is aangewezen als *lid van een technisch team*.[61] Een opsporingsambtenaar van de politie, de KMar, de bijzondere opsporingsdiensten of een buitengewoon opsporingsambtenaar die geen lid is van een technisch team kan door de korpschef worden aangewezen als *deelnemer aan een technisch team* als hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van een bevel in een individueel opsporingsonderzoek. De aanwijzing tot deelnemer

[56] Artikel 33 lid 1 Wet politiegegevens.
[57] Artikel 29 Bogw, inclusief de passage uit de nota van toelichting bij dit artikel.
[58] Artikel 9 lid 4 Wet politiegegevens.
[59] Artikel 3 lid 1 Besluit bewaren en vernietigen niet-gevoegde stukken.
[60] Zoals vastgelegd in de 'Regeling kwalificaties opsporingsambtenaren technisch team'. Deze regeling is op 27 februari 2019 in de Staatscourant gepubliceerd (Stcrt. 2019, nr. 10910).
[61] Artikel 3 Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).

vindt plaats voor de duur van het bevel. Om de kwaliteit en professionaliteit van het onderzoek te borgen, bepaalt het Bogw dat een opsporingsambtenaar die op ad hoc basis deelneemt aan een technisch team gedurende de uitvoering van het onderzoek wordt begeleid door een lid van een technisch team.[62]

De Inspectie stelt vast dat binnen DIGIT een groep opsporingsambtenaren door de korpschef is aangewezen als leden van het technisch team. Deze leden van het technisch team voldoen aan de gestelde kwalificatie-eisen. De Inspectie JenV stelt vast dat in vijf van de zaken waarin de bevoegdheid in 2019 is toegepast, alle handelingen voor het binnendringen en onderzoeken in het geautomatiseerde werk zijn verricht door leden van het technisch team. In de overige drie zaken zijn deelnemers toegevoegd aan het technisch team. Deze deelnemers hebben de commerciële binnendringsoftware en het hieraan gekoppelde technisch hulpmiddel bediend. De teamleiding van DIGIT heeft aangegeven dat de aanwijzingsbesluiten van de betreffende deelnemers nog niet zijn ondertekend en dat de deelnemers zonder begeleiding door een lid van het technisch team uitvoering hebben gegeven aan bevelen tot onderzoek in een geautomatiseerd werk. Hierbij heeft de teamleiding aangegeven dat alle deelnemers wel een specifieke training hebben gevolgd voor het bedienen van de gebruikte commerciële software.

In de toelichting bij het Bogw is aangegeven dat er gedurende het opsporingsonderzoek, dat plaatsvindt onder het gezag van officier van justitie, sprake is van een strikte taakverdeling en functiescheiding. Hierbij is aangegeven dat deze functiescheiding het risico op tunnelvisie vermindert. De opsporingsambtenaren die verantwoordelijk zijn voor de voorbereiding en de uitvoering van het onderzoek in een geautomatiseerd werk maken deel uit van een technisch team en behoren niet tot het tactisch team. Het tactisch team is belast met het uitvoeren van het operationele onderzoek. Hierbij is in de toelichting bij het Bogw aangegeven dat de organisatorische scheiding tussen het technisch team en het tactisch team de samenwerking tussen de teams gedurende het opsporingsonderzoek niet behoeft te belemmeren. Afhankelijk van het verloop van het onderzoek kan de grens tussen het technisch optreden en het tactisch optreden verschillen, maar de samenwerking zal 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. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt, vervult hierbij een *schakelfunctie*.[63]

De Inspectie stelt vast dat tijdens de inzet van de bevoegdheid in 2019 direct telefonisch contact heeft plaatsgevonden tussen leden van het technisch team en leden van het tactisch team. Overigens heeft de Inspectie JenV geen aanwijzing dat het tactisch team tijdens de inzet van de bevoegdheid invloed heeft uitgeoefend op het binnendringen in het geautomatiseerde werk en op de plaatsing, inzet en verwijdering van een technisch hulpmiddel.

De Inspectie heeft van de teamleiding van DIGIT vernomen dat inmiddels is gestart met het uitwerken van procesbeschrijvingen waarin onder meer wordt vastgelegd hoe de communicatie tussen het technisch en tactisch team verloopt.

[62] Artikel 4 Bogw, inclusief de passage uit de nota van toelichting bij dit artikel.
[63] Nota van Toelichting Bogw. Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340), p. 17.

Bijlage Afkortingen en begrippen

Afkorting	Betekenis
Bogw	Besluit onderzoek in een geautomatiseerd werk
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)
College	College van procureurs-generaal, bepaalt het landelijke opsporings- en vervolgingsbeleid van het OM. Het College ziet erop toe dat er bij de strafrechtelijke handhaving van de rechtsorde sprake is van samenhang, consistentie en kwaliteit.
CTC	Centrale toetsingscommissie. De CTC, samengesteld uit leden van het openbaar ministerie en politie, is een intern adviesorgaan van het openbaar ministerie, dat het College adviseert omtrent de voorgenomen inzet van bepaalde bijzondere opsporingsbevoegdheden en methodieken.
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.
KMar	Koninklijke Marechaussee
OM	Openbaar Ministerie
PG-HR	Procureur-generaal bij de Hoge Raad der Nederlanden
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek

Begrip	Betekenis
binnendringsoftware	Software waarmee daadwerkelijk wordt ingebroken (bijvoorbeeld door misbruik te maken van een (onbekende) kwetsbaarheid). In de praktijk kan het voorkomen dat er gebruik wordt gemaakt van een softwarepakket dat bestaat uit onderdelen voor het verrichten van onderzoekshandelingen (een technisch hulpmiddel) en onderdelen voor het binnendringen van een geautomatiseerd werk. De wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk, maakt geen deel uit van het keuringsproces. In het geval binnendringsoftware wordt ingekocht wordt het functioneren in een testomgeving gecontroleerd. Tevens wordt in de procedure rondom de inzet van de bevoegdheid aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden.
geautomatiseerd werk	Een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.
tactisch team	Team dat is belast met de uitvoering van het operationele onderzoek.
technische infrastructuur	Technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel.
technisch team	Onderdeel van de Landelijke Eenheid dat is belast met de uitoefening van de hackbevoegdheid, dit team maakt deel uit van DIGIT.

Missie Inspectie Justitie en Veiligheid

De Inspectie Justitie en Veiligheid houdt voor de samenleving, de ondertoezichtgestelden en de politiek en bestuurlijk verantwoordelijken toezicht op het terrein van justitie en veiligheid
om inzicht te geven in de kwaliteit van de taakuitvoering en de naleving van regels en normen,
om risico's te signaleren
en om organisaties aan te zetten tot verbetering.
Hiermee draagt de Inspectie bij aan een rechtvaardige en veilige samenleving.

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

Juli 2020