Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Verslag toezicht wettelijke hackbevoegdheid politie 2022

Toezicht op de toepassing door de politie van de bevoegdheid tot het binnendringen en doen van onderzoek in een geautomatiseerd werk.

Inhoudsopgave

Voorwoord 3
1. Inleiding 5
Hackbevoegdheid 5
Aanleiding toezicht 5
Leeswijzer 6
2. Resultaten van het toezicht 8
2.1 Algemeen beeld 8
2.2 Bevindingen ter verbetering 9
2.2.1 Inzet commerciële software voldoet niet aan uitgangspunten 9
2.2.2 Inrichting en toepassing logging nog niet op orde 12
2.2.3 Verdere verbeteringen nodig in handmatige verslaglegging 13
2.2.4 Informatiebeveiliging nog steeds niet aantoonbaar op niveau 14
2.2.5 Voortgang kwaliteitszorg en interne controle stagneert 15
2.2.6 Vernietiging en omgang geheimhouderinformatie verdient aandacht 16
3. Conclusie en aanbevelingen 19
Aanbevelingen en het vervolg 22
Bijlage A: Detailbevindingen 24
A.1 Voorbereiding voorafgaand aan de inzet 24
Haalbaarheidsonderzoek 25
Plan van aanpak voor het binnendringen 25
A.2 Binnendringsoftware en melden onbekende kwetsbaarheden 26
Onbekende kwetsbaarheden 27
A.4 Uitvoering binnendringen en verrichten van onderzoekshandelingen 31
Onderzoekshandelingen met een technisch hulpmiddel 34
Onderzoekshandelingen middels handmatige inzet 41
Functiescheiding tussen technisch team en tactisch team 42
A.5 Logging en andere verslaglegging 42
Betrouwbaarheid logbestanden 46
Vastgelegde gegevens (bewijslogging) 48
Andere verslaglegging (proces-verbaal en journaal) 49
A.6 Bewerking en verstrekking van vastgelegde gegevens 50
A.7 Bewaartermijnen, verwijdering en vernietiging gegevens 51
A.8 Informatiebeveiliging, kwaliteitssysteem en interne controle 54

Bijlage B: Onderzoeksmethodiek 58
Afbakening en aanpak onderzoek 58
Bijlage C: Afkortingen 62
Bijlage D: Hoor- en wederhoortabel 63

Voorwoord

De politie heeft sinds 2019 voor de opsporing van bepaalde ernstige vormen van criminaliteit een krachtig middel beschikbaar: de hackbevoegdheid. De wetgever onderkent de noodzaak van dit middel. Wel hechtte hij grote waarde aan een rechtmatige en zorgvuldige inzet ervan om de inbreuk op de persoonlijke levenssfeer van de betrokkenen zoveel mogelijk te beperken. De politie mag deze bevoegdheid daarom alleen toepassen binnen strikte voorwaarden die in wet- en regelgeving zijn vastgelegd. Daarbij werd voorzien in een stelsel van maatregelen van controle en toezicht. Als onderdeel van dat stelsel is een belangrijke rol weggelegd voor de Inspectie Justitie en Veiligheid. Vanuit die uitdrukkelijke wens van de wetgever voor goed toezicht hebben wij de afgelopen jaren bij de politie - vanuit het perspectief van het publieke belang dat hiermee gemoeid is - met scherpte toezicht gehouden op de naleving van de wettelijke bepalingen van de hackbevoegdheid. In dit verslag rapporteert de Inspectie JenV voor het vierde jaar op rij over de uitkomsten van haar toezicht.

Onze belangrijkste conclusie is dat de politie na vier jaar nog steeds onvoldoende inhoud en opvolging geeft aan diverse regels en uitgangspunten voor het toepassen van de hackbevoegdheid. Veel van onze bevindingen over 2022 zijn gelijk aan die we al rapporteerden in de eerdere drie verslagen. Dit ondanks de inspanning die door de politie is geleverd. In het eerste verslagjaar hebben wij begrip getoond dat het voor de politie een nieuwe bevoegdheid betrof en dat het technisch team van de politie in opbouw was. In de jaren daarna hebben wij het uitblijven van verbeteringen als risico benoemd. Als toezichthouder vind ik het belangrijk dat een onder toezicht gestelde organisatie – in dit geval dus de politie – de risico’s en verbeterpunten die wij signaleren en aanreiken, oppakt en uitvoert. Vanzelfsprekend hebben we oog voor de praktische uitvoerbaarheid van de regels; we hebben daar in ons vorige verslag al op gewezen. Maar dat neemt niet weg dat de politie – juist door de grote waarde die de wetgever aan een zorgvuldige en rechtmatige inzet van de hackbevoegdheid hecht – de strikte voorwaarden die in wet- en regelgeving zijn vastgelegd op een juiste manier naleeft; ook als dat soms tot praktisch ongemak leidt.

Wij zijn natuurlijk niet doof voor de geluiden over uitvoeringsproblemen. We signaleerden in ons derde verslag al dat op enkele onderwerpen spanning is tussen de wettelijke kaders en de uitvoeringspraktijk. Die spanning is er altijd als een bevoegdheid sterk wordt ingekaderd door wettelijke bepalingen. Na vier jaar wordt goed zichtbaar in hoeverre wetgeving en uitvoeringspraktijk met elkaar samengaan. Als dan door voortschrijdend inzicht de behoefte ontstaat om het wettelijk kader aan te passen, dan is de wetgever aan zet om hierin te handelen. Het Wetenschappelijk Onderzoek- en Documentatie Centrum heeft vorig jaar een evaluatie uitgevoerd naar de hackbevoegdheid. De Inspectie JenV heeft er met haar verslagen aan willen bijdragen dat ervaren knelpunten en niet voorziene neveneffecten in de uitvoering van de bevoegdheid door wettelijke regels zichtbaar zouden worden en in die evaluatie zouden worden meegenomen. Op deze manier dragen we eraan bij dat de toepassing van de hackbevoegdheid door de politie ook

uitvoerbaar blijft. Indien besloten wordt tot aanpassing van het wettelijk kader, zal de Inspectie haar toezicht daar vanzelfsprekend op inrichten.

Ik hoop daarnaast dat dit verslag eraan bijdraagt dat de politie op korte termijn en met urgentie de verbeterpunten oppakt die wij haar als inspectie hebben aangereikt. Want de hackbevoegdheid is een belangrijk maar ook gevoelig middel voor de politie en daarmee de samenleving. Een dergelijk opsporingsmiddel verdient alle aandacht en urgentie.

Esther de Kleuver
Inspecteur-generaal Inspectie Justitie en Veiligheid

1. Inleiding

De politie en de bijzondere opsporingsdiensten zijn sinds 1 maart 2019 bevoegd om onder strikte voorwaarden heimelijk en op afstand binnen te dringen en onderzoek te doen in een geautomatiseerd werk (zoals een laptop of smartphone) dat in gebruik is bij een verdachte. Deze bevoegdheid wordt ook wel de 'hackbevoegdheid' genoemd.[1] De Inspectie Justitie en Veiligheid (hierna: de Inspectie) houdt toezicht op de uitvoering van deze bevoegdheid en doet daarover jaarlijks verslag. Voor het vierde achtereenvolgende jaar rapporteert de Inspectie met dit verslag over de inzet van de bevoegdheid door de politie.

Hackbevoegdheid

De hackbevoegdheid is geïntroduceerd in de Wet computercriminaliteit III (hierna: Wet CCIII). Deze wet is op 1 maart 2019 in werking getreden. De bevoegdheid is vastgelegd in de artikelen 126nba, 126uba en 126zpa Wetboek van Strafvordering. Op grond van deze artikelen kunnen opsporingsambtenaren die daarvoor aangewezen zijn, onder voorwaarden een geautomatiseerd werk, dat bij een verdachte in gebruik is, op afstand heimelijk binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Nadat een geautomatiseerd werk is binnengedrongen mogen onderzoekshandelingen worden verricht die al dan niet met een technisch hulpmiddel in een geautomatiseerd werk worden uitgevoerd. Met het uitvoeren van de onderzoekshandelingen worden gegevens vastgelegd die kunnen dienen als bewijs in een strafzaak. Hierbij kan gedacht worden aan het overnemen van e-mailberichten of het opslaan van locatiegegevens. 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 de bepalingen uit het wetboek van Strafvorderingen, zijn verdere regels omtrent de hackbevoegdheid onder andere beschreven in het Besluit onderzoek in een geautomatiseerd werk (hierna: Bogw of het Besluit). [2]

Aanleiding toezicht

Tijdens de parlementaire behandeling van het wetsvoorstel van de Wet computercriminaliteit III is door de toenmalige minister van Justitie en Veiligheid gemotiveerd dat het op afstand binnendringen in een geautomatiseerd werk een ernstige aantasting van de persoonlijke levenssfeer met zich mee kan brengen, omdat persoonlijke informatie ter kennis kan komen van de politie.[3] Daarnaast is door de toenmalige minister het belang benadrukt van de betrouwbaarheid, integriteit en herleidbaarheid van verkregen en vastgelegde gegevens die kunnen

[1] Daar waar de term "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.
[2] Volledig: 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 de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Stb., 2018, 340. De wettelijke grondslag van dit besluit is gelegen in artt. 126nba lid 1 en lid 8, 126uba lid 1 en lid 3, 126zpa lid 1 en lid 3, 126ee Sv, en art. 18 lid 1 van de Wet Politiegegevens.
[3] *Kamerstukken I*, 2017/2018, 34372, nr. G, p.1.

dienen als bewijs in een strafzaak. De hackbevoegdheid is om deze redenen volgens de wetgever aan strikte voorwaarden gebonden en met stevige waarborgen omkleed. De bevoegdheid mag uitsluitend worden ingezet in geval van verdenking van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, bij ernstige misdrijven in georganiseerd verband of bij aanwijzingen van een terroristisch misdrijf. De voorwaarden en waarborgen zijn ingesteld om te komen tot een rechtmatige en zorgvuldige inzet met betrekking tot de verdachte en anderen wiens gegevens mogelijk ter beschikking komen van de opsporing.[4]

De wetgever heeft daarbij tevens voorzien in een stelsel van maatregelen van controle en toezicht om de naleving van deze regels te waarborgen. Als onderdeel van dat stelsel is een belangrijke rol weggelegd voor de Inspectie.[5] De Inspectie is op grond van de Politiewet 2012 belast met het toezicht op de kwaliteit van de taakuitvoering door de politie. Het structurele[6] toezicht door de Inspectie is verder verankerd in het Wetboek van Strafvordering en het Bogw. Het toezicht van de Inspectie ziet toe op de uitvoering van het bevel van de officier van de justitie en op de naleving van wet- en regelgeving rond de toepassing van de hackbevoegdheid. Hierbij is tevens geregeld dat het toezicht van de Inspectie zich ook richt op de buitengewoon opsporingsambtenaren en bijzondere opsporingsdiensten.[7] Het toezicht omvat zowel de gevallen die de officier van justitie in het kader van strafvervolging aan de rechter voorlegt als gevallen die niet tot strafvervolging leiden.[8] 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 in voorkomende gevallen aan te zetten tot verbetering.[9] Indien uit haar toezicht structurele problemen blijken, dan kunnen die voor de Inspectie 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]

Leeswijzer

Dit rapport beschrijft de bevindingen van het toezicht op de hackbevoegdheid in de periode 1 januari 2022 tot en met 31 december 2022. Het rapport is als volgt opgebouwd. In hoofdstuk 2 worden de belangrijkste bevindingen van het toezicht op hoofdlijnen beschreven. Als eerste wordt in paragraaf 2.1 het algemeen beeld geschetst over de inzet van de hackbevoegdheid in 2022. Hierna volgen in paragraaf 2.2 de belangrijkste verbeterpunten per thema. In paragraaf 2.2.1 wordt ingegaan op de bevindingen met betrekking tot het gebruik van commerciële software, hierna volgen de bevindingen met betrekking tot het gebruik en de toepassing van logging (paragraaf 2.2.2), de verslaglegging (paragraaf 2.2.3), informatiebeveiliging (paragraaf 2.2.4) en de kwaliteitszorg (paragraaf 2.2.5). Als laatste worden in paragraaf 2.2.6 de bevindingen besproken over het vernietigen van gegevens en over de verwerking van geheimhouderinformatie door DIGIT. Het

[4] *Kamerstukken I*, 2017/18, 34372, G, p.2.
[5] *Kamerstukken I*, 2017/18, 34372, G, p.19.
[6] *Kamerstukken I*, 2017/18, 34372, G, p.10.
[7] Art. 126nba lid 7 Sv; Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 23.
[8] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 23; *Kamerstukken II* 2016/17, 34 372, nr.6, p.82.
[9] Meerjarenperspectief 2021-2024, Inspectie Justitie en Veiligheid. https://www.inspectie-jenv.nl/actueel/nieuws/2021/02/11/inspectie-jenv-publiceert-meerjarenperspectief-2021-2024
[10] *Kamerstukken I*, 2017/18, 34 372 G, p. 20.

rapport sluit af met de conclusie en de aanbevelingen. Het rapport bevat vier bijlagen. In bijlage A worden de detailbevindingen besproken. Bijlage B beschrijft de gehanteerde onderzoeksmethodiek. Bijlage C bevat de afkortingenlijst en in bijlage D is de hoor- en wederhoortabel opgenomen. In de hoor- en wederhoortabel heeft de politie hun wederhoorreactie beschreven. De tabel is aangevuld met de reactie van de Inspectie hierop.

2. Resultaten van het toezicht

In dit hoofdstuk beschrijft de Inspectie de belangrijkste resultaten van haar toezicht in de periode 1 januari 2022 tot en met 31 december 2022. Als eerste wordt een kort algemeen beeld geschetst. Daarna wordt ingegaan op de belangrijkste bevindingen van het toezicht die de Inspectie ter verbetering signaleert. Details en overige bevindingen zijn nader beschreven in de bijlage A van dit verslag.

2.1 Algemeen beeld

In het eerste verslag van de Inspectie over 2019 was sprake van acht zaken waarin de politie de hackbevoegdheid heeft toegepast. In 2020 en 2021 was sprake van respectievelijk 14 en 28 zaken. In 2022 heeft DIGIT in 31 zaken bevel gekregen voor het toepassen van de bevoegdheid tot het binnendringen en het doen van onderzoek in een geautomatiseerd werk.

Onderwerp	**Aantal**
Totaal aantal zaken waarin DIGIT bevel heeft gekregen om in 2022 de wettelijke hackbevoegdheid toe te passen op grond van de Wet CCIII[11]	31
Aantal van deze zaken waarin bevel is gegeven voor de inzet van een technisch hulpmiddel dat vooraf goedgekeurd is	*4*
Aantal van deze zaken waarin bevel is gegeven voor de inzet van een niet vooraf gekeurd technisch hulpmiddel	*26*
Aantal zaken waarin onderzoekshandelingen handmatig zijn uitgevoerd[12]	*8*
Aantal van deze zaken waarin commerciële binnendringsoftware is ingezet	*25*
Aantal van deze zaken waarin door de politie aangetroffen onbekende kwetsbaarheden door DIGIT zijn gebruikt	*3*
Aantal ter keuring aangeboden technische hulpmiddelen	3
Aantal van deze technische hulpmiddelen die zijn goedgekeurd	*3*

Bovenstaande tabel geeft inzicht in het aantal zaken waarin deze bevoegdheid in 2022 is ingezet.[13] Tevens is hierin opgenomen in hoeveel zaken de politie commerciële binnendringsoftware en door hen aangetroffen onbekende kwetsbaarheden[14] heeft gebruikt. Ten slotte is in de tabel opgenomen hoeveel

[11] Per zaak kunnen meerdere bevelen voor de inzet van de hackbevoegdheid zijn afgegeven, waaronder eventuele verlengingen, aanvullingen of wijzigingen. Een eerste bevel in deze zaken kan al in 2021 of eerder afgegeven zijn. Hierdoor kan een dubbeling ontstaan met de telling uit de overzichten uit eerdere verslagen van de Inspectie.

[12] In één zaak kunnen zowel bevelen afgegeven zijn voor het verrichten van onderzoekshandelingen met als zonder technisch hulpmiddel (handmatig).

[13] De Inspectie hanteert als uitgangspunt in de telling dat (een deel van) de periode van een afgegeven bevel voor de toepassing van de hackbevoegdheid in een zaak valt binnen de periode waarover de Inspectie in dit verslag rapporteert, namelijk 1 januari t/m 31 december 2022.

[14] Onder onbekende kwetsbaarheid wordt volgens artikel 126ffa lid 4 Sv verstaan "een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen."

technische hulpmiddelen de politie heeft laten keuren en hoeveel hiervan zijn goedgekeurd door de keuringsdienst. Het algemeen beeld van de Inspectie is dat de hackbevoegdheid in 2022 voornamelijk is ingezet voor onderzoeken gericht op mobiele telefoons. Bij deze zaken is een commercieel technisch hulpmiddel ingezet.

De Inspectie stelt vast dat DIGIT in het overgrote deel van de zaken binnen de reikwijdte van de afgegeven bevelen heeft gehandeld. Waar sprake is geweest van een afwijking met mogelijke gevolgen voor een rechtmatige inzet van de bevoegdheid heeft DIGIT dit zelf tijdig onderkend en maatregelen genomen. De binnengehaalde gegevens zijn verwijderd en niet overgedragen aan het tactisch team. De Inspectie constateert dat indien sprake was van een (mogelijke) afwijking tussen het bevel en de uitvoering altijd door DIGIT afstemming is gezocht met de DIGIT-officier van justitie voor verdere oordeelsvorming en besluitvorming. Het detecteren van afwijkingen in de uitvoering is echter nog geen ingericht en ingebed proces binnen DIGIT. Hierdoor is sprake van een grote afhankelijkheid van de oplettendheid van de individuele medewerkers. Dit onderstreept het belang van voortgang op het gebied van kwaliteitszorg en interne controle (zie paragraaf 2.2.5).

Bij het uitvoeren van onderzoekshandelingen met een zogenoemd technisch hulpmiddel is het uitgangspunt dat deze handelingen worden verricht met een hiervoor goedgekeurde softwareapplicatie. De Inspectie stelt vast dat de keuringsdienst van de Landelijke Eenheid van de politie de keuringen van de aangeboden technische hulpmiddelen heeft uitgevoerd volgens de daaraan gestelde eisen. Het gevolgde keuringsproces en de totstandkoming van de keuringsuitslag is goed navolgbaar. De Inspectie constateert evenals in 2021 dat de personele bezetting van de keuringsdienst van de Landelijke Eenheid kwetsbaar is. Net als in 2021 was slechts één medewerker inzetbaar voor de uitvoering van dit type keuringen.

2.2 Bevindingen ter verbetering

Naast de hiervoor genoemde positieve bevindingen ziet de Inspectie dat de politie zich op een aantal gebieden niet houdt aan de regels en uitgangspunten bij de toepassing van de hackbevoegdheid. Deze afwijkingen zijn ook benoemd in de voorgaande verslagen van de Inspectie.[15] In de volgende paragrafen volgen de belangrijkste bevindingen van het toezicht die de Inspectie ter verbetering signaleert.

2.2.1 Inzet commerciële software voldoet niet aan uitgangspunten

De inzet van commerciële software is tijdens de parlementaire behandeling van de wet CCIII een veelbesproken onderwerp geweest. Ook recent is de mogelijke inzet van commerciële software door opsporings- en inlichtingendiensten het onderwerp

[15] Verslag 2019, https://www.inspectie-jenv.nl/Publicaties/rapporten/2020/08/20/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019 ; Verslag 2020, https://www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020 ; Verslag 2021, https://www.inspectie-jenv.nl/Publicaties/rapporten/2022/05/31/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2021

van het politieke en het maatschappelijk gesprek. Dit maakt dat het ook in 2023 een actueel thema is.

In de parlementaire behandeling van de wet CCIII zijn door de toenmalig minister toezeggingen gedaan over het gebruik van commerciële software. Zo is toegezegd dat de geïnfecteerde geautomatiseerde werken niet in verbinding mogen staan met een server van de leverancier van de binnendringsoftware en dat alleen aangewezen ambtenaren toegang mogen hebben tot het systeem (i.c. een server) van waaruit het binnendringen wordt uitgevoerd. Bij software voor het uitvoeren van onderzoekshandelingen is tevens toegezegd dat de leverancier geen mogelijkheid dient te hebben om zelfstandig updates uit te voeren en zelf de controle over het geautomatiseerd werk over te nemen. Tevens geldt de regel dat de, met de onderzoekshandelingen, verkregen gegevens uitsluitend toegankelijk mogen zijn voor de door de korpschef aangewezen ambtenaren.

De wetgever heeft daarnaast als algemeen uitgangspunt gesteld dat software die als technisch hulpmiddel is aangemerkt, vooraf goedgekeurd moet zijn als deze middelen worden ingezet. Als een technisch hulpmiddel is gekeurd mag men er vanuit gaan dat voldaan is aan de wettelijke eisen, waaronder aan de eis dat het transport van de verzamelde gegevens naar een technische infrastructuur binnen de politieorganisatie beveiligd dient te zijn tegen wijziging van de werking ervan en wijziging en kennisneming van geregistreerde gegevens door onbevoegde personen.[16] In uitzonderingsgevallen kan de keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet.[17] Van deze uitzondering zal in de praktijk niet lichtzinnig gebruik worden gemaakt.[18]

De aanschaf van commerciële binnendringsoftware met mogelijk onbekende kwetsbaarheden[19] is in het Regeerakkoord 2017–2021 beperkt. Toegezegd is dat de markt voor onbekende kwetsbaarheden zo min mogelijk moet worden gestimuleerd. Om deze reden dient de aanschaf van licenties voor deze software per zaak plaats te vinden. Tijdens de parlementaire behandeling is toegezegd dat de inzet van deze commerciële binnendringsoftware met mogelijk onbekende kwetsbaarheden moet worden beperkt tot uiterste gevallen. De software mag alleen worden ingezet als lichtere middelen niet mogelijk zijn. De afweging en besluitvorming per zaak daarover wordt overigens gedaan door het OM.

Evenals in eerdere verslagjaren heeft de politie in 2022 in het merendeel van de zaken gebruik gemaakt van commerciële software. Bij de gebruikte commerciële software is de functionaliteit van het binnendringen gecombineerd met een technisch hulpmiddel voor het uitvoeren van onderzoekshandelingen. Voor zowel de politie als de Inspectie is deze software een 'black box'. Het kenmerk van een 'black box' is dat de resultaten zichtbaar zijn, maar voor de gebruiker niet bekend is hoe de software precies werkt en of deze software gebruik maakt van onbekende kwetsbaarheden. De Inspectie heeft er begrip voor dat deze software in het belang

[16] *Kamerstukken I* 2016/17, 34 372 nr. D, p. 19 en 20
[17] Art. 21 lid 4 Bogw.
[18] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 45.
[19] Onbekende kwetsbaarheden (of zerodays) zijn fouten in software die nog onbekend zijn bij de maker van de software. De maker heeft geen dagen gehad om het gat te dichten.

van de opsporing veelvuldig wordt ingezet, maar signaleert dat hierdoor spanning ontstaat met het rechtskader.

Toegang leverancier

De politie heeft in een addendum bij het contract procedurele afspraken gemaakt met de leverancier, waaronder het beperken van toegang door de leverancier tot de verzamelde gegevens. Deze afspraken zijn echter niet technisch afdwingbaar en controleerbaar. Hierdoor is het onzeker wat de leverancier van deze software precies en op welk moment doet. Dit geldt bijvoorbeeld voor werkzaamheden die de leverancier uitvoert aan de software. Deze werkzaamheden kunnen ongewenste en onbedoelde gevolgen hebben voor de werking en functionaliteit van de software. De werkzaamheden kunnen ook worden uitgevoerd tijdens de uitvoering van een bevel, dus als een apparaat reeds is gehackt. De leverancier kan technisch gezien ook toegang verkrijgen tot de met deze software verkregen gegevens. De politie kan niet uitsluiten dat de geïnfecteerde geautomatiseerde werken in verbinding staan met een server van de leverancier. Dit is dan ook niet in lijn met de toezeggingen die door de toenmalig minister zijn gedaan.

Achterwege blijven keuring

Evenals in voorgaande jaren stelt de Inspectie vast dat in het merendeel van de zaken een commercieel technisch hulpmiddel is ingezet, dat niet vooraf goedgekeurd is. Dit geldt voor een specifieke categorie inzetten, namelijk voor het uitvoeren van onderzoekshandelingen op mobiele telefoons. Dit is niet in lijn met het door de wetgever gestelde uitgangspunt dat technische hulpmiddelen in beginsel vooraf goedgekeurd zijn als deze worden ingezet. Door het OM is, in deze zaken, als uitzondering op de hoofdregel bepaald dat het onderzoeksbelang dringend vordert dat een niet vooraf goedgekeurd technisch hulpmiddel wordt ingezet. In een deel van de zaken is inmiddels door het OM beslist dat het ingezette technisch hulpmiddel vanwege zijn aard niet te keuren is en dat daarmee ook een keuring achteraf achterwege blijft. Gelet op het feit dat de hackbevoegdheid voor het merendeel van de zaken in 2022 is ingezet voor het hacken van telefoons met een commercieel technisch hulpmiddel (dat door zijn aard niet te keuren is) signaleert de Inspectie dat hiermee de door de wetgever voorziene uitzonderingen van het inzetten van een niet vooraf goedgekeurd technisch hulpmiddel en het afzien van keuring achteraf, standaardpraktijk zijn geworden. De Inspectie benadrukt dat de besluitvorming door de officier van justitie buiten de reikwijdte van het toezicht door de Inspectie valt. De Inspectie acht het van belang deze bevinding op te nemen in het rapport gelet op de het maatschappelijke en politieke gesprek over commerciële software.

Aanschaf licenties

Om de markt voor onbekende kwetsbaarheden zo min mogelijk te stimuleren dient de aanschaf van licenties voor deze software per zaak plaats te vinden. De Inspectie signaleert, evenals over de drie afgelopen jaren, 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.

Zie hoofdstuk A.2 (binnendringsoftware) en hoofdstuk A.4 (binnendringen en communicatie met leverancier technisch hulpmiddel) in de bijlage voor de detailbevindingen.

2.2.2 Inrichting en toepassing logging nog niet op orde

Onder logging verstaat het Besluit de elektronische verslaglegging over de uitvoering van een bevel. Zoals is toegezegd door de minister geldt de logplicht zowel voor de handelingen in de voorbereidende fase als voor de handelingen die gedurende de onderzoeksfase worden verricht. De logging is van belang zodat zowel tijdens als na afloop van een hack geen twijfel kan bestaan over aard en consequenties van de handelingen die door de politie zijn verricht bij de uitvoering van het bevel.[20] Deze logging kan worden gebruikt ter verificatie van de betrouwbaarheid, integriteit en herleidbaarheid van de verkregen gegevens. Dit is van belang omdat deze gegevens gebruikt kunnen worden als bewijs in strafzaken. Daarnaast heeft ook de Inspectie deze logging nodig om effectief toezicht uit te kunnen oefenen.

Ook in 2022 heeft de politie nog niet vooraf beschreven op welke wijze zij invulling geeft aan het vereiste van een doorlopende en automatische vastlegging van gegevens in logbestanden. De wijze van loggen kan door het gebruik van verschillende hacktechnieken en middelen per inzet verschillen. De Inspectie constateert dat voor de inrichting en toepassing van de logging de politie vooral als uitgangspunt heeft genomen wat technisch standaard voorhanden is binnen de gebruikte toepassingen[21], in plaats van wat op basis van een risicoanalyse nodig is en wat volgt als vereiste uit het Bogw. Hierdoor is wel veel logging aanwezig en is daarmee technisch gezien sprake van doorlopende en automatische logging op verschillende niveaus. DIGIT kan echter niet aantonen dat deze beschikbare logging voldoende effectief is gelet op het doel en het gebruik van de logging.

Het inrichten van logging is een activiteit die procesmatig moet worden ingericht en worden uitgevoerd op basis van een risicoanalyse. Deze slag moet nu worden gemaakt. Onderdeel hiervan is dat door de politie vooraf wordt beschreven op welke wijze invulling wordt gegeven aan het vereiste van een doorlopende en automatische vastlegging van gegevens in logbestanden en op welk moment DIGIT overgaat tot handmatige vastlegging. Hierbij dient vooraf door DIGIT nagedacht te worden over welke informatie in de logging noodzakelijk is voor de controle van de betrouwbaarheid en integriteit van de gegevens en de controleerbaarheid van de uitgevoerde handelingen. Het is aan DIGIT om ontwerpkeuzes te maken en te kunnen verantwoorden welke gebeurtenissen op welke wijze worden gelogd om afwijkingen en risico's tijdig te kunnen signaleren. Het is dan ook aan te bevelen om de ontwerpkeuzes voor de logging te baseren op voorbedachte scenario's en gebruikssituaties, waaronder scenario's gericht op het detecteren van vooraf gedefinieerde onregelmatigheden. Het risico bestaat anders dat het optreden daarvan niet kan worden gesignaleerd omdat de inrichting van logging daarin niet voorziet.

Duidelijkheid is ook van belang voor de politie om te kunnen komen tot het treffen van passende maatregelen voor de betrouwbaarheid en de integriteit van de betreffende logbestanden. Deze maatregelen dienen in de gehele keten getroffen te worden. Dit strekt zich uit vanaf de bron waar deze logbestanden gegenereerd

[20] *Kamerstukken I* 2016/17, 34372 nr. D, p.6 en *Kamerstukken II* 2015/16, 34372 nr. 3, p.31.
[21] De Inspectie doelt hier op diverse ICT-componenten waaronder servers, werkstations, netwerkcomponenten zoals firewalls en applicaties.

worden, tot en met het transport en de eventuele (tussentijdse) verwerking en opslag daarvan.

Ook het functioneren van de technische infrastructuur moet worden gelogd. Hierbij is het belangrijk dat de politie bepaalt wat de reikwijdte van de technische infrastructuur is, zodat duidelijk wordt wat daaronder valt. Dit heeft de politie in 2022 nog niet volledig bepaald.

De Inspectie stelt vast dat beschikbare logging door de politie veelal op ad-hocbasis gebruikt wordt om zowel tijdens de uitvoering van het bevel als achteraf toe te zien en eventuele afwijkingen of onregelmatigheden te signaleren. Zoals ook in eerdere jaren door de Inspectie is gerapporteerd, is niet door de politie uitgewerkt op welke wijze, door wie en wanneer het structureel monitoren vanuit een interne verantwoordelijkheid plaatsvindt. Dit is naar oordeel van de Inspectie illustratief voor het nog onvoldoende ontwikkeld en effectief zijn van de eigen controle van de politie.

Beeldschermopnamen en opname van toetsaanslagen

In de praktijk wordt voor de logging vooral gesteund op beeldscherm- en toetsaanslagopnamen. In eerdere verslagjaren heeft de Inspectie gerapporteerd dat deze vorm van logging niet altijd volledig was. Alhoewel de Inspectie in haar verslag over 2021 heeft gemeld dat in de loop van dat jaar deze logging was verbeterd, is in de eerste maanden van 2022 gebleken dat deze opnamen, mede door technische problemen niet altijd aanwezig waren. Door de Inspectie is vastgesteld dat in de loop van 2022 een nieuwe opnamevoorziening is ontwikkeld en is ingezet. Deze extra voorziening is gebaseerd op andere technologie waardoor de opnamen gedurende de rest van het jaar wel volledig zijn.

De Inspectie signaleert echter dat deze opnamevoorzieningen slecht geschikt zijn om zonder gerichte aanwijzingen onderzoek te doen naar het optreden van mogelijke afwijkingen of onregelmatigheden. Reden hiervoor is de grote hoeveelheid van deze schermopnamen. Ook de opname van de toetsaanslagen zijn voor dit doel van beperkte waarde gebleken. De Inspectie constateert dat met alleen deze vorm van logging er geen effectieve uitvoering gegeven wordt aan het wettelijk vereiste dat onregelmatigheden zowel tijdens de uitvoering van een bevel als achteraf vastgesteld moeten kunnen worden. De Inspectie verwijst daarvoor naar de hiervoor beschreven benodigde nadere uitwerking door DIGIT van de (ontwerp)keuzen van de inrichting van de logging om invulling te (kunnen) geven aan het door de wetgever beoogde doel van de toepassing en gebruik van logging.

Zie hoofdstuk A.5 in de bijlage voor de detailbevindingen.

2.2.3 Verdere verbeteringen nodig in handmatige verslaglegging

Het Besluit stelt als uitgangspunt voor de logging dat vastlegging doorlopend en automatisch plaatsvindt. De gegevens over de verrichte handelingen (inzetlogging) mogen als uitzondering handmatig vastgelegd worden als deze gegevens naar hun aard niet automatisch vastgelegd kunnen worden. De nota van toelichting benoemt in dit kader het journaal van de opsporingsambtenaar en de vastlegging van

gebruikte scripts en softwareversies. In het journaal wordt door de opsporingsambtenaren, als een soort dagboek, handmatig verslaglegging gedaan over het procesverloop, de afspraken en de verrichtingen die zich niet lenen voor automatische vastlegging.

De Inspectie constateert ten opzichte van 2021 verbeteringen in de detaillering van het journaal. Hierover is zij positief. De Inspectie constateert wel dat niet in alle gevallen het journaal een juiste weergave biedt. Ook ontbreken registraties van handelingen en is de vastlegging in het journaal niet in alle gevallen duidelijk. De kwaliteit van de verantwoording in het journaal lijkt daarbij sterk af te hangen van de individuele opsporingsambtenaar die zorggedragen heeft voor de registratie. Evenals vorig jaar stelt de Inspectie vast dat niet controleerbaar is vastgelegd welke (versies van) scripts op welk moment zijn ingezet.

Onjuiste of onvolledige handmatige verslaglegging heeft direct gevolgen voor de juistheid van de processen-verbaal omdat de processen-verbaal gebaseerd zijn op de informatie uit het journaal. De Inspectie heeft waargenomen dat de afgelegde verantwoording in enkele processen-verbaal op onderdelen niet geheel overeenkomt met de daadwerkelijke uitvoering. Zo blijkt op basis van systeemlogging dat bepaalde opsporingsambtenaren betrokken zijn geweest bij uitvoeren van onderzoekshandelingen maar dat zij niet als verbalisant zijn opgenomen in het proces-verbaal en in het journaal. Daarnaast is een juist en volledig journaal van groot belang omdat DIGIT door het Openbaar Ministerie geïnstrueerd is om in het belang van de afscherming van opsporingsmethodieken en -middelen minimaal te verbaliseren en maximaal te journaliseren.

Zie hoofdstuk A.5 (logging en andere verslaglegging) in de bijlage voor de detailbevindingen.

2.2.4 Informatiebeveiliging nog steeds niet aantoonbaar op niveau

Het Besluit stelt eisen aan de (informatie)beveiliging. Ook heeft de politie zelf eisen gesteld aan deze beveiliging. In de beleidsreactie van de minister op het verslag van de Inspectie over 2021 is daarnaast toegezegd dat de aanpak van informatiebeveiliging geïntensiveerd zou worden.[22]

Ook in 2022 stelt de Inspectie vast dat de voortgang van het planmatig aantoonbaar en controleerbaar op niveau brengen en houden van beheersingsmaatregelen voor de (informatie)beveiliging stagneert. Dit betekent dat, evenals voorgaande jaren, DIGIT onvoldoende is nagegaan of haar processen en systemen voldoen aan de gestelde eisen.

De politie heeft, evenals in 2021, nog geen samenhangend pakket van de te treffen beheersings- en beveiligingsmaatregelen vastgesteld. Op specifieke onderdelen zijn er door DIGIT in 2022 enkele technische maatregelen doorgevoerd. Deze maatregelen zijn nog niet in alle gevallen volledig en juist doorgevoerd. De Inspectie stelt vast dat DIGIT in 2022 geen aantoonbare verantwoording kon overleggen over de inrichting van beveiligingsmaatregelen en het functioneren

[22] Kamerbrief met 1e halfjaarbericht 2022 politie, 17 juni 2022.

daarvan. De Inspectie kan hierdoor ook in 2022 voor haar toezicht niet steunen op een intern beheersingsmechanisme ten aanzien van informatiebeveiliging. Zie hoofdstuk A.8 in de bijlage voor de detailbevindingen.

Autorisatie- en toegangsbeheer

De Inspectie stelt vast dat ook in 2022 het autorisatiebeheerproces voor de eigen systemen en toepassingen van DIGIT nog niet goed is ingericht. Het proces voor het aanvragen, accorderen, uitvoeren, controleren en intrekken van autorisaties en het beleggen daarvan is nog in ontwikkeling. Aan de vastlegging van de uitgangspunten in de vorm van autorisatiematrices werd door DIGIT in 2022 nog gewerkt.

Voor het beperken van het risico voor ongeautoriseerde toegang vertrouwt DIGIT op maatregelen waarmee de fysieke toegang tot haar locatie wordt beperkt. In 2022 is het echter niet mogelijk gebleken inzicht te krijgen in de uitgegeven autorisaties voor deze fysieke toegang.

Het vastleggen van de uitgangspunten, het hebben van inzicht en het periodiek (laten) uitvoeren van controles van de juistheid van deze autorisaties levert een belangrijke bijdrage aan het aantoonbaar beperken van het risico voor onbevoegde toegang en kennisname.

2.2.5 Voortgang kwaliteitszorg en interne controle stagneert

De Inspectie heeft de afgelopen jaren aandacht gevraagd voor de uitwerking en toepassing van de kwaliteitszorg door de politie waaronder de interne controle van het operationele proces en een controleerbare en aantoonbare juiste werking van de informatiebeveiliging. De Inspectie stelt vast dat de ontwikkeling en toegezegde inbedding van kwaliteitszorg en de bijbehorende (interne) controle stagneert. Alhoewel er kleine stapjes gezet zijn en soms in de praktijk ook toegepast, blijft er ook in 2022 sprake van een versnipperde aanpak en inrichting. De Inspectie constateert dat op deze onderwerpen door de politie ook in 2022 weinig vooruitgang is geboekt. Overeenkomstig haar bevindingen in 2021 constateert de Inspectie dat de politie nog niet in beeld heeft gebracht voor welke onderdelen van de belangrijkste (werk)processen kwaliteitsbewaking en interne controle moet worden ingericht. Een overkoepelende visie waarin deze activiteiten in samenhang gebracht zijn en welke instrumenten daartoe door wie, wanneer moeten worden ingezet, is nog niet gereed. Niet bepaald is wie precies welke taken en verantwoordelijkheden hierin heeft. Ook is niet bepaald hoe en aan wie verantwoording over de uitvoering en resultaten daarvan wordt afgelegd. Tevens ontbreekt documentatie om de kwaliteit van de taakuitvoering te borgen en te voorkomen dat dit uitsluitend rust op de professionele inschatting van individuele medewerkers. Hierdoor ontbreekt structurele borging.

Zie hoofdstuk A.8 in de bijlage voor de detailbevindingen.

2.2.6 Vernietiging en omgang geheimhouderinformatie verdient aandacht

In haar verslag over 2021 heeft de Inspectie aandacht gevraagd voor de noodzaak dat de politie haar processen, procedures en technische voorzieningen zodanig inricht en toepast dat op het moment dat de officier van justitie daartoe verzoekt, gegevens tijdig, juist en volledig worden verwijderd en vernietigd.

Van een dergelijke situatie kan sprake zijn als met de hackbevoegdheid geheimhouderinformatie is verzameld.[23] Dergelijke gegevens dienen op grond van artikel 126aa Sv te worden vernietigd. Het beschermen van dergelijke informatie heeft als doel': 'cliënten en andere belanghebbenden zekerheid te geven dat zij vrijelijk met [bijvoorbeeld] de advocaat kunnen spreken.'[24] [25] Uit jurisprudentie volgt dat deze gegevens onmiddellijk dienen te worden vernietigd, zodat is verzekerd dat de gegevens geen deel uitmaken van de processtukken en het verdere verloop van het strafproces, waaronder ook het eindonderzoek ter terechtzitting.[26]

De procedure voor de vernietiging van de vastgelegde gegevens is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.[27] Op grond van dit besluit dient de opsporingsambtenaar onverwijld de officier van justitie in kennis te stellen als hij weet of redelijkerwijs kan vermoeden dat mededelingen zijn gedaan door een geheimhouder. De officier van justitie beoordeelt vervolgens of de gegevens vernietigd dienen te worden en indien dit het geval is wordt een schriftelijk bevel hiervoor afgegeven. Ook kan op grond van het besluit de officier van justitie bij voorbaat een generiek bevel tot vernietiging aan de opsporingsambtenaar verstrekken. De vernietiging kan dan terstond plaatsvinden, zonder tussenkomst van de officier. Daarnaast is in 2011 het systeem van nummerherkenning opgenomen in het Besluit bewaren en vernietigen niet-gevoegde stukken. Indien een advocaat gebruik maakt van een nummer dat overeenkomstig de regeling is aangemeld, wordt dit nummer door middel van een geautomatiseerd systeem herkend. Het opnemen van de communicatie dient automatisch te worden beëindigd en mogelijk opgenomen communicatie wordt onmiddellijk vernietigd. Deze werkwijze is ook van toepassing op de hackbevoegdheid als sprake is van het aftappen van telecommunicatie.[28]

Herkennen van geheimhouderinformatie

De Inspectie constateert dat in 2022 de DIGIT-officier van justitie door DIGIT onverwijld in kennis gesteld wordt indien de opsporingsambtenaren van DIGIT bij toeval kennisnemen van de aanwezigheid van mogelijke geheimhouderinformatie. Er zijn echter aan de kant van DIGIT geen processen, werkinstructies en

[23] Geheimhouderinformatie betreft informatie, zoals documenten en communicatie, die onder de geheimhoudersplicht vallen. Bepaalde beroepsgroepen hebben deze plicht, zoals advocaten, artsen of notaris (zogenaamde verschoningsgerechtigde). Artt. 218 en 218a Sv.
[24] Zie onder andere HR 1 maart 1985, ECLI:NL:HR:1985:AC9066 en Gerechtshof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329, r.o. 3.6.1.
[25] Het verschoningsrecht is geen absoluut recht. In zeer uitzonderlijke omstandigheden kan het belang dat de waarheid aan het licht komt, prevaleren boven het verschoningsrecht (vlg. HR 2 maart 2010, ECLI:NL:HR:BJ9262).
[26] Zie onder andere HR 12 januari 1999, LJN ZD1402, NJ 1999, 290 en ECLI:NL:HR:2007:BA5632
[27] Art.4 lid 1 en lid 2 Bogw.
[28] *Kamerstukken II 2016/16*, 34372, nr. 3, p. 18.

ondersteunende systemen zoals nummerherkenning ingericht om geheimhouderinformatie te herkennen. De, door DIGIT vastgelegde gegevens, worden als geheel - dus inclusief mogelijke geheimhouderinformatie – overgedragen.[29]

Door de gegevens in zijn geheel over te dragen uit de afgeschermde omgeving van DIGIT, wordt het risico vergroot dat dergelijke gegevens in de processtukken terecht kunnen komen. Ook verhoogt deze werkwijze het risico dat de kring van personen die mogelijk kennis kunnen nemen van geheimhouderinformatie onnodig wordt vergroot. Het is dan ook aan te bevelen dat DIGIT zich inspant waarborgen, waaronder nummerherkenning, in te richten om geheimhouderinformatie in een vroeg stadium te kunnen herkennen. Hiermee wordt uitdrukkelijk geen inhoudelijk toets bedoeld, maar slechts een technische filtering.

Een dergelijke werkwijze sluit aan bij het Besluit onderzoek in een geautomatiseerd werk waarin staat beschreven dat het technische team zorgdraagt voor de selectie van onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team.[30] Bij de selectie van gegevens dient op grond van het besluit gebruik te worden gemaakt van een forensische kopie van de ter uitvoering van het bevel vastgelegde gegevens. Het technische team dient dan vast te leggen welke bewerkingen hebben plaatsgevonden met betrekking tot de op de forensische kopie vastgelegde gegevens.[31] Ook kan hiermee vooruit worden gelopen op het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering waarin een werkwijze wordt beschreven waarbij gegevens die mogelijk toebehoren aan een verschoningsgerechtigde worden uitgefilterd.[32]

Vernietigen

Met betrekking tot het vernietigen onderscheidt de Inspectie twee bevindingen. Ten eerste constateert de Inspectie dat het proces van vernietigen ook in 2022 nog onvoldoende is uitgewerkt. De Inspectie baseert zich hiervoor op een situatie dat sprake was van een bevel tot vernietiging en dat het bij DIGIT voor geruime tijd onduidelijk was welke gegevens vernietigd moesten worden, waar deze gegevens zich bevonden en hoe de vernietiging plaats moest vinden. Ook wijst de Inspectie op wetgeving waarin onderscheid gemaakt wordt tussen vernietigen en verwijdering van gegevens en het bewaken van bijbehorende termijnen daarvoor. De Inspectie heeft in haar verslag 2021 aandacht gevraagd voor het uitwerken en oppakken van deze onderwerpen door de politie zodat zij daarop tijdig kan anticiperen. De Inspectie constateert dat de politie ook in 2022 geen nadere uitwerking en invulling hieraan heeft gegeven. De Inspectie beveelt aan om het proces van vernietigen zodanig uit te werken, dan indien sprake is van een situatie dat gegevens dienen te worden vernietigd, dat de vernietiging juist, volledig en direct kan worden uitgevoerd en dat de vernietiging op zodanige wijze wordt

[29] In Inspectie heeft geen onderzoek gedaan naar de omgang met geheimhouderinformatie na de overdracht van de gegevens door DIGIT en heeft dan ook geen bevindingen over dit deel van het proces.
[30] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 17.
[31] Artikel 29 Bogw.
[32] Memorie van toelichting bij het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, juli 2020, v.a. pagina 532.

vastgelegd dat dit ook controleerbaar is voor zowel de eigen organisatie, als de Inspectie.

Ten tweede stelt de Inspectie vast dat gegevens, ook na de onderkenning als geheimhouderinformatie, bij DIGIT beschikbaar zijn en blijven. Geheimhouderinformatie wordt niet vernietigd in de systemen van DIGIT. Reden hiervoor is dat de officier van justitie geen bevel tot vernietiging af heeft gegeven aan DIGIT om de gegevens te vernietigen. Door de DIGIT-officier van justitie is gemotiveerd dat sprake is van tegenstrijdige regelgeving waarbij het vernietigen van gegevens door DIGIT niet in overeenstemming is met het Besluit Onderzoek in een geautomatiseerd werk. Hierin wordt geregeld dat gegevens die zijn vastgelegd in de technische infrastructuur niet gewijzigd mogen worden. Dit resulteert in een werkwijze waarbij geheimhouderinformatie nog beschikbaar blijft binnen de politie. De Inspectie verbindt hieraan echter geen waardeoordeel gelet op het feit dat de politie hier handelt op aangeven van het OM en de Inspectie geen toezicht houdt op het openbaar ministerie. De Inspectie signaleert echter wel een praktijk die niet in overeenstemming is met artikel 126aa Sv.

3. Conclusie en aanbevelingen

De Inspectie concludeert dat de politie na vier jaar nog onvoldoende inhoud en opvolging geeft aan de regels en uitgangspunten voor het toepassen van de hackbevoegdheid

De Inspectie stelt vast dat de politie in 2022 voor het vierde jaar op rij aan diverse regels en uitgangspunten uit het geldende rechtskader geen of onvoldoende inhoud en opvolging geeft. De Inspectie stelt wel vast dat de politie in 2022 gehandeld heeft binnen de reikwijdte van de afgegeven bevelen en de keuringen heeft uitgevoerd volgens de daaraan gestelde regels.

De Inspectie concludeert dat veel van haar bevindingen gelijk zijn aan de eerdere drie verslagen die zijn gepubliceerd. Dit betekent dat de afgelopen vier jaar, ondanks de inspanningen die daartoe zijn geleverd, te weinig vooruitgang is geboekt door DIGIT met het verbeteren van het proces en de technische inrichting om te kunnen voldoen aan de wettelijke vereisten en de toezeggingen die zijn gedaan door de (toenmalige) minister van Justitie en Veiligheid.

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

- *De inzet en gebruik van commerciële software voldoen niet aan de door de wetgever gestelde regels en uitgangspunten*. Evenals eerdere verslagjaren stelt de Inspectie vast dat in het overgrote deel van de zaken waar de hackbevoegdheid is ingezet, gebruik is gemaakt van commerciële software. Deze software is zowel ingezet voor de fase van het binnendringen als voor de fase van het uitvoeren van onderzoekshandelingen. De Inspectie heeft er begrip voor dat deze software in het belang van de opsporing wordt ingezet, maar signaleert dat hierdoor spanning ontstaat met het rechtskader. De wetgever heeft verschillende regels en uitgangspunten gesteld aan het gebruik van dergelijke software. Zo is toegang tot het systeem van waaruit wordt binnengedrongen alleen toegestaan voor aangewezen opsporingsambtenaren. Dit betekent dat een leverancier van deze software geen toegang mag hebben tot dit systeem. Voor software die ingezet wordt voor het uitvoeren van onderzoekshandelingen mag de leverancier geen toegang hebben tot de gegevens die verkregen worden en mag de leverancier niet de mogelijkheid hebben om zelfstandig updates uit te voeren of zelf de controle over het geautomatiseerde werk over te nemen. Door de politie zijn procedurele afspraken gemaakt met de leverancier over toegang restricties. De Inspectie concludeert dat de politie dit - door het black-box karakter van de gebruikte software - technisch niet kan afdwingen en niet kan controleren.

  Daarnaast merkt de Inspectie als onderdeel van de gesignaleerde spanning de volgende twee punten op. Ten eerste heeft de wetgever als hoofdregel gesteld dat software die ingezet wordt als technisch hulpmiddel vooraf goedgekeurd moet zijn als deze wordt ingezet. In uitzonderingsgevallen kan keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technisch hulpmiddel zich naar het oordeel van de officier van justitie

daartegen verzet. Gelet op het feit dat de hackbevoegdheid voor het overgrote deel van de zaken in 2022 is ingezet voor het hacken van telefoons met een niet gekeurd commercieel technisch hulpmiddel signaleert de Inspectie dat hiermee de door de wetgever voorziene uitzonderingsgevallen standaardpraktijk zijn geworden. De Inspectie benadrukt dat besluitvorming door de officier van justitie buiten de reikwijdte van het toezicht door de Inspectie valt.

Ten tweede is tijdens de parlementaire behandeling toegezegd dat de markt voor onbekende kwetsbaarheden zo min mogelijk moet worden gestimuleerd. De Inspectie signaleert, evenals over de drie afgelopen jaren, dat in de praktijk het voorgeschreven licentiemodel juist leidt tot extra kosten voor de politie en daarmee mogelijk tot een extra stimulans van voor deze markt.

- *De inrichting en toepassing van geautomatiseerde logging en handmatige verslaglegging is nog niet op orde*. De wetgever stelt eisen aan de doorlopende en automatische vastlegging van gegevens in logbestanden, de beveiliging van deze logbestanden en het gebruik en controle daarvan. Als uitzondering mag de verantwoording over de verrichte handelingen handmatig worden vastgelegd. De logging is van belang om meerdere redenen. Ten eerste is de logging van belang zodat zowel tijdens als na afloop van een inzet geen twijfel kan bestaan over aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel. Daarnaast dient de logging ter verificatie van de betrouwbaarheid, integriteit en herleidbaarheid van de verkregen gegevens die mogelijk kunnen worden gebruikt als bewijs. Als derde kan de politie op basis van de logging zelf tijdig afwijkingen of onregelmatigheden signaleren en controles uitvoeren. Als laatste is de logging van belang voor het inrichten van effectief toezicht door de Inspectie.

  Ook in 2022 heeft de politie nog onvoldoende uitgewerkt hoe zij logging inricht en toepast. Controles van de logging door de politie zelf vinden op ad-hocbasis plaats. Beeldschermopnamen blijken ook begin 2022 nog niet volledig. Door de grote hoeveelheid aan logging in de vorm van beeldschermopnamen is de toepassing hiervan niet goed bruikbaar voor proactieve controle doeleinden.

  Daarnaast is de handmatige verslaglegging, in de vorm van het journaal, niet in alle gevallen juist en volledig. Dit heeft gevolgen voor de juistheid van de processen-verbaal omdat de processen-verbaal gebaseerd zijn op de informatie uit het journaal. DIGIT is door het Openbaar Ministerie geïnstrueerd om minimaal te verbaliseren en maximaal te journaliseren. Hierdoor is een juist en volledig journaal van nog groter belang.

- *De voortgang van de inbedding van kwaliteitszorg en interne controle stagneert*. De Inspectie heeft de afgelopen jaren aandacht gevraagd voor de uitwerking en toepassing van kwaliteitszorg door de politie, waaronder de interne controle. Een dergelijke invulling mag verwacht worden van een volwassen en professionele organisatie. Alhoewel kleine stapjes gezet zijn en soms in de praktijk ook zijn toegepast, blijft er ook in 2022 sprake van een versnipperde aanpak en inrichting. De Inspectie constateert dat op dit onderwerp door de politie ook in 2022 weinig vooruitgang is geboekt. De

Inspectie concludeert dat onvoldoende uitvoering is gegeven aan het verder inbedden van de kwaliteitszorg bij de toepassing van de hackbevoegdheid door de politie. De Inspectie vindt het belangrijk dat de politie, als basis voor systeemtoezicht, zelf zorgdraagt voor de kwaliteit van de inzet van de hackbevoegdheid tijdens alle fasen van de uitvoering. De Inspectie heeft hiertoe in haar eerdere verslagen het belang van kwaliteitszorg en interne controle benadrukt.

- *De informatiebeveiliging is nog steeds niet aantoonbaar op niveau*. Het Besluit stelt eisen aan de (informatie)beveiliging. Ook heeft de politie zelf eisen gesteld aan de beveiliging. De voortgang van het planmatig aantoonbaar en controleerbaar op niveau brengen en houden van beheersingsmaatregelen voor de (informatie)beveiliging stagneert. Dit betekent dat, evenals voorgaande jaren, DIGIT onvoldoende is nagegaan of haar processen en systemen voldoen aan de gestelde eisen.

  De Inspectie vindt het belangrijk dat de politie, als basis voor goed systeemtoezicht, zelf zorgdraagt voor het controleerbaar en aantoonbaar treffen van passende maatregelen om beveiligingsrisico's te beheersen en de betrouwbaarheid en integriteit van de logging en de technische infrastructuur te waarborgen. Dit vormt de basis voor de politie om vanuit een eigen interne verantwoordelijkheid toe te zien op het inrichten van deze maatregelen, de structurele naleving daarvan en daarover op een controleerbare wijze verantwoording af te kunnen leggen.

- *Vernietiging en herkenning geheimhouderinformatie*. Specifiek voor geheimhouderinformatie concludeert de Inspectie dat de DIGIT-officier van justitie onverwijld in de praktijk in kennis wordt gesteld door DIGIT als opsporingsambtenaren per toeval kennisnemen van mogelijke geheimhouderinformatie.

  Er zijn echter aan de kant van DIGIT geen processen, werkinstructies en ondersteunende systemen zoals nummerherkenning ingericht om geheimhouderinformatie te herkennen. Op grond van het Besluit bewaren en vernietigen niet-gevoegde stukken dient in ieder geval het nummerherkenningsysteem te worden toegepast als het gaat om het aftappen van communicatie. Ook dienen op grond van het Besluit onderzoek in een geautomatiseerd werk alleen de gegevens te worden overgedragen door het technisch team die van belang zijn voor het onderzoek. Geheimhouderinformatie is dit vanzelfsprekend niet. In de huidige praktijk worden alle verzamelde gegevens door DIGIT overgedragen.

  In opdracht van het OM blijft geheimhouderinformatie, ook na herkenning, opgeslagen in de systemen van DIGIT en hiermee dus van de politie. Aan deze laatste constatering verbindt de Inspectie echter geen waardeoordeel gelet op het feit dat de politie hier handelt in opdracht van de DIGIT-officier van justitie en de Inspectie geen toezicht houdt op het openbaar ministerie. De Inspectie signaleert echter wel een praktijk die niet in overeenstemming is met artikel 126aa Sv.

Daarnaast geldt in het algemeen dat het proces van vernietigen, net als in 2021, in 2022 nog onvoldoende is uitgewerkt en is ingericht. Hierdoor duurt het in de praktijk te lang voordat gegevens volledig, tijdig en/of juist zijn vernietigd door DIGIT als hiervoor het bevel is gegeven door de officier van justitie.

Aanbevelingen en het vervolg

De Inspectie benadrukt het, door de wetgever genoemde, grote belang dat met een goede naleving van de regels voor de hackbevoegdheid is gemoeid. De wetgever heeft in de nota van toelichting behorende bij de Wet Computercriminaliteit III gesteld dat het toezicht door de Inspectie op de naleving van deze regels aan de hand van systeemtoezicht wordt uitgevoerd. Een effectieve (interne) controle en kwaliteitszorg door de politie is daarvoor randvoorwaardelijk. De politie dient in staat te zijn zelf te kunnen controleren of sprake is van naleving van het rechtskader dat geldt voor de hackbevoegdheid. De Inspectie wil daar met haar toezicht op een effectieve wijze aan bijdragen. Dat vereist dat de politie binnen de mogelijkheden die zij zelf heeft, de verbeteringen uitvoert die daarvoor nodig zijn en die door de Inspectie vanuit haar toezicht aan de politie zijn gesignaleerd. Dit kan alleen als dat net zoveel prioriteit krijgt als de operationalisering van de bevoegdheid zelf. Zolang de kwaliteitszorg en (interne) controle onvoldoende aanwezig is, kan de Inspectie het aan haar gevraagde systeemtoezicht niet uitoefenen en moet de Inspectie intensief toezicht blijven uitvoeren. De Inspectie vindt dat de politie daar na vier jaar van intensief toezicht onvoldoende opvolging aan geeft. Dit is reeds in eerdere verslagen door de Inspectie geconstateerd. Desondanks blijft de praktijk van DIGIT op deze punten onveranderd.

De Inspectie vindt dat het nu tijd is dat er verandering komt in de opvolging door de politie. De Inspectie vindt het voor een rechtmatige en zorgvuldige toepassing van de hackbevoegdheid en voor de effectiviteit van het toezicht van belang dat - zolang de regels en uitgangspunten onveranderd blijven - de politie op korte termijn aantoonbaar en zonder voorbehoud invulling geeft aan alle vigerende regels en deze naleeft.

Daarbij vindt de Inspectie het van belang dat de minister een standpunt inneemt over een mogelijke aanpassing van het wettelijk kader zodat duidelijk wordt in welke mate mogelijke knelpunten bij de praktische uitvoerbaarheid van de hackbevoegdheid zoals die nu door de politie worden ervaren, in het wettelijk kader worden weggenomen. Daarmee wordt voor de Inspectie en voor de politie helderheid gegeven waarop het nalevingstoezicht zich moet richten.

De Inspectie komt daarmee tot de volgende aanbevelingen:

<u>Aanbeveling aan de minister van Justitie en Veiligheid:</u>

- Neem een standpunt in over aanpassingen in het wettelijke kader om mogelijke knelpunten bij de praktische uitvoerbaarheid zoals deze door de politie worden ervaren weg te nemen.

Aanbevelingen aan de politie:

- Draag zorg voor een aantoonbare invulling en controleerbare naleving van de geldende regels en uitgangspunten voor de toepassing van de hackbevoegdheid.
- Investeer daarbij met voorrang en op korte termijn om verbeteringen op te pakken en door te voeren door het in samenhang inrichten en inbedden van kwaliteitszorg en interne controle, het op orde brengen van de logging, verbeteringen in de kwaliteit van de handmatige verslaglegging en het aantoonbaar op niveau brengen en houden van informatiebeveiliging.

De Inspectie zal haar toezicht vanaf nu specifiek richten op de volgende onderwerpen: de logging en handmatige verslaglegging, informatiebeveiliging, kwaliteitszorg en interne controle. Het toezicht op de andere aspecten van de hackbevoegdheid zal de Inspectie weer uitvoeren nadat de minister duidelijkheid heeft verschaft over eventuele aanpassingen in het wettelijk kader.

Bijlage A: Detailbevindingen

Deze bijlage beschrijft in meer detail de bevindingen van het uitgevoerde toezicht door de Inspectie op de toepassing van de hackbevoegdheid door het technisch team van de politie in 2022. Tevens wordt in deze bijlage ingegaan op bevindingen over de keuring van technische hulpmiddelen en op de keuringsdienst die deze keuringen heeft uitgevoerd.

De voornaamste bevindingen zijn op onderwerp bij elkaar gebracht. De volgorde van de paragrafen sluit zoveel mogelijk aan bij het procesverloop van de toepassing van de hackbevoegdheid zoals dat is beschreven in de nota van toelichting bij het Besluit. In elke paragraaf is in de blauw gearceerde kaders een korte beschrijving uit het gehanteerde rechtskader opgenomen. Een uitgebreidere toelichting is opgenomen in het eerder door de Inspectie gepubliceerde toetsingskader.[33]

A.1 Voorbereiding voorafgaand aan de inzet

De hackbevoegdheid mag gelet op het Besluit alleen worden ingezet door een technisch team. Dit team dient te bestaan uit opsporingsambtenaren. Het Besluit stelt regels aan deze opsporingsambtenaren. Een opsporingsambtenaar moet hiervoor zijn aangewezen door zijn werkgever. Daarnaast dient de ambtenaar lid of deelnemer te zijn van het technisch team.[34] Om lid te kunnen worden van een technisch team moet worden voldaan aan de benodigde kwalificaties waaronder deskundigheid- en ervaringsvereisten.[35] Deze vereisten voor leden van een technisch team zijn vastgelegd in de regeling *kwalificaties opsporingsambtenaren*.[36] Voor deelnemers geldt geen kwalificatie-eis, zij kunnen door de korpschef op incidentele basis voor de duur van het bevel in een concrete zaak worden aangewezen indien zij beschikken over specifieke kennis en vaardigheden die daarvoor nodig zijn.[37]

De Inspectie stelt vast dat de leden van het technisch team, evenals in 2021, voldeden aan de gestelde kwalificatie-eisen. In 2022 hebben geen personele wijzigingen plaatsgevonden die hierop van invloed zijn. Deze opsporingsambtenaren zijn door hun werkgever aangewezen voor het mogen toepassen van de bevoegdheid. Namens de korpschef zijn zij daarnaast aangewezen als lid van het technisch team.

[33] https://www.inspectie-jenv.nl/Publicaties/toetsingskaders/2022/07/12/toetsingskader-hackbevoegdheid-2022
[34] Art. 3 lid 2 Bogw.
[35] Art. 3 lid 3Bogw.
[36] Regeling van de minister van Justitie en Veiligheid van 15 februari 2019, kenmerk 2429311, houdende regels betreffende de kwalificaties van opsporingsambtenaren die door de korpschef kunnen worden aangewezen als lid van een technisch team.
[37] Art. 4 lid 2 Bogw (incidentele samenwerking) en artikelsgewijze toelichting op het Besluit, artikel 4 p. 35. "*Hierbij kan worden gedacht aan de situatie dat een opsporingsambtenaar van een bijzondere opsporingsdienst met specifieke kennis op het gebied van digitale fraude wordt toegevoegd aan een technisch team in verband met gewenste technische expertise op dit gebied in een bepaald onderzoek.*" Kamerstuk 34372 nr.27 p.8 heeft het over "*…ter versterking van de technische expertise van een technisch team in een concrete zaak*". Hieruit kan afgeleid worden dat het specifieke kennis betreft, waarover leden van het technisch team niet beschikken.

De Inspectie stelt daarnaast vast dat de aanwijzing en inzet van deelnemers, evenals in 2021, niet voldeed aan de vereisten. De politie kiest ervoor om middels een generieke aanwijzing alle deelnemers in alle in 2022 uitgevoerde zaken achteraf aan te wijzen. Deze werkwijze heeft daarmee een vooral administratief karakter. Bovendien gaat het structureel aanwijzen van deze deelnemers voorbij aan de door de wetgever bedoelde aanwijzing van deelnemers op een incidentele basis. Deze structurele aanwijzing en inzet van dezelfde deelnemers heeft daarmee vooral het kenmerk van het leveren van extra 'handjes' en niet zozeer op het inzetten van specifieke kennis of vaardigheden. De Inspectie merkt hierbij wel op dat alle aangewezen deelnemers onderdeel uitmaken van het team DIGIT en opsporingsambtenaar zijn.

Haalbaarheidsonderzoek

Op grond van de toelichting bij het Besluit dient het technisch team in de voorbereidende fase een rapport 'Haalbaarheidsonderzoek' op te stellen waarin aandacht wordt besteed aan de haalbaarheid van het onderzoek en de inschatting en beheersing van risico's. Voor wat betreft risico's moet gedacht worden aan de mate van inbreuk op de persoonlijke levenssfeer van de verdachte, gevolgen voor het geautomatiseerde werk, kans op nadeel of schade bij derden, maar ook de kans op ontdekking van de inzet van het technisch team door de betrokkene.[38]

In 2022 heeft DIGIT wijzigingen aangebracht in de opzet van het haalbaarheidsonderzoek. Het haalbaarheidsonderzoek maakt sindsdien samen met het plan van aanpak voor het uitvoeren van de onderzoekshandelingen onderdeel uit van een 'advies inzet'. Een belangrijke wijziging in positieve zin is dat de door DIGIT voorgenomen te treffen waarborgen[39] voor de herleidbaarheid, integriteit en betrouwbaarheid nu vooraf in het plan benoemd zijn. De Inspectie stelt vast dat in alle zaken waar het bevel tot inzet van de hackbevoegdheid is gegeven, een 'advies inzet' of rapport 'haalbaarheidsonderzoek' aanwezig was. De Inspectie stelt vast dat in deze documenten op hoofdlijnen aandacht besteed wordt aan de risico's en een uitspraak gedaan wordt over de haalbaarheid. De inschatting van de haalbaarheid en van de risico's is echter niet altijd in het haalbaarheidsonderzoek onderbouwd.

Plan van aanpak voor het binnendringen

In de toelichting bij het Besluit is beschreven dat het technisch team na afgifte van een bevel een plan van aanpak opstelt voor het binnendringen in het geautomatiseerde werk. De gekozen aanpak wordt vervolgens getest in een proefopstelling.[40] Met het testen kan onderzocht worden wat het effect is op onderkenning van het onderzoek en hoe de kans daarop beperkt kan worden en van welke eventuele gevolgschade door het binnendringen sprake is. Ook kan getest worden wat het effect van het binnendringen is en in hoeverre daarbij het geautomatiseerde werk na afloop in oorspronkelijke staat achtergelaten kan worden. Een kwaliteitsaspect voor het controleerbaar en betrouwbaar uitvoeren van

[38] *Kamerstukken II* 2015/16, 34372, nr.3, p. 33.
[39] Zie paragraaf A.4 voor de context van deze waarborgen. In het bijzonder de paragraaf "Gebruik technisch hulpmiddel waarvan keuring achterwege blijft" en de paragraaf "Onderzoekshandelingen middels handmatige inzet".
[40] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 16

testen is de aanwezigheid van een testplan, een representatieve testomgeving en van vastlegging van de resultaten van de uitgevoerde test.

De Inspectie stelt, evenals in 2021, vast dat in 2022:
- niet voor elke toepassing van de hackbevoegdheid een plan van aanpak voor het binnendringen aangetroffen is. De status van de wel aanwezige plannen van aanpak is veelal onduidelijk. Deze plannen van aanpak gaan niet altijd in op de wijze en methode van binnendringen waaraan volgens de parlementaire stukken aandacht besteed zou moeten worden;
- een testplan en resultaten van testen in proefopstellingen niet in alle zaken controleerbaar zijn vastgelegd. Verslaglegging over de uit te voeren testen en testresultaten is fragmentarisch vastgelegd. De Inspectie heeft wel voldoende aanwijzingen dat er getest is. De Inspectie heeft er begrip voor dat de mate waarin het testen plaatsvindt, afhankelijk is van de aard en complexiteit van de zaak en de daartoe in te zetten middelen;
- testen niet altijd zijn uitgevoerd in een testomgeving die controleerbaar representatief is.

A.2 Binnendringsoftware en melden onbekende kwetsbaarheden

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. Het technisch team kan daartoe binnendringsoftware inkopen bij een leverancier. In het Regeerakkoord 2017-2021 en in het Besluit is opgenomen dat deze zogenoemde commerciële binnendringsoftware van derden alleen zal worden aangeschaft als daartoe in een specifieke zaak een noodzaak bestaat. Aan de inzet van commerciële binnendringsoftware zijn strenge voorwaarden verbonden, waaronder:
- De leverancier is gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en levert niet aan dubieuze regimes.[41] De toets of de leverancier niet levert aan dubieuze regimes wordt uitgevoerd door de politie. Door de minister van JenV is bepaald onder welke condities een regime als dubieus wordt aangemerkt.[42]
- Het functioneren van de binnendringsoftware wordt gecontroleerd in een testomgeving.[43] Dit is onder meer van belang met het oog op het voorkomen van schade aan derden.
- 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.[44]

Zoals de Inspectie in haar eerdere verslagen heeft vermeld, is volgens de daartoe vastgestelde procedure, in 2019 screening van de betreffende leverancier bij de

[41] *Kamerstukken II* 2017/18, 34372, nr. 27, p.7, p.3 (Regeerakkoord 2017-2021 "Vertrouwen in de toekomst")
[42] *Handelingen* I 2017/18, 34 item 5, p.29.
[43] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 16, 18 en 20.
[44] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 15 en 16.

AIVD aangevraagd en is de toets aangaande het niet leveren aan dubieuze regimes door de politie uitgevoerd door een verklaring hierover op te vragen bij de leverancier. De Inspectie heeft vastgesteld dat de politie eind 2022 een hernieuwde uitvraag voor een verklaring door de leverancier gedaan heeft. Afgevraagd kan worden, wat de waarde is van een dergelijke eigen verklaring die niet inhoudelijk wordt getoetst. Een hernieuwde screeningsaanvraag door de AIVD heeft niet plaatsgevonden. De Inspectie merkt op dat wet- en regelgeving niet verplicht tot het periodiek hernieuwd doorlopen van het proces van de screeningsaanvraag en de toets of een leverancier niet levert aan dubieuze regimes.

In 2022 heeft DIGIT in 25 zaken commerciële binnendringsoftware ingezet. Het door DIGIT testen van het functioneren van de commerciële binnendringsoftware vindt impliciet plaats als onderdeel van de test- en verificatieopstelling. Deze testopstelling is door DIGIT als waarborg benoemd in de situaties waar een niet-vooraf goedgekeurde technisch hulpmiddel van een commerciële leverancier wordt ingezet.[45] De test zoals die wordt uitgevoerd, dient daarmee verschillende doelen. In de commerciële software is namelijk de functionaliteit van het binnendringen gecombineerd met een technisch hulpmiddel voor het uitvoeren van onderzoekshandelingen. De Inspectie stelt vast dat de testopstelling en -activiteiten vooral gericht zijn op de functionaliteit ten behoeve van de onderzoekshandelingen en niet op het functioneren van de binnendringsoftware en de mogelijke negatieve effecten bij het binnendringen zoals de wetgever heeft beoogd.

De Inspectie heeft evenals voorgaande jaren vastgesteld dat per zaak waarin commerciële binnendringsoftware succesvol is ingezet, één licentie is ingekocht nadat is binnengedrongen. De Inspectie heeft er begrip voor dat licenties pas na succesvol binnendringen worden aangeschaft om onnodige kosten te vermijden. Het softwarepakket wordt in de praktijk niet verwijderd na afronding van het onderzoek. Ook wordt een licentie niet verbruikt. Hierdoor is hergebruik mogelijk. Dit is niet in lijn met het door de wetgever gestelde uitgangspunt dat licenties niet mogen worden hergebruikt.

Onbekende kwetsbaarheden

Commerciële binnendringsoftware maakt soms gebruik van fouten in software die nog onbekend zijn bij de producent van deze software. 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 dit soort kwetsbaarheden en de daaraan verbonden negatieve gevolgen voor de veiligheid van het internet.[46]

De Inspectie signaleert, evenals over de drie afgelopen jaren, 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.

Softwarecode bevat in zijn algemeenheid vrijwel altijd fouten. Onbekende kwetsbaarheden zijn fouten in software die nog onbekend zijn bij de producent van deze software. Er zijn partijen die bereid zijn veel geld te betalen voor informatie

[45] Zie daartoe paragraaf A.4 "Gebruik technisch hulpmiddel waarvan keuring achterwege blijft".
[46] Zie *Kamerstukken I 2016/17,* 34 372, nr. E, p. 4 en p. 11; *Kamerstukken I* 2016/17, 34372, D (MvA I), p. 20-22.

over bepaalde onbekende kwetsbaarheden. Om deze markt voor onbekende kwetsbaarheden niet te stimuleren, is het uitgangspunt dat als de politie beschikt over informatie van onbekende kwetsbaarheden[47] hiervan melding gemaakt wordt rechtstreeks aan de leverancier/producent.[48] De meldingsplicht is overigens niet wettelijk verankerd: in het Wetboek van Strafvordering is alleen het uitstel van een melding van een onbekende kwetsbaarheid geregeld. Wel is de meldplicht benoemd in een Kamerbrief.[49] In een ander Kamerstuk is aangegeven dat de officier van justitie dit uitstel uitsluitend kan bevelen op grond van een zwaarwegend opsporingsbelang en na machtiging van een rechter-commissaris.[50] Dit impliceert dat de officier van justitie bij de afweging voor uitstel tevens beoordeelt of sprake is van een onbekende kwetsbaarheid zoals bedoeld in artikel 126ffa van het Wetboek van Strafvordering.

In 2022 heeft DIGIT in enkele opsporingsonderzoeken kwetsbaarheden aangetroffen die kunnen worden gebruikt om een geautomatiseerd werk binnen te dringen. DIGIT en de DIGIT-officier van justitie hebben begin 2023 besloten dat in de gevallen waar deze kwetsbaarheden zijn ingezet in één geval een melding zal plaatsvinden van een onbekende kwetsbaarheid. In een ander geval zal hiervoor een traject voor uitstel van melding zoals bedoeld in artikel 126ffa in gang gezet worden. Twee onbekende kwetsbaarheden zijn door DIGIT in 2022 gemeld bij het meldpunt van het Nationaal Cyber Security Center (NCSC).[51] DIGIT heeft van het NCSC een terugkoppeling van deze meldingen ontvangen.

Daarnaast kan in de zaken waar de commerciële binnendringsoftware wordt ingezet niet uitgesloten worden dat deze software gebruik maakt van één of meerdere onbekende kwetsbaarheden. Dit gelet op het black-box karakter van deze software. Vanuit een commercieel oogpunt zal de leverancier van deze binnendringsoftware geen inzage verschaffen in de toegepaste (onbekende) kwetsbaarheden. De exacte werking van deze software blijft daarmee voor DIGIT onbekend. DIGIT draagt dan ook geen kennis van onbekende kwetsbaarheden waarvan deze binnendringsoftware mogelijk gebruik maakt. Het is daarmee evident dat melding door DIGIT in dat kader niet kan plaatsvinden.

[47] Onder onbekende kwetsbaarheid wordt volgens Sv. artikel 126ffa vierde lid verstaan "een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen."
[48] *Kamerstukken II* 2016/17, 34372 nr.6, p.9.
[49] *Kamerstukken I* 2016/17, 26643, nr. 428, pagina 4.
[50] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 31; Sv. Artikel 126ffa lid 3.
[51] Zie https://www.ncsc.nl/contact/kwetsbaarheid-melden

A.3 Keuring technisch hulpmiddel

Na het binnendringen voert het technisch team onderzoek uit in het apparaat. In het Wetboek van Strafvordering is aangegeven dat bij het verrichten van onderzoekshandelingen al dan niet gebruik kan worden gemaakt van een technisch hulpmiddel.[52] Volgens het Besluit is een *technisch hulpmiddel* 'een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel'.[53] Om de betrouwbaarheid en integriteit van technische hulpmiddelen, de betrouwbaarheid en integriteit van de hiermee geregistreerde gegevens en de herleidbaarheid van de gegevens te borgen, stelt het Besluit diverse technische eisen[54] aan een technisch hulpmiddel.[55]

Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er volgens de toelichting bij het Besluit vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.[56] Daarnaast biedt een goedgekeurd technisch hulpmiddel als voordeel dat risico's op misbruik door derden worden beperkt en dat specificaties van het middel niet worden prijsgegeven. Dit is van groot belang voor de afscherming van gevoelige opsporingsmethoden.[57]

De beoordeling of een technisch hulpmiddel voldoet aan de eisen wordt uitgevoerd door een keuringsdienst. De minister heeft de keuringsdienst van de Landelijke Eenheid aangewezen als keuringsdienst voor de keuring van technische hulpmiddelen.[58]

De Inspectie stelt vast dat in 2022 de keuringsdienst van de Landelijke Eenheid van de politie deze keuringen heeft uitgevoerd.

Zoals ook in 2021 vermeld, zijn aan de keuringsdienst van de Landelijke Eenheid geen specifieke eisen gesteld, zoals deze wel voor de aangewezen keuringsdienst TNO in 2020 golden.[59] Dergelijke eisen bieden waarborgen om de kwaliteit, capaciteit en beschikbaarheid van middelen zeker te stellen. De Inspectie merkt op dat het Besluit de ruimte biedt om middels een ministeriele regeling eisen te stellen aan de keuringsdienst van de Landelijke Eenheid.

In het Besluit is gespecificeerd aan welke eisen een technisch hulpmiddel moet voldoen om te worden goedgekeurd. De wijze van keuring en keuringscriteria zijn door de keuringsdienst op hoofdlijnen vastgelegd in een keuringsprotocol dat door de minister is goedgekeurd.[60] De Inspectie stelt vast dat de minister van Justitie en Veiligheid op 28 februari 2021 het door de keuringsdienst van de Landelijke

[52] Artt. 126nba, 126uba, 126zpa lid 1, Wetboek van Strafvordering.
[53] Artikel 1 sub g Bogw.
[54] Artt. 8 t/m 13 Bogw.
[55] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 18..
[56] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 19.
[57] *Kamerstukken II* 2015/16, 34372, nr. 3, p.110.
[58] Art. 16 lid 1, Bogw .
[59] *Stcrt.,* 2019, nr.10713. (Regeling eisen keuringsdienst technisch hulpmiddel).
[60] Art. 17 Bogw (keuringsprotocol) en Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 42.

Eenheid opgestelde keuringsprotocol heeft goedgekeurd. De keuring van technische hulpmiddelen moet worden uitgevoerd op basis van dit keuringsprotocol.[61] Het keuringsprotocol is in 2022 onveranderd van kracht.

In 2022 is namens de korpschef drie keer een technisch hulpmiddel ter keuring aangeboden. Bij alle in 2022 uitgevoerde keuringen is de keuringsdienst van oordeel dat het aangeboden technisch hulpmiddel voldoet aan de gestelde eisen uit het Besluit. De Inspectie heeft vastgesteld dat door de keuringsdienst voor elk goedgekeurd technisch hulpmiddel testactiviteiten zijn uitgewerkt die aansluiten op het keuringsprotocol.

De Inspectie is per keuringseis nagegaan hoe en op basis waarvan de keuringsdienst tot haar oordeel is gekomen. De Inspectie stelt vast dat:
- de keuringsuitslagen op een systematische en navolgbare wijze tot stand gekomen zijn;
- het onderliggende keuringsdossier gestructureerd en goed toegankelijk is;
- verantwoording over de uitgevoerde testactiviteiten, bijbehorende uitkomsten en afwegingen gestructureerd en op een controleerbare wijze zijn vastgelegd in een voor het keuringsdoel ontwikkelde voorziening. Hieruit is voor de Inspectie in voldoende mate af te leiden in hoeverre het betreffende technische hulpmiddel voldoet aan de hieraan gestelde technische eisen[62] en is goed 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.[63] Tevens heeft de keuringsdienst bij elk goedgekeurd technisch hulpmiddel een handleiding opgesteld;[64]
- door de keuringsdienst een centrale registratie bijgehouden wordt van de keuringsrapporten.[65]

Het Besluit biedt de keuringsdienst de ruimte om vervangende waarborgen te stellen op onderdelen waar het technisch hulpmiddel niet voldoet aan in het Besluit gestelde technische eisen.[66] Deze verplicht te treffen vervangende waarborgen worden door de keuringsdienst in het keuringsrapport vastgelegd.[67]

De Inspectie stelt vast dat in alle keuringsrapporten van de goedgekeurde technische hulpmiddelen door de keuringsdienst verplicht te treffen vervangende waarborgen zijn benoemd. Deze waarborgen zijn volgens de Inspectie duidelijk genoeg geformuleerd, maar niet altijd goed uitvoerbaar in de praktijk. Het risico is dat in die situaties het ingezette technisch hulpmiddel daardoor niet voldoet aan de gestelde voorwaarden voor goedkeuring. In paragraaf A.4 wordt ingegaan op de

[61] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 42
[62] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 37 t/m 40.
[63] Art. 18 Bogw.
[64] van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 38.
[65] Art. 19 Bogw
[66] De nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk .vermeldt op pagina 43 verplicht te treffen vervangende procedurele waarborgen. Dit kan tot verwarring leiden. Voor de uniformiteit hanteert de Inspectie hier het begrip "vervangende waarborgen".
[67] Art. 18 lid 3 sub e, Bogw. "*Het keuringsrapport van een goedgekeurd technisch hulpmiddel vermeldt ten minste: e) relevante verplichte vervangende waarborgen waarmee voldaan kan worden aan één of meer eisen, bedoeld in artikelen 8 tot en met 13*".

naleving en verantwoording door DIGIT van deze vervangende waarborgen bij een ingezet goedgekeurd technisch hulpmiddel.

De Inspectie constateert evenals in 2021 dat de personele bezetting van de keuringsdienst van de Landelijke Eenheid kwetsbaar is. Net als in 2021 was slechts één medewerker inzetbaar voor de uitvoering van dit type keuringen. Deze medewerker is in 2022 op afroepbasis ondersteund en gecontroleerd door medewerkers van TNO. Met deze ondersteuning door TNO kon de keuringsdienst van de Landelijke Eenheid in 2022 invulling geven aan de eigen gestelde minimale kwaliteitsvereisten van een vier-ogen principe. Het contract met TNO voor deze ondersteuning na 2022 is niet meer verlengd. In 2022 is er wel zicht gekomen op een uitbreiding van de personele capaciteit bij de keuringsdienst. Een nieuwe medewerker is eind 2022 aangenomen en volgt een inwerk- en opleidingstraject. Voorzien is dat deze medewerker vanaf 2023 ingezet kan worden bij het keuren van technische hulpmiddelen voor de hackbevoegdheid.

Samenvattend concludeert de Inspectie dat de keuringsdienst van de Landelijke Eenheid de keuringen heeft uitgevoerd volgens de daaraan gestelde eisen en dat het gevolgde keuringsproces en de totstandkoming van de keuringsuitslag goed navolgbaar is.

A.4 Uitvoering binnendringen en verrichten van onderzoekshandelingen

Het op afstand en heimelijk binnendringen en het verrichten van onderzoek in een geautomatiseerd werk kan worden uitgevoerd zodra daartoe, na machtiging van de rechter-commissaris, een bevel is afgegeven door de officier van justitie.

In het bevel specificeert de officier van justitie de onderzoeksdoelen waarvoor de bevoegdheid in een bepaalde zaak door de politie ingezet mag worden. De opsporingsambtenaar van het technisch team mag alleen handelingen uitvoeren die passen binnen deze afgegeven doelen. De mogelijke onderzoeksdoelen zijn limitatief in het Wetboek van Strafvordering omschreven.[68] Het betreft de doelen:

- de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker zoals de identiteit of locatie, en de vastlegging daarvan;
- het opnemen van vertrouwelijke communicatie (ovc) of het aftappen en opnemen van telecommunicatie;[69]
- stelselmatige observatie, waarbij door de officier van justitie bepaald kan worden dat het technisch hulpmiddel op de persoon wordt bevestigd;[70]
- de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen (historische gegevens) of die binnen de looptijd van het bevel nog worden opgeslagen;
- de ontoegankelijk making van gegevens.

[68] Artt. 126nba, 126uba en 126zpa lid 1 Sv.
[69] Aan de uitvoering hiervan ligt respectievelijk een bevel ten grondslag op basis van artikel 126l Sv. (opnemen van vertrouwelijk communicatie) en artikel 126m Sv. (opnemen van niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst).
[70] Aan de uitvoering ligt een bevel op basis van 126g Sv. (stelselmatige observatie) ten grondslag.

De totstandkoming van de afgifte en de inhoud van een bevel is de verantwoordelijkheid van de officier van justitie en valt daarmee buiten de reikwijdte van het toezicht door de Inspectie. Het door de officier van justitie afgegeven bevel vormt wel het kader waarbinnen de politie uitvoering aan de hackbevoegdheid moet geven. In het bevel vermeldt de officier van justitie naast de eerdergenoemde doelen, het nummer of een andere aanduiding van het geautomatiseerde werk en ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering gegeven moet worden. Ook vermeldt het bevel het tijdstip of de periode waarbinnen aan het bevel door de politie uitvoering moet worden gegeven.[71] Indien bevel is gegeven voor het opnemen van vertrouwelijke communicatie (ovc)[72], zijn in het bevel de locaties gespecificeerd waar dit mag plaatsvinden.

Deze in het bevel benoemde onderdelen zijn door de Inspectie als kader gehanteerd om te bepalen of het technisch team heeft gehandeld binnen de reikwijdte van het bevel.[73] De Inspectie heeft dit vervolgens afgezet tegen een digitaal logboek (journaal) dat door DIGIT wordt bijgehouden ter verantwoording van de uitgevoerde werkzaamheden. Ook is door de Inspectie voor deze controle de beschikbare logging gebruikt.

Gehandeld binnen de reikwijdte van de afgegeven bevelen
De Inspectie concludeert dat DIGIT in het overgrote deel van de zaken binnen de reikwijdte van de afgegeven bevelen heeft gehandeld. Waar sprake is geweest van een afwijking met mogelijke gevolgen voor een rechtmatige inzet van de bevoegdheid heeft DIGIT dit zelf tijdig onderkend en maatregelen genomen. De binnengehaalde informatie is verwijderd en niet overgedragen aan het tactisch team. De Inspectie constateert dat indien sprake was van een (mogelijke) afwijking tussen het bevel en de uitvoering altijd door DIGIT afstemming is gezocht met de DIGIT-officier van justitie voor verdere oordeelsvorming en besluitvorming. De Inspectie merkt wel op dat deze situaties zijn gejournaliseerd en niet in alle gevallen zijn geverbaliseerd. Gevolg hiervan is dat deze informatie alleen voor DIGIT beschikbaar is en geen deel uitmaakt van het procesdossier. Deze werkwijze is door DIGIT per casus afgestemd met de DIGIT-officier van justitie. Het detecteren van afwijkingen in de uitvoering is echter nog geen ingericht en ingebed proces binnen DIGIT. Hierdoor is sprake van een grote afhankelijkheid van de oplettendheid van de individuele medewerkers. Dit onderstreept het belang van voortgang op het gebied van kwaliteitszorg en interne controle. Zie daartoe tevens de bevindingen in hoofdstuk A.8 van deze bijlage.

Uitvoering door opsporingsambtenaren
Het binnendringen, het plaatsen en verwijderen van een technisch hulpmiddel en het verrichten van onderzoekshandelingen, al dan niet met een technisch

[71] Artt. 126nba,126uba en 126zpa lid 2 en lid 3 Sv.
[72] Hier wordt gedoeld op de afgegeven combibevelen voor de inzet van de bevoegdheid op basis van 126nba (doel b) en 126l Sv. of 126uba (doel b) en 126s Sv.
[73] Artt. 126nba, 126uba en 126zpa lid 7 Sv. "*Het toezicht op de uitvoering van het bevel door de ambtenaren wordt uitgeoefend door de Inspectie overeenkomstig het bepaalde in hoofdstuk 6 van de Politiewet 2012*."

hulpmiddel is voorbehouden aan de opsporingsambtenaren die lid of deelnemer zijn van een technisch team.[74]

In 2022 zijn in het merendeel van de zaken onderzoekshandelingen verricht door medewerkers van DIGIT die niet vooraf formeel aangewezen zijn als deelnemer van het technisch team. Daarmee wordt niet voldaan aan de gestelde regel. De aanwijzing als deelnemer van het technisch team in deze zaken heeft namelijk pas achteraf, in januari 2023, plaatsgevonden. Zie tevens hoofdstuk A.1 (voorbereiding). In het vervolg van deze bijlage wordt door de Inspectie gesproken over deze deelnemers alsof zij formeel aangewezen zijn. Voor alle zaken in 2022 geldt dat de Inspectie op basis van logging vastgesteld heeft dat de personen die in 2022 opsporingshandelingen hebben verricht of wel lid zijn of wel middels de aanwijzing achteraf als deelnemer aangewezen zijn.

Om de kwaliteit en professionaliteit van het onderzoek te borgen moeten de opsporingsambtenaren die op een ad-hocbasis deelnemen aan een technisch team (i.c. deelnemers) volgens het Besluit gedurende de uitvoering van het onderzoek begeleid worden door een lid van een technisch team.[75]

Aan de begeleiding van deelnemers wordt volgens de politie invulling gegeven door het instrueren van de deelnemers tijdens de briefings. Tevens wordt volgens de politie het zogenoemde vier-ogen principe toegepast. Dit vier-ogen principe betekent dat bij deze zaken ten minste twee personen betrokken zijn bij het binnendringen en het verrichten van onderzoekshandelingen. De Inspectie leidt uit het journaal af dat in de zaken waar deelnemers ingezet zijn, voorzien is in het vier-ogen principe.

Tijdens de uitvoering van het bevel behoeven de deelnemers volgens de politie niet permanent begeleid te worden. De politie geeft aan dat deze invullingswijze in overeenstemming is met de afspraak die daarover met de DIGIT-officier van justitie is gemaakt. De Inspectie heeft begrip voor deze werkwijze gelet op het gebruiksgemak van het gebruikte technisch hulpmiddel in de zaken waarvoor deze deelnemers zijn ingezet en de vaststelling dat een vaste groep deelnemers in deze zaken structureel ingezet is en daarmee ook de nodige kennis en ervaring met het gebruik van het betreffende technisch hulpmiddel opgedaan hebben.

Binnendringen

Tijdens de behandeling van het wetsvoorstel CCIII is door de minister aangegeven dat alleen de technische, daartoe aangewezen ambtenaren toegang mogen hebben tot het systeem van waaruit het op afstand binnendringen van het geautomatiseerde werk wordt uitgevoerd.[76] Tevens is door de minister aangegeven dat de geïnfecteerde geautomatiseerde werken niet in verbinding mogen staan met een server van de leverancier van de binnendringsoftware.[77]

[74] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 16; Artt. 23 lid 1, 24 lid 1 en 25 lid 2 Bogw.
[75] Art. 4 lid 3 Bogw (incidentele samenwerking); Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 36.
[76] *Kamerstukken II* 2016/17, 34372, nr. 6, p.52.
[77] *Kamerstukken II* 2016/17, 34372, nr. 6, p.78.

De Inspectie heeft vastgesteld dat de politie in 2022 in 25 zaken commerciële binnendringsoftware heeft ingezet voor het binnendringen. Net als in de voorgaande jaren stelt de Inspectie vast dat deze software gebruik maakt van servers die technisch beheerd worden door een leverancier. Naast de daartoe aangewezen ambtenaren heeft dus ook de leverancier toegang tot het systeem (i.c. de servers) waaruit het op afstand binnendringen van het geautomatiseerde werk wordt uitgevoerd. De Inspectie merkt hierbij op dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor deze commerciële software. Contractueel is afgesproken dat de leverancier uitsluitend inlogt op de servers na toestemming van de politie. De politie kan de toegang door de leverancier echter niet technisch controleren of beperken.

De, door de politie, ingekochte binnendringsoftware is een 'black box'[78] voor de politie, waarbij door hen niet kan worden uitgesloten dat de geïnfecteerde geautomatiseerde werken in verbinding staan met een server van de leverancier van de binnendringsoftware.

In de zaken waar DIGIT geen gebruik heeft gemaakt van commerciële binnendringsoftware heeft de Inspectie vastgesteld dat de systemen van waaruit op afstand is binnengedrongen, in beheer en onder controle staan van de politie. De Inspectie heeft geen aanwijzingen dat ongeautoriseerde toegang tot deze systemen heeft plaatsgevonden.

Onderzoekshandelingen met een technisch hulpmiddel

Na het binnendringen voert het technisch team onderzoek uit in het geautomatiseerde werk. Bij het verrichten van onderzoekshandelingen wordt al dan niet gebruik gemaakt van een technisch hulpmiddel.[79] Als voor het verrichten van onderzoekshandelingen een technisch hulpmiddel ingezet wordt, is het uitgangspunt dat dit een vooraf goedgekeurd hulpmiddel betreft.[80]

In 2022 is in 27 zaken een bevel gegeven voor het gebruik van een technisch hulpmiddel voor het uitvoeren van onderzoekshandelingen. Bij twee van deze zaken is een vooraf door de keuringsdienst goedgekeurd technisch hulpmiddel ingezet. In de andere 25 zaken heeft de officier van justitie bepaald dat het onderzoeksbelang dringend vordert dat een niet gekeurd technisch hulpmiddel wordt gebruikt.[81] De Inspectie stelt vast dat hiermee niet is tegemoetgekomen aan het uitgangspunt dat een vooraf goedgekeurd hulpmiddel wordt ingezet.

In de situatie dat de officier van justitie bepaald heeft dat het onderzoeksbelang dringend vordert dat een niet gekeurd technisch hulpmiddel wordt gebruikt, beschrijft het Besluit twee mogelijke vervolgtrajecten. In de eerste situatie, wat tevens het uitgangspunt is, vindt keuring achteraf plaats en vermeldt de officier van justitie de uitkomst van de keuring na afloop van het gebruik in de

[78] Bij een 'black box' is het gedrag en de exacte werking van een product onbekend bij de afnemer of gebruiker.
[79] Artt. 126nba, 126uba, 126zpa lid 1 Sv
[80] Art.14 lid 1 Bogw en Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 40.
[81] Art. 21 lid 2 Bogw.

processtukken.[82] De Inspectie stelt vast dat deze situatie zich in 2022 niet heeft voorgedaan. In 2022 zijn geen technische hulpmiddelen achteraf ter keuring aangeboden.

Gebruik technisch hulpmiddel waarvan keuring achterwege blijft

In de tweede situatie kan, als uitzondering op de hoofdregel, de keuring van een technisch hulpmiddel geheel achterwege blijven.[83] De officier van justitie is in die situatie van oordeel dat de aard van het technisch hulpmiddel zich verzet tegen keuring.[84] In dat geval vermeldt de officier in de processtukken welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen.[85] De aanvullende waarborgen kunnen op aangeven van de officier van justitie ook (deels) buiten de inzet van het technisch team getroffen zijn.

In 2022 is in 25 zaken door de officier van justitie bepaald dat het onderzoeksbelang dringend vordert dat een niet vooraf gekeurd technisch hulpmiddel wordt ingezet. In 2022 is vooraf vastgelegd welke aanvullende waarborgen door DIGIT voorzien zijn voor de betrouwbaarheid, integriteit en herleidbaarheid van de te vergaren of vast te leggen gegevens. Zie tevens bevinding bij ‘advies inzet’ in hoofdstuk A.2 van deze bijlage.

De DIGIT-officier van justitie heeft in een deel van deze zaken inmiddels beslist dat het betreffende middel zich naar zijn aard verzet tegen keuring. Dit middel wordt ingezet voor een specifieke categorie inzetten. De Inspectie signaleert dat het door de wetgever voorziene uitzonderingstraject van het achterwege blijven van keuring daarmee standaardpraktijk is geworden voor deze specifieke categorie inzetten. Hierbij merkt de Inspectie op dat in 2022 de hackbevoegdheid voornamelijk is ingezet voor deze specifieke categorie inzetten, te weten inzetten op een telefoon.

Door DIGIT getroffen waarborgen
In de aanwezige processen-verbaal in deze zaken heeft DIGIT een beschrijving opgenomen van diverse maatregelen die op aangeven van de DIGIT-officier van justitie zijn getroffen om risico’s te mitigeren voor de betrouwbaarheid van de verzamelde gegevens.

Eén van deze maatregelen is dat het technisch hulpmiddel is getest in een test- en verificatieopstelling. In de loop van 2022 is de gehanteerde testaanpak daartoe door DIGIT aangepast. Testen vinden niet meer zaak-gericht plaats. De testen worden namelijk op voorhand op verschillende typen en versies van geautomatiseerde werken uitgevoerd. Op een later moment kan dan bij een voorgenomen inzet in een zaak verwezen worden naar een testresultaat van een zoveel mogelijk gelijkend geautomatiseerd werk. De Inspectie stelt op basis van logging en het journaal vast dat testen zijn uitgevoerd en dat het testresultaat

[82] Art. 15 eerste lid, art. 21 derde lid en artikelsgewijze toelichting bij artikel 21, p. 44, Bogw; *Kamerstukken I* 2017/18, 34372, nr. G, p.15.
[83] In de nota van toelichting horende bij het Bogw is in de toelichting van artikel 21 aangegeven dat hiervan in de praktijk geen lichtzinnig gebruik gemaakt zal worden en dat het naar verwachting om uitzonderlijke gevallen gaat.
[84] Artt. 15 lid 2 en 21 lid 4 en nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 45.
[85] Art. 21 lid 4 Bogw.

inmiddels in aparte rapportages is vastgelegd. De Inspectie stelt vast dat in de meeste gevallen het geautomatiseerde werk waarnaar voor het testresultaat verwezen wordt, zoveel mogelijk gelijkend is aan het geautomatiseerde werk waarop het technisch hulpmiddel daadwerkelijk is ingezet. De Inspectie constateert echter, evenals in voorgaande jaren, dat de test- en verificatieopstelling als aanvullende waarborg beperkt bijdraagt om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen. Er is namelijk enerzijds een afhankelijkheid met de daadwerkelijke inrichting van het geautomatiseerde werk in gebruik door de verdachte, waarover niet altijd op voorhand uitsluitsel gegeven kan worden. Anderzijds stelt de Inspectie vast dat het gebruikte technisch hulpmiddel dusdanig frequent wordt bijgewerkt, dat in de meeste gevallen de versie van het technisch hulpmiddel tijdens de inzet niet identiek is aan de gehanteerde versie in de betreffende test- en verificatieopstelling. De waarde van het testresultaat is daarmee vooral beperkt tot een momentopname. De Inspectie heeft begrip dat het verkrijgen van identieke omstandigheden bij het testen van dit technisch hulpmiddel een utopie is.

De Inspectie constateert dat een controleerbare duiding en appreciatie van de uitkomsten van de uitgevoerde test voor het geautomatiseerde werk in de voorgenomen inzetten ontbreekt. Dit betekent dat onduidelijk is wat de impact is van niet of niet-succesvol geteste onderdelen bij een voorgenomen inzet en wie daarover beslist. De test- en verificatieopstelling is een vrij kostbare aangelegenheid. De effectieve opbrengst en daarmee de toegevoegde waarde van de test- en verificatieopstelling als maatregel om risico’s te mitigeren voor de betrouwbaarheid van de verzamelde gegevens kan met deze constateringen dan ook betwist worden.

Een andere aanvullende waarborg is dat controles van de integriteit van gegevens moeten plaatsvinden. Deze controles dienen plaats te vinden voor en na de vastlegging van deze gegevens in de technische infrastructuur. Een softwarematige oplossing (script) waarmee deze controles voor een belangrijk deel geautomatiseerd uitgevoerd worden, is eind 2022 in gebruik genomen. De schermopnamevoorziening waarmee de uitvoering van het script controleerbaar vastgelegd zou moeten worden, heeft door technische problemen echter niet gefunctioneerd. De Inspectie stelt dan ook vast dat niet altijd controleerbaar is vastgelegd dat deze controles op elk onderdeel in de keten zijn uitgevoerd.

Gelet op de aard van de waarborgen die door het technisch team getroffen zijn, merkt de Inspectie op dat het uitsluitend treffen van deze waarborgen onvoldoende lijkt om de betrouwbaarheid van de gegevens te waarborgen. Naast de aanvullende waarborgen van het technisch team, kunnen per zaak op aangeven van de zaaksofficier ook diverse aanvullende waarborgen getroffen zijn door de tactische teams. De door de tactische teams getroffen waarborgen zijn niet door de Inspectie onderzocht. Het oordeel of en in welke mate het samenstel van waarborgen afdoende is, is in het Nederlandse strafproces uiteindelijk voorbehouden aan de rechter.

Inzet goedgekeurd technisch hulpmiddel

Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er volgens

de toelichting bij het Besluit vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.[86]

In 2022 is in twee zaken een door de keuringsdienst vooraf goedgekeurd technisch hulpmiddel ingezet. De Inspectie kan echter op basis van logging niet met zekerheid vaststellen dat deze door DIGIT ingezette technische hulpmiddelen tijdens alle fasen van de inzet identiek zijn aan de middelen die door de keuringsdienst zijn gekeurd. Door de keuringsdienst wordt in het keuringsrapport een kenmerk aangebracht om het goedgekeurde technisch hulpmiddel uniek te identificeren. In de ene zaak is echter tijdens de plaatsing en het gebruik van het middel het kenmerk niet op een controleerbare wijze door DIGIT vastgelegd (dan wel handmatig dan wel in de geautomatiseerde logging) en in de andere zaak komt het unieke kenmerk van het goedgekeurde technische hulpmiddel niet overeen met het kenmerk van het technisch hulpmiddel dat door DIGIT is ingezet.

Vervangende waarborgen

Het Besluit biedt de keuringsdienst de ruimte om vervangende waarborgen te stellen op onderdelen waar het technisch hulpmiddel niet voldoet aan in het Besluit gestelde technische eisen.[87] Deze door de politie dan verplicht te treffen vervangende waarborgen worden door de keuringsdienst in het keuringsrapport vastgelegd. Het is bij de uitvoering van het bevel dan ook zaak dat DIGIT deze vervangende waarborgen aantoonbaar implementeert en verantwoording over de naleving aflegt.

In de keuringsrapporten van de ingezette technische hulpmiddelen zijn door de keuringsdienst vervangende waarborgen benoemd. Onderdeel van deze, door DIGIT verplicht te treffen, vervangende waarborgen is dat DIGIT in een proces-verbaal verantwoording aflegt over de handelingen voor het treffen van deze waarborgen.

De Inspectie heeft vastgesteld dat in beide zaken processen-verbaal van bevindingen opgemaakt zijn waarin DIGIT ingaat op deze vervangende waarborgen. De Inspectie constateert dat de processen-verbaal vooral een verklarend karakter hebben, maar niet altijd de gevraagde verantwoording van de handelingen betreft waarmee uitvoering aan de gestelde waarborg gegeven is. Deze verantwoording is ook niet aangetroffen in andere vastlegging, zoals in het journaal. Hierdoor is het voor de Inspectie onvoldoende controleerbaar of de juiste en voldoende activiteiten zijn uitgevoerd om over naleving van deze waarborgen te kunnen rapporteren. Bij navraag heeft de Inspectie gesignaleerd dat soms de door DIGIT uitgevoerde handelingen waarop de verklaring over naleving van een waarborg is gebaseerd, niet ter zake deed of onvoldoende bleek te zijn.

Inzet technisch hulpmiddel dat wordt afgekeurd

Indien de situatie zich voor zou doen dat een reeds ingezet hulpmiddel toch achteraf wordt afgekeurd, dan wordt dit voorgelegd aan de rechter in de strafzaak

[86] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 19.
[87] Art. 18 lid 3 sub e Bogw; artt. 16 t/m 18 Bogw en Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 43.

die beslist over het gebruik van de gegevens als bewijs.[88] In 2022 zijn door DIGIT geen technische hulpmiddelen ingezet die zijn afgekeurd.

Definitie technisch hulpmiddel

In 2022 constateert de Inspectie dat de officier van justitie in enkele zaken het bevel heeft gegeven voor een handmatige inzet in plaats van gebruik te maken van een technisch hulpmiddel. Het Besluit biedt ruimte voor een handmatige inzet.[89] Gelet op de toelichting van het Besluit geniet het de voorkeur dat wordt gewerkt met een goedgekeurd technisch hulpmiddel, omdat er dan vanuit gegaan mag worden dan aan wettelijke vereisten omtrent de betrouwbaarheid, integriteit en herleidbaarheid van het verzamelde bewijs is voldaan.[90] Het besluit voor een al dan niet handmatige inzet wordt genomen door de officier op basis van advies van het technisch team van DIGIT. De Inspectie constateert dat in twee situaties gebruik is gemaakt van software, waarbij het transport van de gegevens van het geautomatiseerd werk naar de technische infrastructuur niet automatisch was ingericht. Om deze reden is volgens de officier van justitie niet voldaan aan de definitie van het technisch hulpmiddel. Naar oordeel van de officier van justitie is in die situaties daarmee sprake van een handmatige inzet. De software voldeed wel aan de overige criteria van een technisch hulpmiddel. De Inspectie heeft bij DIGIT nagevraagd welke (ontwerp)overwegingen ten grondslag lagen aan het advies om het transport naar de technische infrastructuur op een handmatige wijze te verrichten. DIGIT heeft deze vraag niet kunnen beantwoorden. Wanneer was gekozen voor een ontwerp waarbij het transport geautomatiseerd plaats zou vinden, is sprake van een technisch hulpmiddel. In dat geval zou in beginsel de weg bewandeld moeten worden van de keuring van een technisch hulpmiddel door de keuringsdienst.

Naast het feit dat het de Inspectie onduidelijk is om welke reden door DIGIT is gekozen voor een handmatig transport, signaleert de Inspectie dat bij een soortgelijke situatie waar ook geen geautomatiseerd transport was ingericht door de DIGIT-officier van justitie is bepaald dat het ingezette middel zich naar zijn aard verzet tegen keuring. Dit impliceert dat in die situatie wel sprake is van een technisch hulpmiddel.

Deze situatie roept vragen op over het begrip 'technisch hulpmiddel'. Het begrip technisch hulpmiddel is in het Besluit gedefinieerd en op hoofdlijnen omschreven in de parlementaire stukken. In de uitvoeringspraktijk geeft deze definitie en omschrijving ruimte voor discussie en wordt het begrip door de verschillende betrokkenen anders uitgelegd. Ook de Hoge Raad heeft in zijn hoedanigheid als toezichthouder op het OM eind 2022 in zijn onderzoeksrapport[91] een aanbeveling gedaan het begrip op een bepaalde manier uit te leggen. Het is dan ook van belang dat door de wetgever een eenduidige definitie en uitleg gegeven wordt wanneer al dan niet sprake is van een technisch hulpmiddel bij de toepassing van de hackbevoegdheid. Het Besluit stelt namelijk eisen aan een technisch hulpmiddel. De keuringsdienst beoordeelt vervolgens of voldaan wordt aan deze eisen en daarmee

[88] *Kamerstukken II* 2018/19, 34372, nr. 29, p.13.
[89] Zoals bedoeld in art. 21 lid 5 Bogw.
[90] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 19.
[91] https://www.hogeraad.nl/actueel/nieuwsoverzicht/2022/november/hacken-opdracht-gaat-grotendeels-volgens-regels-wel-ruimte-verbetering/

sprake is van een goedgekeurd technisch hulpmiddel. Met een goedgekeurd technisch hulpmiddel wordt volgens de wetgever gewaarborgd dat gegevens die daarmee verzameld worden herleidbaar, integer en betrouwbaar zijn.

Verwijdering van een technisch hulpmiddel

Volgens het Bogw verwijdert een opsporingsambtenaar van het technisch team het technisch hulpmiddel voordat het onderzoek is beëindigd.[92] Hierbij zal worden geprobeerd het geautomatiseerde werk in de oorspronkelijke staat achter te laten, dat wil zeggen als ware de bevoegdheid nooit toegepast.[93]

In 2022 is in 25 zaken bevel gegeven voor de inzet van een commercieel technisch hulpmiddel waarvan uitsluitend de leverancier inzicht heeft in de precieze werking van het betreffende middel. Hierdoor kan niet worden vastgesteld of in alle gevallen verwijdering daadwerkelijk volledig heeft plaatsgevonden.

In de andere zaken waar een technisch hulpmiddel is ingezet, zijn geen aanwijzingen dat een onvolledige verwijdering heeft plaatsgevonden.

Er kan zich een situatie voordoen dat een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk. In de parlementaire stukken is aangegeven dat de met verwijdering belaste opsporingsambtenaar in dat geval het transport van de door het technisch hulpmiddel geregistreerde gegevens naar de technische infrastructuur beëindigt.[94]

In de zaken waarvoor in 2022 een bevel tot het inzetten van de hackbevoegdheid is gegeven, heeft deze situatie zich niet voorgedaan.

Toegang leverancier technisch hulpmiddel

Tijdens de parlementaire behandeling van het wetsvoorstel CCIII is door de minister in beantwoording op vragen aangegeven dat in het kader van het onderzoek met een technisch hulpmiddel er geen verbinding tot stand gebracht wordt met een server van de maker van het technisch hulpmiddel. Er wordt uitsluitend een verbinding tot stand gebracht tussen het binnengedrongen geautomatiseerde werk en de server van de politie.[95] In de beantwoording geeft de minister aan dat de leverancier geen mogelijkheid dient te hebben om zelfstandig updates uit te voeren en zelf de controle over het geautomatiseerd werk over te nemen. Evenmin kunnen andere klanten van de leverancier toegang krijgen tot het geautomatiseerd werk.[96]

In 2022 zijn in 20 zaken onderzoekshandelingen verricht met een technisch hulpmiddel dat een 'black box' is voor de politie. De leverancier van het technisch hulpmiddel heeft de servers die de politie hiervoor gebruikt in technisch beheer en kan op afstand inloggen om beheer- en supportwerkzaamheden uit te voeren.

---

[92] Artikel 126nba lid 6 Sv.
[93] *Kamerstukken II* 2015/16, 34372 nr. 3, p.36 (MvT); *Kamerstukken II* 2016/17, 34372 nr. 6, p.76.
[94] Artikel 26 lid 1 Bogw; *Kamerstukken II* 2015/16, 34 372 nr. 3 memorie van toelichting, p.36. "*Wanneer de software aanwezig blijft in het geautomatiseerde werk waarin de bevoegdheid is toegepast, wordt vanuit de server van de politie het dataverkeer stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerde werk.*"; *Kamerstukken II* 2016/17, 34 372 nr.6 p.78. "*Hier zien de opsporingsambtenaren van het technisch team op toe*".
[95] *Kamerstukken II* 2016/17, 34372, nr.6, p.45 en p.51.
[96] *Kamerstukken II* 2016/17, 34372, nr.6, p.74.

Werkzaamheden die de leverancier uitvoert, mogelijk zelfs tijdens uitvoering van een bevel, kunnen gevolgen hebben voor de werking en functionaliteit van het technisch hulpmiddel. De Inspectie merkt hierbij op dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor deze commerciële software. De politie stelt dat er geen alternatief voorhanden is dat dezelfde functionaliteit biedt zonder deze nadelen. Contractueel is afgesproken dat de leverancier uitsluitend inlogt op de servers na toestemming van de politie. De Inspectie heeft voorbeelden gezien van gevraagde toestemming die door de politie is verleend en waarvan een overzicht door DIGIT bijgehouden is. Door het 'black box' karakter van het technisch hulpmiddel kan de politie de toegang door de leverancier echter niet technisch beperken of controleren. Tevens kan hierdoor niet gegarandeerd worden dat bij gebruik van het technisch hulpmiddel uitsluitend verbindingen tot stand gebracht worden tussen het geautomatiseerde werk en de servers van de politie. De Inspectie merkt daarnaast op dat de door de politie verzamelde gegevens geruime tijd beschikbaar blijven in het technisch hulpmiddel waar ook de leverancier op afstand toegang toe heeft. De toegang tot deze onderzoeksgegevens door de leverancier is ook mogelijk voordat permanente vastlegging van de onderzoeksgegevens in de technische infrastructuur bij DIGIT plaatsvindt. Dit heeft de Inspectie ook in haar eerdere verslagen geconstateerd. In reactie hierop heeft de minister benadrukt dat alleen het technisch team van de politie toegang heeft tot de servers waarop onderzoeksgegevens worden vastgelegd.[97] Hierbij doelt de minister op de technische omgeving waarin de onderzoeksgegevens uiteindelijk permanent door DIGIT worden bewaard. De toegang tot deze gegevens in die omgeving is beperkt tot enkele medewerkers van DIGIT. De leverancier heeft geen toegang tot deze specifieke omgeving.

Centrale registratie toegang en toegangsverlening technisch hulpmiddel

In het Besluit is aangegeven 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).[98] De korpschef wijst een of meer ambtenaren aan die belast zijn met de centrale registratie van de toegang tot technische hulpmiddelen. Deze ambtenaar verschaft toegang tot het technisch hulpmiddel aan de met plaatsing van het technisch hulpmiddel belaste opsporingsambtenaar voor de duur van het bevel. De ambtenaar die belast is met de centrale registratie registreert de naam van de opsporingsambtenaar die om toegang heeft verzocht, het tijdstip van toegangsverlening en enkele kenmerken van het technisch hulpmiddel.[99]

Evenals voorgaande jaren stelt de Inspectie vast dat binnen DIGIT geen proces geïmplementeerd is voor de registratie van toegang, uitgifte en inname van technische hulpmiddelen. In een reactie heeft de politie eerder aangegeven dat in overleg met de DIGIT-officier van justitie afgeweken wordt van de eis voor centrale registratie en toegangsverlening tot technische hulpmiddelen. Dit omdat een

[97] *Kamerstukken II* 2020/21, 29628, nr. 1030, p.7.
[98] Besluit technische hulpmiddelen strafvordering, *Stb* 2006, nr. 524. ' Dit Besluit is op 7 november 2006 in het Staatsblad gepubliceerd.
[99] Art. 22 Bogw en Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 45.

dergelijk proces praktisch niet werkbaar zou zijn. De Inspectie merkt op dat DIGIT in 2022 een systeem in gebruik heeft genomen waarmee de uitgifte van digitale sleutels (fysieke tokens) kan worden geregeld en geregistreerd. Dergelijke tokens worden ook gebruikt door het technisch team voor toegang tot het commerciële technische hulpmiddel. Ook zijn er ontwikkelingen ten aanzien van de geregistreerde overdracht van eigen ontwikkelde software. Hiermee kan naar mening van de Inspectie wel deels tegemoet gekomen worden aan de vereiste centrale registratie en toegangsverlening. DIGIT heeft de mogelijkheden en het proces hiervoor echter in 2022 niet verder verkend, uitgewerkt en geformaliseerd.

Onderzoekshandelingen middels handmatige inzet

Indien de officier van justitie besluit dat het verrichten van onderzoekshandelingen plaatsvindt zonder technisch hulpmiddel, dan worden procedurele waarborgen getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen. Het kunnen afleggen van verantwoording over de implementatie en opvolging van de aan DIGIT gestelde waarborgen op een controleerbare en aantoonbare wijze is een belangrijk aspect voor de kwaliteit van de taakuitvoering door de politie.

In 2022 was in acht zaken voorzien dat onderzoekshandelingen uitgevoerd worden zonder een technisch hulpmiddel. De Inspectie is, aan de hand van de documentatie (het advies inzet) en in voorkomende gevallen het journaal, in deze zaken nagegaan welke waarborgen daartoe door DIGIT voorzien waren en in welke mate deze waarborgen aantoonbaar getroffen en nageleefd zijn.

De Inspectie stelt vast dat in deze zaken verschillende voorziene waarborgen vooraf benoemd en vastgelegd zijn. Ten opzichte van de situatie in 2021 is het vooraf vastleggen van waarborgen een verbetering, omdat deze controleerbare vastlegging van beoogd te treffen waarborgen de basis vormt om achteraf te kunnen controleren of naleving heeft plaatsgevonden.

De Inspectie stelt daarnaast vast dat door DIGIT geen controle op het juist opvolgen van deze waarborgen plaatsvindt. Ook verantwoording achteraf over de feitelijke naleving van deze waarborgen - bijvoorbeeld in het proces-verbaal of journaal - vindt niet plaats. Zo vormt in alle acht zaken het maken van beeldschermopnamen en het vastleggen van toetsaanslagen van de onderzoekshandelingen onderdeel van de te treffen waarborgen. Evenals in 2021, stelt de Inspectie vast dat in enkele zaken de beeldschermopnames en registratie van toetsaanslagen niet volledig zijn. In hoofdstuk A.5 van deze bijlage gaat de Inspectie verder in op deze beeldscherm- en toetsaanslagopnamen.

Daarnaast blijkt in de uitvoering dat van enkele andere voorziene waarborgen bij DIGIT onduidelijk is wat ermee beoogd en bedoeld wordt. De Inspectie leidt mede daaruit af dat in de praktijk geen expliciete aandacht besteed wordt aan het voldoen aan deze waarborgen.

Door onduidelijke waarborgen en het mede daardoor ontbreken van een controleerbare implementatie en opvolging van deze waarborgen vraagt de Inspectie zich af of in voldoende mate tegemoet gekomen wordt aan het onderliggende door de wetgever beoogde doel. Dat doel is namelijk om met het

treffen van deze waarborgen de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens zeker te stellen. Hierbij merkt de Inspectie op dat bij een zaak, naast de aanvullende waarborgen van het technisch team, op aangeven van de zaaksofficier ook diverse aanvullende waarborgen getroffen kunnen worden door de tactische teams. Deze waarborgen zijn niet door de Inspectie onderzocht. Het oordeel over of en in welke mate het samenstel van waarborgen afdoende is om de betrouwbaarheid, de integriteit en de herleidbaarheden zeker te stellen, is in het Nederlandse strafproces uiteindelijk voorbehouden aan de rechter.

Functiescheiding tussen technisch team en tactisch team

De resultaten van de onderzoekshandelingen worden ter beschikking gesteld aan de opsporingsambtenaren die zijn betrokken bij het operationele onderzoek, ook wel aangeduid als het tactisch team.[100] Om het risico van tunnelvisie te beperken moet volgens het Besluit gedurende het opsporingsonderzoek een strikte taakverdeling en functiescheiding tussen het technisch en het tactisch team aanwezig zijn.[101] 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.[102] Tevens hebben de tactisch opsporingsambtenaren geen toegang tot de technisch infrastructuur waar de tijdens onderzoekhandelingen verkregen gegevens door het technisch team zijn vastgelegd.[103]

Volgens het journaal van het technisch team is in 2022 enkele malen contact geweest met leden van tactische teams over de inzet van een technisch hulpmiddel. De Inspectie heeft er begrip voor dat tijdens een operationele inzet hiertoe tussen de teams contact is en dat de door de wetgever beoogde strikte scheiding in de praktijk niet altijd werkbaar is. De Inspectie heeft geen aanwijzingen dat door het tactisch team invloed is uitgeoefend op het binnendringen in het geautomatiseerd werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel. De Inspectie heeft geen aanwijzingen dat leden van een tactisch team toegang hebben tot technische hulpmiddelen en de technische infrastructuur van DIGIT. Van een eigenstandige beïnvloeding van de werking en gebruik van de software door het tactisch team is dan ook geen sprake.

A.5 Logging en andere verslaglegging

Onder logging verstaat het Besluit de elektronische verslaglegging over de uitvoering van een bevel.[104] Hierbij wordt onderscheid gemaakt tussen gegevens over:

[100] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p.14; *Kamerstukken II* 2015/16, 34372 nr.3 p.14.
[101] *Kamerstukken II* 2016/17, 34372 nr.6, p.28. Vanwege de functiescheiding wordt het onderzoek in een geautomatiseerd werk uitgevoerd door speciaal daarvoor opgeleide opsporingsambtenaren die niet betrokken zijn bij het betreffende opsporingsonderzoek.
[102] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 36; *Kamerstukken II* 2016/17, 34372, nr. 6, p.40 en p.59; Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p.17: "*De organisatorische scheiding tussen het technische team en het tactische team behoeft de samenwerking tussen de teams gedurende het opsporingsonderzoek niet te belemmeren. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt, vervult hierbij een schakelfunctie.*"
[103] Bogw, Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 20; *Kamerstukken II* 2016/17, 34372, nr.6, p.52.
[104] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 17.

- de verrichte handelingen tijdens de voorbereidende fase, het binnendringen in het geautomatiseerd werk alsmede de handelingen die gedurende de onderzoeksfase worden verricht.[105] De toelichting noemt dit 'inzetlogging'. Hierbij wordt de vastlegging genoemd van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar, de communicatie tussen de technische infrastructuur en het geautomatiseerd werk en gebruikte scripts en softwareversies.
- gegevens over de toegang tot een technisch hulpmiddel en het functioneren van de technische infrastructuur.[106] De toelichting noemt dit 'systeemlogging' die automatisch door alle gebruikte systemen wordt gegenereerd en centraal wordt verzameld en vastgelegd en betrekt hierbij ook de logging van toegang tot een technisch hulpmiddel;[107]
- gegevens over de ter uitvoering van het bevel door middel van onderzoekshandelingen verkregen gegevens (metadata).[108]

Het uitgangspunt voor deze logging is dat vastlegging doorlopend en automatisch plaatsvindt.[109] De gegevens over de verrichte handelingen (inzetlogging) mogen als uitzondering handmatig vastgelegd worden als deze gegevens naar hun aard niet automatisch vastgelegd kunnen worden.[110] De nota van toelichting benoemt in dit kader het journaal van de opsporingsambtenaar en de vastlegging van gebruikte scripts en softwareversies.[111]

Een voorwaarde om te kunnen komen tot een juiste en volledige implementatie en controleerbare naleving van de logging is dat de politie zelf vastlegt en verantwoordt op welke wijze zij beoogt invulling te geven aan de vastlegging van gegevens over de uitvoering in logbestanden. De invulling en inrichting hiervan kan bovendien per zaak verschillen. Aanvullend moet in de praktijk helder zijn wat de door de wetgever bedoelde technische infrastructuur omvat zodat door DIGIT op een juiste en volledige wijze invulling gegeven kan worden aan het vastleggen van gegevens over het functioneren van de technische infrastructuur.

In het verslag over 2021 heeft de Inspectie gemeld dat de politie een start gemaakt had met het vastleggen en uitwerken van de wijze waarop zij invulling wil geven aan de diverse typen van logging die zijn beschreven in de nota van toelichting bij het Bogw. Ook heeft de Inspectie in dat verslag vermeld dat de politie een aanzet gemaakt had om de reikwijdte van de technische infrastructuur te bepalen en invulling te geven aan het begrip onregelmatigheid maar dat het proces daarvoor nog niet was afgerond.

De Inspectie stelt vast dat DIGIT in 2022 op deze onderwerpen geen voortgang heeft geboekt. De politie heeft nog onvoldoende uitgewerkt en vastgelegd hoe zij in

[105] Art. 5 lid 1 sub a Bogw en artikelsgewijze toelichting artikel 5, p.36 waarin aangegeven is dat alle handelingen die tijdens het onderzoek in een geautomatiseerd werk plaatsvinden, worden gelogd.
[106] Artikel 5 lid 1 sub b en d Bogw.
[107] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p.18.
[108] Artikel 5 lid 1 sub d Bogw.
[109] Artikel 5 lid 1 en lid 2 Bogw.
[110] Artikel 5 lid 2 Bogw, handelingen naar hun aard niet automatisch vast te leggen; Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 36; B Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 17. "*De inzetlogging zal zoveel mogelijk geautomatiseerd plaatsvinden. Voor zover dit technisch niet mogelijk is, wordt procedureel binnen de politieorganisatie vastgelegd dat handmatige logging plaatsvindt.*"
[111] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 17.

de praktijk, per zaak, invulling geeft aan de bedoelde doorlopende en automatische vastlegging van gegevens over de uitvoering van een bevel in logbestanden. De Inspectie constateert dat de politie de kaders voor deze logging en een controleerbare implementatie hiervan nog niet op orde heeft. De voornaamste reden hiervan is volgens DIGIT het gebrek aan personele capaciteit en dat DIGIT een operationeel opsporingsteam is waardoor de prioriteit vooral ligt bij het operationele proces.

In de praktijk heeft de politie ook in 2022 voor de inrichting en toepassing van de logging vooral als uitgangspunt genomen wat technisch standaard voorhanden is binnen de gebruikte toepassingen[112], in plaats van wat op basis van een risicoanalyse nodig is en wat volgt als vereiste uit het Bogw. Hierdoor is wel veel logging aanwezig en is daarmee technisch gezien sprake van doorlopende en automatische logging op verschillende niveaus. DIGIT kan echter niet aantonen dat deze beschikbare logging voldoende effectief is gelet op het doel en het gebruik van de logging. Hierdoor kan de politie niet aantonen dat zij op dit onderwerp in de volle omvang en te allen tijde voldoet aan de vereisten uit het Bogw.

De nota van toelichting benoemt in het kader van de logging ook de vastlegging van gebruikte scripts en softwareversies. Evenals vorig jaar stelt de Inspectie vast dat niet controleerbaar is vastgelegd welke (versies van) scripts op welk moment zijn ingezet.

Belang logging en onregelmatigheid

De logging is in de eerste plaats van belang voor het uitvoeren van de interne controle door de politie op de verrichte handelingen en de controle op het functioneren van de technische infrastructuur.[113] Op basis van deze logging moet de politie zowel tijdens de uitvoering van een bevel als na afloop daarvan kunnen vaststellen of een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de met de onderzoekshandelingen verkregen gegevens.[114] In aanvulling daarop moet de politie op basis van logging verantwoording kunnen afleggen in een strafzaak of als in het kader van het toezicht door de Inspectie JenV twijfels ontstaan over de verrichte handelingen en/of de betrouwbaarheid van het hiermee vergaarde bewijs.[115] Ook is de logging van belang mocht er sprake zijn van het optreden van schade en een mogelijke schadeclaim door betrokkene.[116]

---

[112] De Inspectie doelt hier op diverse ICT-componenten waaronder servers, werkstations, netwerkcomponenten zoals firewalls en applicaties.

[113] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, 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.*". 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; *Kamerstukken I* 2016/17, 34 372 D, pagina 20. "*Op deze wijze kan zowel tijdens het verrichten van onderzoekshandelingen als achteraf intern toezicht plaatsvinden binnen de politieorganisatie op de uitvoering van het bevel van de officier van justitie*."

[114] Art. 6 lid 1 Bogw, vaststelling van onregelmatigheden; Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 17 en 36.

[115] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 36 en 37.

[116] *Kamerstukken II* 2016/17 34372, nr. 6, p.69 en p.80.

Een nadere uitwerking van welke gebeurtenissen de politie als 'onregelmatigheid' ziet, is ook in 2022 niet aangetroffen. Die uitwerking is van belang omdat de logging zodanig ingericht moet zijn dat vastgesteld kan worden of deze onregelmatigheden hebben plaatsgevonden om daarover vervolgens ook te kunnen rapporteren.[117] De politie geeft in een reactie aan dat het uitwerken van een onregelmatigheid niet direct voortvloeit uit een wettelijke verplichting en om deze reden de uitwerking niet plaatsvindt.

De Inspectie stelt vast dat omdat een controleerbaar afwegingskader ontbreekt, de eerste afweging of sprake is van een onregelmatigheid in belangrijke mate gebaseerd is op de professionele inschatting door individuele medewerkers van DIGIT. Daarnaast merkt de Inspectie op dat de door de politie geformuleerde definitie een technische focus heeft op gebeurtenissen binnen de technische infrastructuur en niet op de gegevens zelf en ook niet op het gehele inzet-proces. Hierdoor worden procesmatige afwijkingen mogelijk niet als onregelmatigheid aangemerkt. Dit geldt tevens voor technische afwijkingen die optreden buiten de technische infrastructuur.

De politie kan hierdoor, zoals ook in voorgaande jaren door de Inspectie is geconstateerd, niet aantonen dat voldoende en juist gelogd wordt om het optreden van onregelmatigheden, zowel tijdens de uitvoering van het bevel als achteraf, te kunnen vaststellen. Evenals in 2021 is niet door de politie uitgewerkt op welke wijze, door wie en wanneer het monitoren op onregelmatigheden vanuit een interne verantwoordelijkheid plaatsvindt. Dit heeft raakvlakken met de bevindingen m.b.t. de informatiebeveiliging, het kwaliteitssysteem en controle in hoofdstuk A.8 van deze bijlage.

Beeldschermopnamen en opname van toetsaanslagen

DIGIT verwijst voor de logging van handelingen die verricht worden door de opsporingsambtenaren naar een voorziening die zij gebruikt om beeldschermopnamen te maken. Naast deze beeldschermopnamen worden in bepaalde gevallen ook de bijbehorende toetsaanslagen vastgelegd. In de voorgaande verslagjaren heeft de Inspectie vastgesteld dat deze opnamen mede door technische problemen niet altijd aanwezig waren. Ook begin 2022 was sprake van hiaten in zowel de beeldscherm- als toetsaanslagopnamen. In de loop van 2022 is naast de al aanwezige opnamevoorziening een nieuwe voorziening gebaseerd op andere technologie ingezet, waardoor deze opnamen gedurende de rest van het jaar wel volledig waren.

De Inspectie heeft in de afgelopen jaren onder andere deze opnamen als onderdeel van de beschikbare logging gebruikt om achteraf, in combinatie met de handmatige vastlegging van DIGIT in het journaal, te reconstrueren welke handelingen in zaken uitgevoerd zijn en of dat met elkaar in overeenstemming is.

De inmiddels structurele vastlegging van deze opnamen heeft echter ook een keerzijde. Alleen al in 2022 is duizenden uren aan beeldmateriaal beschikbaar. De aard en grote hoeveelheid van de beeldschermopnamen leidt ertoe dat deze

[117] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 36.

opnamen inmiddels niet geschikt zijn om zonder gerichte aanwijzingen onderzoek te doen naar het optreden van mogelijke afwijkingen of onregelmatigheden. Daarnaast constateert de Inspectie dat de vastlegging van toetsaanslagen mede door het ontbreken van belangrijke contextinformatie, waaronder een tijdsaanduiding, van beperkte waarde is gebleken. Kortom, deze manier van logging is niet ingericht om controle en toezicht in alle gevallen effectief te kunnen uitoefenen.

De Inspectie stelt vast dat deze logging van beeldscherm- en toetsaanslagopnamen door de politie zelf in de praktijk niet actief gebruikt wordt om tijdens de uitvoering van het bevel en achteraf eventuele afwijkingen of onregelmatigheden te signaleren. Naast deze vorm van logging zijn ook andere vormen van logging, waaronder systeemlogging en authenticatielogging beschikbaar. Hiervan heeft de Inspectie - zoals eerder in dit verslag vermeld - echter geconstateerd dat voor de inrichting en toepassing van deze logging door DIGIT vooral als uitgangspunt genomen is wat technisch standaard voorhanden is in plaats van wat op basis van een risicoanalyse nodig is en wat volgt als vereiste uit het Bogw. De Inspectie stelt vast dat beschikbare logging door de politie veelal op ad-hocbasis gebruikt wordt om zowel tijdens de uitvoering van het bevel als achteraf toe te zien en eventuele afwijkingen of onregelmatigheden te signaleren. Een afwegingskader om te bepalen of daar sprake van is, ontbreekt. Zoals ook in eerdere jaren door de Inspectie is gerapporteerd, is niet door de politie uitgewerkt op welke wijze, door wie en wanneer het structureel monitoren vanuit een interne verantwoordelijkheid plaatsvindt en hoe daarover verantwoording wordt afgelegd. Het is in beginsel aan de politie zelf om te monitoren of dergelijke gebeurtenissen optreden. De Inspectie acht het van belang dat het signaleren en monitoren op eventuele afwijkingen of onregelmatigheden door DIGIT zelf plaatsvindt. Dit dient door DIGIT structureel en controleerbaar ingericht en uitgevoerd te worden. Bij het uitvoeren van systeemtoezicht moet de Inspectie kunnen steunen op de kwaliteitszorg en de door de politie zelf uitgevoerde (interne) controles. Zie daarvoor tevens in breder verband in hoofdstuk A.8 de bevindingen met betrekking tot kwaliteitszorg en de eigen (interne) controle door de politie die onvoldoende ontwikkeld en effectief is.

De Inspectie concludeert dat met alleen beeldscherm- en toetsaanslagopnamen er geen doelmatige en effectieve invulling gegeven kan worden aan de vereiste vaststelling of onregelmatigheden tijdens de uitvoering van een bevel en achteraf zijn opgetreden. De Inspectie verwijst dan ook naar de hiervoor beschreven benodigde uitwerking door DIGIT hoe invulling gegeven wordt aan de doorlopende en automatische logging en de wijze waarop het optreden van onregelmatigheden wordt gesignaleerd.

Betrouwbaarheid logbestanden

Gelet op het belang van de logging schrijft het Besluit voor dat de inhoud van logbestanden niet gewijzigd kan worden en dat de toegang tot logbestanden beperkt is tot alleen daartoe geautoriseerde personen.[118] Een uitwerking hiervan is dat de doorlopende en automatische logging over de uitgevoerde handelingen

[118] Art. 7 Bogw en de artikelsgewijze toelichting op het Besluit artikel 7, p.37. Art. 7 tweede lid Bogw stelt dat logbestanden uitsluitend toegankelijk moeten zijn voor door de korpschef aangewezen ambtenaren.

vastgelegd worden op een server van de politie[119] en dat leden van het technisch team geen toegang hebben tot de server waarop de logging plaatsvindt.[120]

Zoals hiervoor is aangegeven constateert de Inspectie dat door de politie nog niet is uitgewerkt hoe en waar de doorlopende en automatische vastlegging van gegevens in logbestanden plaatsvindt. Een inrichting van logging die bovendien per opsporingsonderzoek (zaak) kan verschillen. Deze uitwerking is van belang voor de politie om te kunnen komen tot het treffen van passende maatregelen voor het waarborgen van de betrouwbaarheid en de integriteit van deze logbestanden.

De Inspectie stelt vast dat logbestanden op verschillende plekken (soms tijdelijk) opgeslagen zijn. Uiteindelijk wordt een groot deel van deze logbestanden vastgelegd in een voorziening die door de politie tot de technische infrastructuur gerekend wordt. Naast de eerdergenoemde beeldscherm- en toetsaanslagopnamen gaat het daarbij om logging van diverse systemen en applicaties in gebruik door DIGIT. Op basis van de netwerkarchitectuur en de getroffen maatregelen heeft de Inspectie geen aanwijzingen dat deze logbestanden kunnen worden aangepast nadat deze opgeslagen zijn in deze technische voorziening. Uitsluitend beheerders van het infrastructuur beheerteam van DIGIT kunnen informatie uit deze technische voorziening verwijderen. De Inspectie heeft vastgesteld dat de logbestanden uitsluitend in leesbare vorm uit deze technische infrastructuur kunnen worden gekopieerd door twee medewerkers van DIGIT die beschikken over de benodigde toegang tot de betreffende digitale sleutel (hardware token).

De Inspectie benadrukt dat maatregelen voor het waarborgen van de betrouwbaarheid van de logbestanden niet alleen binnen deze technische infrastructuur getroffen moeten worden, maar van belang zijn in de gehele keten van logging. Hiermee doelt de Inspectie op het door de politie in kaart brengen van deze keten en het op basis van risicomanagement aantoonbaar treffen van preventieve en repressieve maatregelen vanaf de bron waar deze logbestanden gegenereerd worden tot en met het transport en de eventuele (tussentijdse) verwerking en opslag daarvan. Het loggingsproces zelf moet bovendien zo ingericht zijn dat de loggingsinformatie tijdens de fase van bewijsvergaring te allen tijde blijft functioneren en niet valt te manipuleren, te wijzigen of te verwijderen zonder dat dit achteraf zichtbaar is.[121] Een aandachtspunt is daarnaast dat maatregelen niet alleen gericht moeten zijn op de integriteit van de logbestanden, maar tevens op de vertrouwelijkheid. Dit is vooral relevant voor de voorzieningen die verder af staan van de technische infrastructuur.

Samengevat herhaalt de Inspectie haar aanbeveling uit eerdere verslagjaren dat het van belang is dat de politie zelf vastlegt en uitwerkt hoe de doorlopende en automatische vastlegging van gegevens in logbestanden zowel in het algemeen als zaak-specifiek plaatsvindt en dat de logging ook aantoonbaar en controleerbaar wordt ingezet. Daarbij moet duidelijkheid geboden worden wat, waar, hoe en met welk doel de logging plaatsvindt en welke controles daarop door wie, wanneer plaatsvinden. Dit is randvoorwaardelijk voor het aantoonbaar kunnen bepalen en

[119] *Kamerstukken II* 2016/17, 34372, nr.6, p. 52.
[120] *Kamerstukken II* 2016/17, 34372 nr. 6, p. 52 en p.59.
[121] *Kamerstukken II* 2016/17, 34 372, nr. 6, p.52 en p.59.

treffen van passende maatregelen om de betrouwbaarheid en integriteit van deze logbestanden te waarborgen.

Vastgelegde gegevens (bewijslogging)

Door het technisch team verzamelde gegevens die kunnen dienen als bewijs in een strafzaak moeten vastgelegd worden op een technische infrastructuur.[122] Het Besluit definieert de technische infrastructuur als een technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel.[123]

De Inspectie heeft in voorgaande verslagjaren geconstateerd dat de politie nog niet bepaald had wat de reikwijdte van de technische infrastructuur is waardoor de Inspectie niet met zekerheid kon vaststellen of alle bewijslogging wel op de juiste plek en op betrouwbare wijze is vastgelegd. De Inspectie stelde in haar verslag over 2021 vast dat DIGIT een aanvang gemaakt heeft met het bepalen en vastleggen van de reikwijdte van de technische infrastructuur. De Inspectie stelt vast, zoals in de inleiding van deze paragraaf vermeld, dat DIGIT op dit onderwerp in 2022 geen voortgang heeft geboekt. Daarmee is nog steeds onvoldoende duidelijk wat de reikwijdte van de technische infrastructuur volgens DIGIT is.

Volgens de toelichting op het Besluit dienen de betrouwbaarheid en integriteit van de vastgelegde gegevens onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing.[124] De gegevens mogen niet inhoudelijk worden bewerkt en dienen te worden beveiligd tegen wijziging en kennisneming door onbevoegden. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben daartoe geen toegang.[125] Vereist is dat de opslag van deze gegevens uitsluitend plaatsvindt op een beveiligde politieserver in beheer van de politie die zich in Nederland bevindt.[126] Voor de opslag van onderzoeksgegevens op de technische infrastructuur van de politie wordt geen gebruik gemaakt van een server van de leverancier van de (onderzoeks)software.[127]

Een belangrijk onderdeel van de technische infrastructuur vormt een speciaal hiervoor ontwikkelde technische voorziening waar de bewijslogging (de verzamelde gegevens) uiteindelijk wordt vastgelegd. Ten aanzien van die voorziening en de gegevens die daarin opgeslagen zijn, stelt de Inspectie vast dat in 2022:

- de door DIGIT verkregen bewijslogging vastgelegd is in deze voorziening die onderdeel uitmaakt van de technische infrastructuur;
- maatregelen van kracht waren om de gegevens in deze voorziening te beschermen tegen wijzigingen en tegen kennisname door onbevoegden;
- de gegevens uitsluitend toegankelijk waren voor medewerkers van DIGIT, waaronder het technisch team. Ook waren de gegevens toegankelijk voor de

[122] Art. 27 lid 1 Bogw. Vastlegging van gegevens op een technische infrastructuur.
[123] Artikel 1 sub g Bogw, definitie van een technische infrastructuur.
[124] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 21.
[125] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 47.
[126] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 18 en 47; *Kamerstukken II* 2016/17, 34372, nr.6, p.74.; *Kamerstukken II* 2018/19, 34. 372, nr. 29 p. 11 en p. 12.
[127] *Kamerstukken II* 2018/19, 34372, nr. 29, p.12.

Inspectie ten behoeve van het toezicht. De toegang voor het technisch team is volgens de letter niet in lijn met de beantwoording door de toenmalige minister van Justitie en Veiligheid op vragen van de vaste commissie van Justitie en Veiligheid.[128] In een reactie geeft de minister aan dat zodra de gegevens zijn vastgelegd op de technische infrastructuur hiertoe geen toegang meer verkregen kan worden door leden van een technisch team. Een dergelijke strikte uitleg is echter niet te verenigen met de overdracht van gegevens aan een tactisch team die afkomstig moeten zijn uit de technische infrastructuur. Van belang lijkt vooral dat vastgelegde gegevens beschermd zijn tegen wijzigingen. De Inspectie stelt vast dat toegang tot deze gegevens in de technische infrastructuur beperkt is tot alleen raadplegen en dat vastgelegde gegevens niet gewijzigd kunnen worden door leden van het technisch team;

- de opslag van de gegevens in deze voorziening plaatsvindt op een beveiligde politieserver in beheer van de politie die zich in Nederland bevindt. De Inspectie stelt echter vast dat een gedeelte van de bewijslogging daarnaast ook is opgeslagen op locaties die geen onderdeel vormen van deze technische infrastructuur. In die situaties bevonden deze gegevens zich daar geruime tijd voordat sprake was van vastlegging binnen de technische infrastructuur. Deze tijdelijke opslag van een deel van de bewijslogging vond in het merendeel van deze gevallen plaats op servers die technisch worden beheerd door een externe leverancier. Behoudens procedurele afspraken in een addendum bij het contract, kan de politie niet waarborgen dat deze gegevens op deze locatie zijn beschermd tegen wijziging en onbevoegde kennisname door de leverancier.

Andere verslaglegging (proces-verbaal en journaal)

Een proces-verbaal is een officieel op papier gesteld verslag van de politie.[129] Een proces-verbaal vormt samen met het journaal en de elektronische logging een belangrijke waarborg voor de controleerbaarheid van de uitvoering van het bevel.[130] De verbaliseringsplicht houdt in dat de opsporingsambtenaren proces-verbaal[131] opmaken van de door hen verrichte handelingen zodat daarover verantwoording afgelegd kan worden.[132]

In het journaal wordt door de opsporingsambtenaren, als een soort dagboek, handmatig verslaglegging gedaan over het procesverloop, de afspraken en de verrichtingen die zich niet lenen voor automatische vastlegging. Het journaal is een intern werkdocument van de politie dat niet bij de processtukken hoeft te worden gevoegd.[133]

De Inspectie stel vast dat in 2022:

- De doorlooptijd van het opstellen en ondertekenen van het proces-verbaal in 2022 toegenomen is. Dit terwijl de Inspectie in haar verslag over 2021 juist gerapporteerd had dat sprake was van een verbetering. Het toenemen van de doorlooptijd doet zich vooral voor bij de processen-verbaal van

[128] *Kamerstukken II* 2018/19, 34372, nr.29, p.9.
[129] https://www.politie.nl/informatie/wat-is-een-proces-verbaal.html
[130] *Kamerstukken II* 2015/16, 34372 nr. 3, p. 78.
[131] Zie wetboek van stafvordering art.152 (ten spoedigste), art. 153 (ambtseed, persoonlijk, gedagtekend, ondertekend en redenen van wetenschap), art. 156 (onverwijld toekomen).
[132] *Kamerstukken II* 2016/17 34372, nr.6 p. 84.
[133] Aanwijzing opsporingsbevoegdheden https://wetten.overheid.nl/BWBR0035498/2014-09-01

onderzoekshandelingen en de processen-verbaal bevindingen met verwijzing naar artikel 21 lid 4 Bogw. De Inspectie heeft waargenomen dat het moment van ondertekenen tot wel 10 maanden na afloop van het bevel plaatsvindt.
- Evenals in 2021 de afgelegde verantwoording in enkele processen-verbaal op onderdelen niet geheel overeenkomt met de daadwerkelijke uitvoering. Zo blijkt op basis van systeemlogging dat bepaalde opsporingsambtenaren betrokken zijn geweest bij het uitvoeren van onderzoekshandelingen maar dat zij niet als verbalisant opgenomen zijn in het proces-verbaal;
- DIGIT door de DIGIT-officier van justitie geïnstrueerd is om in het belang van de afscherming van opsporingsmethodieken en -middelen minimaal te verbaliseren en maximaal te journaliseren. De Inspectie stelt vast dat evenals in 2021 de redenen van wetenschap in de processen-verbaal summier zijn vastgelegd.[134] Een juist en volledig journaal wordt daarmee van nog groter belang;
- De vastlegging in het journaal verbeterd is ten opzichte van 2021. De Inspectie ziet ontwikkeling in de detaillering en de structuur van het journaal. Desondanks ziet de Inspectie nog steeds voorbeelden dat het journaal een onjuiste of onvolledige weergave geeft van de uitgevoerde handelingen. Ook ontbreken soms registraties van handelingen en is de vastlegging niet in alle gevallen duidelijk. Evenals in 2021 blijkt namelijk dat het journaal niet in alle gevallen juist en volledig is wanneer dit wordt afgezet tegen de systeemlogging. De kwaliteit van de verantwoording in het journaal lijkt daarbij sterk af te hangen van de individuele opsporingsambtenaar. Dit heeft gevolgen voor de juistheid van de processen-verbaal omdat de processen-verbaal gebaseerd zijn op de informatie uit het journaal.

A.6 Bewerking en verstrekking van vastgelegde gegevens

De resultaten van het onderzoek worden door het technisch team ter beschikking gesteld aan het tactisch team belast met het opsporingsonderzoek. Uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier van justitie vallen, mogen ter beschikking worden gesteld aan het tactisch onderzoeksteam.[135] Het kan hierbij nodig zijn om gegevens te filteren zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen, uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactisch team. Het technisch team draagt in dat geval zorg voor de selectie van onderzoeksgegevens.[136] Het Besluit stelt dat bij het maken van een selectie van vastgelegde gegevens sprake is van een bewerking. Op grond van het Besluit moet deze bewerking plaatsvinden op basis van een forensische kopie van de vastgelegde gegevens op een technische infrastructuur. In het proces-verbaal legt de opsporingsambtenaar de bewerkingen vast die plaatsgevonden hebben op deze kopie. Deze regels zijn van belang omdat de gegevens die tijdens de onderzoeksfase worden vastgelegd, kunnen worden gebruikt als bewijs in een strafzaak. Gelet hierop dienen de betrouwbaarheid en integriteit van de gegevens

[134] De Hoge Raad heeft in zijn rapport over het onderzoek in het geautomatiseerde werk aanbevelingen gedaan het opmaken van een proces-verbaal tijdiger en volledi ger, dat wil zeggen: voorzien van meer concrete informatie, te doen plaatsvinden.
[135] *Kamerstukken II* 2016/17, 34372, nr.6, p.14 en p.27.
[136] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 17.

onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing.[137]

De Inspectie stelt vast dat in 2022 evenals in 2021 voor de Inspectie niet is vast te stellen welke gegevens precies zijn overgedragen aan de tactische teams, omdat hier niet altijd logging en verslaglegging van is. Reden hiervan is het feit dat een, schermopname-voorziening waarmee een deel van deze overdrachten tot op zekere hoogte inzichtelijk gemaakt kon worden, in 2022 niet correct heeft gefunctioneerd.

De Inspectie heeft gezien dat in 2022 het maken van een selectie van gegevens in één zaak heeft plaatsgevonden. Door de Inspectie is vastgesteld dat de selectie conform het Bogw met gebruikmaking van een forensische kopie is uitgevoerd. De selectie en uitgevoerde werkzaamheden zijn door de opsporingsambtenaar verantwoord in het proces-verbaal en zijn voor de Inspectie voldoende navolgbaar.

A.7 Bewaartermijnen, verwijdering en vernietiging gegevens

In de toelichting bij het Besluit is beschreven dat op grond van andere wettelijke bepalingen eisen gelden voor bewaartermijnen, het verwijderen en vernietigingen van verzamelde gegevens, waaronder specifieke regels omtrent geheimhouderinformatie.[138] Vanuit de kwaliteit van de taakuitvoering vloeit voort dat de politie haar processen, procedures en technische voorzieningen zodanig inricht en toepast dat op het moment dat de officier van justitie daartoe verzoekt, gegevens tijdig, juist en volledig worden vernietigd en verwijderd. Ook geldt hierbij dat deze gegevens juist en volledig bewaard en toegankelijk zijn en blijven gedurende de periode dat dat vereist wordt.

In haar verslag over 2021 heeft de Inspectie vermeld dat DIGIT het bevel heeft gekregen gegevens te vernietigen. Dit omdat een zaak uit 2019 was geëindigd en de betrokkene schriftelijk door de officier van justitie in kennis is gesteld[139] van het feit dat heimelijk is binnengedrongen in een geautomatiseerd werk en onderzoekshandelingen zijn verricht. De Inspectie stelt vast dat in 2022 het proces van vernietigen in deze zaak nog niet volledig is afgerond. Reden hiervoor is dat geruime tijd onduidelijk was, welke gegevens precies vernietigd moesten worden, waar deze gegevens zich bevonden en hoe de vernietiging plaats moest vinden. Deze situatie acht de Inspectie onwenselijk en dient dan ook te worden opgepakt.

Processen, procedures en technische voorzieningen

De Inspectie heeft in haar eerdere verslagen er ook op gewezen dat in wetgeving onderscheid gemaakt wordt tussen vernietiging en verwijdering van gegevens. Ook het bewaken van bijbehorende termijnen voor het verwijderen en vernietigen van gegevens is van belang, zodat juiste en volledige uitvoering kan worden gegeven aan het verwijderen en vernietigen van gegevens als dit volgens wetgeving vereist is. Hetzelfde geldt voor de zekerstelling dat gegevens juist en volledig bewaard en

[137] Art. 29 Bogw en nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 21 en 48.

[138] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.*, 2018, 340, p. 22.
[139] Via een notificatie zoals beschreven in artikel 126bb Sv.

toegankelijk zijn en blijven gedurende de periode dat dat vereist wordt. De Inspectie heeft in haar verslag 2021 aandacht gevraagd voor het uitwerken en oppakken van deze onderwerpen door de politie. De Inspectie constateert dat de politie ook in 2022 nog geen nadere uitwerking en invulling hieraan heeft gegeven. De politie heeft haar processen, procedures en technische voorzieningen nog niet zodanig ingericht en toegepast dat op het moment dat de officier van justitie daartoe verzoekt of als dit noodzakelijk is op grond van wetgeving, gegevens tijdig, juist en volledig worden verwijderd en vernietigd.

Geheimhouderinformatie

Op grond van artikel 126aa Sv en het Besluit bewaren en vernietigen niet-gevoegde stukken dienen gegevens die betrekking hebben op informatie tussen de verdachte en verschoningsgerechtigde te worden vernietigd. Bepaalde beroepsgroepen, zoals advocaten, artsen of notaris, vallen onder het verschoningsrecht (zogenaamde verschoningsgerechtigde of wel geheimhouder).[140] Indien gegevens zijn verzameld door het inzetten van de hackbevoegdheid en deze onder de geheimhoudingsplicht vallen, dienen de gegevens te worden vernietigd.[141] Het beschermen van dergelijke informatie heeft als doel: 'cliënten en andere belanghebbenden zekerheid te geven dat zij vrijelijk met [bijvoorbeeld] de advocaat kunnen spreken.'[142] [143] Uit jurisprudentie volgt dat deze gegevens onmiddellijk dienen te worden vernietigd, zodat is verzekerd dat de gegevens geen deel uitmaken van de processtukken en het verdere verloop van het strafproces, waaronder ook het eindonderzoek ter terechtzitting.[144]

De procedure voor de vernietiging van de vastgelegde gegevens is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.[145] Op grond van dit besluit dient de opsporingsambtenaar onverwijld de officier van justitie in kennis te stellen als hij weet of redelijkerwijs kan vermoeden dat mededelingen zijn gedaan door een geheimhouder. De officier van justitie beoordeelt vervolgens of de gegevens vernietigd dienen te worden. Indien dit het geval is, wordt een schriftelijk bevel afgegeven en wordt van de vernietiging een proces-verbaal opgemaakt. Ook kan op grond van het besluit de officier van justitie bij voorbaat een generiek bevel tot vernietiging aan de opsporingsambtenaar verstrekken. Communicatie die in aanmerking komt hiervoor kan hierdoor terstond worden vernietigd zonder tussenkomst van de officier. Daarnaast is in 2011 het systeem van nummerherkenning opgenomen in het Besluit bewaren en vernietigen niet-gevoegde stukken. Indien een advocaat gebruik maakt van een nummer dat overeenkomstig de regeling is aangemeld, wordt dit nummer door middel van een geautomatiseerd systeem herkend. Het opnemen van de communicatie wordt automatisch beëindigd en mogelijk opgenomen communicatie wordt onmiddellijk vernietigd. Deze werkwijze is ook van toepassing op de hackbevoegdheid als sprake is van het aftappen van telecommunicatie.[146] In de nota van toelichting horende bij

[140] Artikel 218 en 218a Sv.
[141] *Kamerstukken II* 2015/16, 34372 nr. 3, p.17.
[142] Zie onder andere HR 1 maart 1985, ECLI:NL:HR:1985:AC9066 en Gerechtshof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329, r.o. 3.6.1.
[143] Het verschoningsrecht is geen absoluut recht. In zeer uitzonderlijke omstandigheden kan het belang dat de waarheid aan het licht komt, prevaleren boven het verschoningsrecht (vlg. HR 2 maart 2010, ECLI:NL:HR:BJ9262)
[144] Zie onder andere HR 12 januari 1999, LJN ZD1402, NJ 1999, 290 en ECLI:NL:HR:2007:BA5632
[145] Art.4 eerste en tweede lid. Besluit bewaren en vernietigen niet-gevoegde stukken.
[146] *Kamerstukken II 2016/16*, 34372 nr. 3 p. 18.

de wijziging van het besluit in 2011 is door de wetgever beschreven dat de kring van geheimhouders groter is dan alleen advocaten. Ook andere beroepsgroepen, zoals artsen en notarissen, kunnen een beroep doen op het wettelijk verschoningsrecht. Dit betekent dat de politie alert zal moeten blijven op het signaleren van communicatie van verschoningsgerechtigden die voor vernietiging in aanmerking komt.[147] Hierbij is tevens beschreven dat maatregelen, zoals de ontwikkeling van de scantool en de vereenvoudiging van de werkinstructies, daaraan een belangrijke bijdrage kunnen leveren.[148]

In de toelichting op het Besluit bewaren en vernietigen niet-gevoegde stukken wordt ingegaan op het begrip 'vernietigen'. Zo is beschreven dat indien het mogelijk is de gegevensdrager te behouden onder het vernietigen van de gegevens mede wordt verstaan het zodanig bewerken van die gegevensdrager, dat van de gegevens die daarop stonden geen kennis meer kan worden genomen. Dit betekent dat het simpelweg wissen van bestanden op een diskette niet voldoende is, maar de gegevensdrager bijvoorbeeld dient te worden geformatteerd.[149] Ook is op grond van artikel 5 van het besluit bepaald dat het zodanig bewerken van gegevens dat deze niet meer kenbaar zijn, gelijk staan aan vernietigen.[150]

Herkennen van geheimhouderinformatie
De Inspectie constateert dat de DIGIT-officier van justitie door DIGIT onverwijld in kennis gesteld wordt indien de opsporingsambtenaren van DIGIT bij toeval kennisnemen van de aanwezigheid van mogelijke geheimhouderinformatie. Er zijn echter aan de kant van DIGIT geen processen, werkinstructies en ondersteunende systemen zoals nummerherkenning ingericht om geheimhouderinformatie te herkennen. De door DIGIT vastgelegde gegevens, worden als geheel - dus inclusief mogelijke geheimhouderinformatie – overgedragen.[151]

Door de gegevens in zijn geheel over te dragen uit de afgeschermde omgeving van DIGIT, wordt het risico vergroot dat dergelijke gegevens in de processtukken terecht kunnen komen. Ook verhoogt deze werkwijze het risico dat de kring van personen die mogelijk kennis kunnen nemen van geheimhouderinformatie onnodig wordt vergroot. Het is dan ook aan te bevelen dat DIGIT zich inspant waarborgen, waaronder nummerherkenning, in te richten om geheimhouderinformatie in een vroeg stadium te kunnen herkennen. Hiermee wordt uitdrukkelijk geen inhoudelijk toets bedoeld, maar slechts een technische filtering.

Een dergelijke werkwijze sluit ook aan bij het Besluit onderzoek in een geautomatiseerd werk waarin staat beschreven dat het technische team zorgdraagt voor de selectie van onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team.[152] Bij de selectie van gegevens dient op grond van het besluit

[147] *Stb* 2011, 380, pagina 6.
[148] De scantool traceert geheimhoudergesprekken door de uitgewerkte gesprekken te vergelijken met een bestand van telefoonnummers van mogelijke geheimhouders en een bestand van (deel)woorden die verwijzen naar een mogelijk geheimhoudergesprek (woordenlijst). Dit was in 2011 nog in ontwikkeling.
[149] *Stb* 1999, 548, pagina 10.
[150] Artikel 5 Besluit bewaren en vernietigen niet-gevoegde stukken.
[151] In Inspectie heeft geen onderzoek gedaan naar de omgang met geheimhouderinformatie na de overdracht van de gegevens door DIGIT en heeft dan ook geen bevindingen over dit deel van het proces.
[152] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 17.

gebruik te worden gemaakt van een forensische kopie van de ter uitvoering van het bevel vastgelegde gegevens. Het technische team dient dan vast te leggen welke bewerkingen hebben plaatsgevonden met betrekking tot de op de forensische kopie vastgelegde gegevens.[153] Ook kan hiermee vooruit worden gelopen op het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering waarin een werkwijze wordt beschreven waarbij gegevens die mogelijk toebehoren aan een verschoningsgerechtigde worden uitgefilterd.[154]

Daarnaast stelt de Inspectie vast dat gegevens, ook na de onderkenning als geheimhouderinformatie, bij DIGIT beschikbaar zijn en blijven. Geheimhouderinformatie wordt niet vernietigd in de systemen van DIGIT. Reden hiervoor is dat de officier van justitie geen bevel tot vernietiging af heeft gegeven aan DIGIT om de gegevens te vernietigen. Door de DIGIT-officier van justitie is gemotiveerd dat sprake is van tegenstrijdige regelgeving waarbij het vernietigen van gegevens door DIGIT niet in overeenstemming is met het Besluit Onderzoek in een geautomatiseerd werk. In dit besluit wordt geregeld dat gegevens die zijn vastgelegd in de technische infrastructuur niet gewijzigd mogen worden. Dit resulteert in een werkwijze waarbij geheimhouderinformatie nog beschikbaar blijft binnen de politie. De Inspectie verbindt hieraan echter geen waardeoordeel gelet op het feit dat de politie hier handelt op aangeven van het OM en de Inspectie geen toezicht houdt op het openbaar ministerie. De Inspectie signaleert echter wel een praktijk die niet in overeenstemming is met artikel 126aa Sv.

A.8 Informatiebeveiliging, kwaliteitssysteem en interne controle

De betrouwbaarheid, integriteit en herleidbaarheid van gegevens is cruciaal voor het gebruik van de verkregen gegevens als bewijs in een strafzaak. Volgens het Besluit dienen hiertoe maatregelen getroffen te worden om onbevoegde kennisname en het wijzigen van deze gegevens te voorkomen en om achteraf te kunnen vaststellen of hiervan sprake was. Op de politie zijn wettelijke regelingen[155] van toepassing die aanknopingspunten bieden voor een nadere invulling van deze maatregelen. De politie dient op basis hiervan te komen tot een samenhangend geheel van te treffen beheersingsmaatregelen die zijn afgestemd op de risico's.

Tijdens de parlementaire behandeling van het wetsvoorstel van de wet CCIII is door de toenmalig staatssecretaris van Veiligheid en Justitie aangegeven dat de politie haar eigen geautomatiseerde omgeving zo veilig mogelijk zal inrichten en de gebruikte systemen voortdurend zal beschermen en bewaken tegen mogelijke aanvallen van buiten.

De beheersing van beveiligingsrisico's is van belang om te waarborgen dat passende beheersingsmaatregelen voor de betrouwbaarheid en integriteit van de logging en de technische infrastructuur getroffen worden en zijn. Dit vormt de basis

[153] Artikel 29 Besluit onderzoek in een geautomatiseerd werk.
[154] Memorie van toelichting bij het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, ambtelijke versie, juli 2020, v.a. pagina 532.
[155] Regeling Informatiebeveiliging Politie (RIP, https://wetten.overheid.nl/BWBR0008599/2017-12-15 en Wet politiegegevens (Wpg, https://wetten.overheid.nl/BWBR0022463/2020-01-01).). Tevens heeft de politie zich gecommitteerd aan de Baseline Informatiebeveiliging Overheid (BIO) en zijn in een addendum per rubriceringsniveau door de politie specifiek te treffen maatregelen vastgesteld (BIO+)

om door de politie vanuit een interne verantwoordelijkheid toe te zien op het inrichten van deze maatregelen, de structurele naleving daarvan en daarover op een controleerbare wijze verantwoording af te kunnen leggen. De Inspectie ziet hierop toe vanuit haar toezicht op de kwaliteit van de taakuitvoering door de politie.[156]

De Inspectie heeft in haar eerdere verslagen gerapporteerd dat DIGIT de eerste stappen had gezet om te komen tot een aantoonbaar en controleerbaar passend beveiligingsniveau. In 2021 constateerde de Inspectie dat er geen vooruitgang geboekt was in de benodigde doorontwikkeling en vervolgstappen. De minister heeft in haar beleidsreactie op het verslag van de Inspectie over de toepassing van de hackbevoegdheid in 2021 toegezegd dat de aanpak van informatiebeveiliging geïntensiveerd wordt.[157]

Ook in 2022 stelt de Inspectie vast dat de voortgang voor het planmatig aantoonbaar en controleerbaar op niveau brengen en houden van beheersingsmaatregelen stagneert. Dit betekent dat evenals voorgaande jaren, ook in 2022, DIGIT onvoldoende in staat is te controleren of haar processen en systemen voldoen aan de door de politie gestelde beveiligingseisen. De politie heeft evenals in 2021 nog geen samenhangend pakket van te treffen beheersings- en beveiligingsmaatregelen vastgesteld. Ook de borging en effectuering van maatregelen voor het voortdurend beschermen en bewaken tegen mogelijke aanvallen van buitenaf en een controleerbare verantwoording daarover moet hiervan onderdeel vormen. Op specifieke onderdelen zijn er door DIGIT in 2022 enkele technische maatregelen doorgevoerd. Deze maatregelen zijn nog niet in alle gevallen volledig en juist doorgevoerd.

DIGIT vertrouwt voor het beperken van het risico voor ongeautoriseerde toegang mede op maatregelen waarmee de fysieke toegang tot haar locatie wordt beperkt. In 2022 is het echter niet mogelijk gebleken inzicht te krijgen in de uitgegeven autorisaties voor deze fysieke toegang. Het vastleggen van de uitgangspunten, het hebben van inzicht en het periodiek (laten) uitvoeren van controles over de juistheid van deze autorisaties kan een belangrijke bijdrage leveren aan het aantoonbaar beperken van het risico voor onbevoegde toegang en kennisname.

Om eventuele risico's in perspectief te kunnen plaatsen, heeft de Inspectie ook zelf gekeken naar de implementatie van enkele maatregelen waaronder de inrichting van logische toegangsbeveiliging. Hoewel het autorisatiebeheer ook in 2022 nog steeds niet op orde is, heeft de Inspectie op basis van haar waarnemingen geen aanwijzingen dat zich grote technische beveiligingsrisico's in de technische infrastructuur van DIGIT hebben voorgedaan.

De Inspectie stelt vast dat DIGIT in 2022 geen aantoonbare verantwoording kon overleggen over de inrichting van beveiligingsmaatregelen en het functioneren daarvan. Om te kunnen komen tot passende maatregelen is het van belang dat door de politie volgens een vastgestelde methodiek en door toepassing van

[156] Art. 65 Politiewet 2012.
[157] Kamerbrief met 1e halfjaarbericht 2022 politie, bijlage moties toezeggingen en aanvullende zaken, 17 juni 2022. https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/17/tk-eerste-halfjaarbericht-2022

risicomanagement gekomen wordt tot een samenhangend geheel van te treffen beheersingsmaatregelen. Aan de hand van een plan moeten deze beheersingsmaatregelen vervolgens worden geïmplementeerd, dient regelmatig gecontroleerd te worden of deze maatregelen juist zijn toegepast en dient eventuele bijstelling plaats te vinden bij verandering van betrouwbaarheidseisen of risico's. Samenvattend betreft het hier het opzetten en effectueren van kwaliteitszorg gericht op informatiebeveiliging door middel van een plan-do-check-act-cyclus (PDCA). De politie moet daaraan invulling geven gelet op (wettelijke) regelingen.[158] Ook voor het effectief kunnen uitoefenen van systeemtoezicht moet de Inspectie kunnen steunen op de opbrengsten van een dergelijke kwaliteitsborging. De Inspectie kan door het ontbreken hiervan ook in 2022 voor haar toezicht niet steunen op een intern beheersingsmechanisme ten aanzien van informatiebeveiliging. Deze constatering heeft raakvlakken met het volgende onderwerp: de kwaliteitszorg en de interne controle.

Kwaliteitszorg en interne controle

De Inspectie houdt toezicht op de kwaliteit van de taakuitvoering door de politie.[159] Interne kwaliteitszorg waaronder een eigen interne controle is een belangrijk onderdeel voor het borgen van deze kwaliteit. In de nota van toelichting bij het Bogw is aangegeven dat de Inspectie systeemtoezicht uitoefent, hetgeen een vorm van interne controle of interne borging binnen de politie veronderstelt. Interne controle is als instrument onderdeel van de kwaliteitszorg waarmee de politie zelf de kwaliteit van de inzet van de bevoegdheid tijdens alle fasen van de uitvoering kan borgen en eventuele tekortkomingen hierin tijdig zelf kan identificeren en verhelpen. Dit sluit aan op de beantwoording van vragen tijdens de wetsbehandeling van de Wet CCIII waarin is aangegeven dat tijdens de uitvoering van het bevel tot het op afstand binnendringen van een geautomatiseerd werk toezicht uitgeoefend wordt door de leidinggevende functionarissen binnen de opsporingsdienst.[160] Hierbij kan bijvoorbeeld gedacht worden aan controles ten aanzien van de kwaliteit van het journaal, haalbaarheidsonderzoeken, processen-verbaal, volledigheid van logging en het adequaat functioneren van voorzieningen voor het doorlopend en automatisch vastleggen van handelingen. Dit is van belang voor een rechtmatige toepassing van de bevoegdheid door de politie.

In haar verslag over 2020 constateerde de Inspectie al dat de politie niet beschikte over een goed functionerend 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. Ook heeft de Inspectie in haar verslag over 2020 vermeld dat de politie soms fouten en hiaten in de verslaglegging niet zelf opmerkte en dat zij onvoldoende toeziet op de kwaliteit van documenten. In het verslag over 2021 heeft de Inspectie vermeld dat zij in de loop van 2021 een aantal verbeteringen constateerde en de positieve effecten daarvan op de kwaliteit in de dagelijkse praktijk heeft gezien.

---

[158] Zie hiertoe bijvoorbeeld de Regeling Informatiebeveiliging Politie (RIP), artikel 2, tweede lid en artikel 6. https://wetten.overheid.nl/BWBR0008599/2017-12-15

[159] Art. 65 Politiewet 2012.

[160] *Kamerstukken II* 2016/17, 34372, nr.6, p.59.

De Inspectie stelt vast dat de ontwikkeling en toegezegde inbedding van kwaliteitszorg en de bijbehorende interne controle van het operationele proces stagneert. In 2022 zijn kleine stapjes gezet ter verbetering van de kwaliteitszorg en interne controle. Er blijft echter sprake van een versnipperde aanpak en inrichting op deze onderwerpen. De Inspectie heeft bijvoorbeeld geconstateerd dat het tijdens inzetten de bedoeling was een bepaalde beheersingsmaatregel te treffen waarmee een onjuiste uitvoering voorkomen kan worden. In de praktijk heeft de Inspectie echter vastgesteld dat deze maatregel in een aantal gevallen onjuist werd toegepast en dat een eigen interne controle op juiste toepassing daarvan ontbrak.

Overeenkomstig haar bevindingen in 2021 constateert de Inspectie dat de politie nog niet in beeld heeft gebracht voor welke onderdelen van de belangrijkste (werk)processen kwaliteitsbewaking en interne controle moet worden ingericht. Een overkoepelende visie waarin deze activiteiten in samenhang gebracht zijn en welke instrumenten daartoe door wie, wanneer moeten worden ingezet, is nog niet gereed. Ook is niet bepaald wie welke taken en verantwoordelijkheden hierin heeft en hoe en aan wie verantwoording wordt afgelegd. Tevens ontbreekt documentatie om de kwaliteit van de taakuitvoering te borgen en te voorkomen dat dit uitsluitend rust op de professionele inschatting van individuele medewerkers. Hierdoor ontbreekt structurele borging. DIGIT geeft aan dat in 2022 het team nog bezig was met het uitwerken en vastleggen van de beoogde kwaliteitszorg waaronder de interne controles. De Inspectie heeft hiervan echter nog geen concrete uitwerkingen op papier van gezien.

Bijlage B: Onderzoeksmethodiek

In deze bijlage wordt de opzet en de gehanteerde methodiek beschreven die is gehanteerd voor het toezicht op de hackbevoegdheid.

Afbakening en aanpak onderzoek

De Inspectie stelt jaarlijks een rapport op waarin zij verslag doet van het toezicht op de uitvoering van de bevoegdheid tot het onderzoek in een geautomatiseerd werk. Met dit verslag rapporteert de Inspectie over de uitvoering van de hackbevoegdheid door de politie over de periode 1 januari 2022 tot en met 31 december 2022.

Conform de nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk (hierna: het Besluit) houdt de Inspectie toezicht op de naleving van de regels die van toepassing zijn op de hackbevoegdheid. Ook is aangegeven dat de Inspectie systeemtoezicht[161] uitoefent, hetgeen een vorm van kwaliteitszorg en interne controle binnen de politie veronderstelt.[162] Tevens heeft de Inspectie telkens aangegeven dat de bevindingen van de Inspectie in haar verslagen als input kunnen dienen voor de evaluatie van de Wet CCIII waarvan bekend was dat deze twee jaar na inwerkingtreding van de hackbevoegdheid geëvalueerd zou worden door het WODC.[163]

Binnen deze context heeft de Inspectie haar toezicht op de hackbevoegdheid vormgegeven en uitgevoerd. Ze geeft daarmee uitvoering aan de nadrukkelijke wens van de wetgever om, gezien de belangen die ermee gemoeid zijn (enerzijds de effectiviteit van de opsporing en anderzijds het zoveel mogelijk beperken van de inbreuk op de privacy van de betrokkenen) op alle aan haar gevraagde aspecten van de uitgebreide regelgeving toe te zien.

Technisch team politie

Het toezicht door de Inspectie is gericht op het functioneren van het wettelijk systeem rond het toepassen van de hackbevoegdheid door de politie.[164] De

[161] "Systeemtoezicht of systeemgericht toezicht is het toezicht door de overheid dat gebruikmaakt van zelfregulerende systemen binnen organisaties of branches. 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. Dit wordt gedaan door audit achtige onderzoeken met reality checks uit te voeren, waarbij gebruik wordt gemaakt van de interne borgingssystemen binnen organisaties of sectoren", aldus (onder meer) het lemma 'systeemtoezicht' (onderdeel Rijksoverheid, begrippenkader rijksinspecties) in de Eerste Nederlandse Systematisch Ingerichte Encyclopaedie (E.N.S.I.E.), elektronische versie (bijgewerkt tot 2018). Zie bovendien: J. Helderman & M.E. Honingh, Systeemtoezicht. Een onderzoek naar de condities en werking van systeemtoezicht in zes sectoren, Den Haag: WODC 2009.

[162] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 24.

[163] Het WODC heeft in september 2022 gerapporteerd over de evaluatie van het proces rondom de uitvoering van de hackbevoegdheid in de eerste twee jaar na inwerkingtreding van de Wet CCIII. (Zie https://www.wodc.nl/actueel/nieuws/2022/09/19/knelpunten-in-uitvoering-van-hackbevoegdheid-door-politie). Op het moment van schrijven van het Inspectie verslag over 2022 is de beleidsreactie van de minister op het WODC rapport nog niet beschikbaar.

[164] *Kamerstukken II* 2016/17, 34372, nr.6, p. 106. Het systeemtoezicht wordt uitgeoefend op de uitvoering van de wettelijke regels in de praktijk; Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 23.

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.[165] Naast politieambtenaren kunnen opsporingsambtenaren van de Koninklijke Marechaussee en opsporingsambtenaren van de bijzondere opsporingsdiensten onderdeel vormen van dit team. Het toezicht door de Inspectie richt zich dan ook op de uitvoering van de hackbevoegdheid door dit team.

Keuring technische hulpmiddelen

De Inspectie houdt tevens toezicht op de naleving van de regels en procedures voor de keuring en inzet van software waarmee op apparaten gegevens worden verzameld.[166] De beoordeling of deze software voldoet aan de eisen wordt uitgevoerd door een keuringsdienst. De minister heeft de keuringsdienst van de Landelijke Eenheid hiervoor aangewezen. De Inspectie houdt toezicht op de uitvoering van de keuring door deze keuringsdienst.

Aanpak

Voor dit onderzoek kijkt de Inspectie of zij voor het uitoefenen van haar systeemtoezicht kan steunen op de opbrengsten van een kwaliteitssysteem en door de politie uitgevoerde (interne) controles. Met de aanwezigheid van een dergelijke systematiek en de resultaten daarvan kan de politie zelf de kwaliteit van de inzet van de bevoegdheid tijdens alle fasen van de uitvoering aantoonbaar borgen. Tevens is de politie daarmee in staat op controleerbare wijze te verantwoorden dat ondersteunende (ICT)-processen aantoonbaar juist ingericht en effectief zijn. Als deze interne beheersingsmechanismen onvoldoende aanwezig zijn, zal de Inspectie om toch een beeld te kunnen verschaffen, zelf op onderdelen aanvullend onderzoek moeten doen. Dit heeft de Inspectie bijvoorbeeld gedaan door zelf controles uit te voeren van het autorisatiebeheer.

De Inspectie is per inzet van de hackbevoegdheid door DIGIT nagegaan of de politie gewerkt heeft binnen de reikwijdte van de afgegeven bevelen en zich daarbij gehouden heeft aan de gestelde regels. Bij het nagaan of de politie de verrichte handelingen juist en volledig heeft uitgevoerd en verantwoord, reconstrueert de Inspectie de aanpak en uitvoering per inzet van de hackbevoegdheid op basis van beschikbare logging, documentatie en interviews. Ter ondersteuning van de reconstructie en analyse activiteiten maakt de Inspectie gebruik van eigen ontwikkelde tools.

Verder verricht de Inspectie onderzoek naar de uitgevoerde keuringen van technische hulpmiddelen en diverse generieke aspecten, zoals de logging en de beveiliging van de technische infrastructuur van DIGIT. Bij de keuringsdienst heeft de Inspectie na afloop van elke uitgevoerde keuring een dossieronderzoek uitgevoerd en zijn gesprekken gevoerd met de keuringsdienst. Voor het beoordelen van de generieke aspecten heeft de Inspectie inrichtingsdocumentatie en

---

[165] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 14.; Art. 1 sub h Bogw: definitie technisch team: Onderdeel van de Landelijke Eenheid dat kan worden belast met de uitvoering van een bevel.

[166] Nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb*., 2018, 340, p. 20 en 37. "*De Inspectie JenV houdt toezicht op de naleving van de technische eisen en de keuringsprocedure*."; *Kamerstukken I,* 2017/18, 34372, nr. G, p. 14 (nadere memorie van antwoord).

systeeminstellingen opgevraagd en beoordeeld. Ook zijn gedurende het jaar diverse gesprekken gevoerd met functionarissen van DIGIT.

Toetsingskader

De Inspectie hanteert voor haar toezicht op de toepassing van de hackbevoegdheid een toetsingskader. Dit kader is gebaseerd op het toepasselijke rechtskader, waarvan de kern wordt gevormd door het Wetboek van Strafvordering en het Besluit. Voor de nadere duiding van de hierin opgenomen regels en hun bedoeling heeft de Inspectie gebruik gemaakt van toelichtingen en verslagen naar aanleiding van de parlementaire behandeling.

Bij het toezicht op de kwaliteit van de taakuitvoering[167] door de politie betrekt de Inspectie de voor de politie geldende regels, inclusief de randvoorwaarden die nodig zijn om daaraan te kunnen voldoen. Een juiste, tijdige, volledige, aantoonbare en controleerbare uitvoering van de bevoegdheid en het daarover door middel van eigen controles kunnen afleggen van verantwoording zijn belangrijke kwaliteitsaspecten.

In bijlage A van het verslag zijn in de blauw gearceerde kaders kort de gehanteerde regels en uitgangspunten benoemd. Het toetsingskader dat als leidraad door de Inspectie is gehanteerd voor haar toezicht is terug te vinden op de website van de Inspectie.[168]

Relatie met het Openbaar Ministerie

De Inspectie toetst de uitvoering van de bevoegdheid aan de wettelijke regels en voorschriften, aan het bevel en de machtiging van de rechter-commissaris. Zij toetst hiermee de rechtmatigheid. Dit met dien verstande dat het begrip «rechtmatigheid» dan betrekking heeft op een rechtmatige toepassing.[169] Het toezicht van de Inspectie is beperkt tot de uitvoering van de hackbevoegdheid door het technisch team. De Inspectie toetst niet het door de officier van justitie afgegeven bevel. Dit is aan de rechter-commissaris. Ook oordeelt de Inspectie niet over het handelen van de officier van justitie. De concrete inzet wordt op rechtmatigheid getoetst tijdens de zitting door de rechter.

De zaaksofficier van justitie heeft de leiding en de eindverantwoordelijkheid over het opsporingsonderzoek waarin de hackbevoegdheid wordt ingezet.[170] De landelijk officier van justitie voor Digital Intrusion (hierna: DIGIT-officier van justitie) heeft de leiding over en is verantwoordelijk voor de uitvoering van het bevel door het technisch team.[171] De officier van justitie kan aanwijzingen geven aan de politie.[172] Indien de Inspectie constateert dat de politie afwijkt van de aan haar gestelde regels, gaat de Inspectie na of dit op aanwijzing van de officier van justitie is gebeurd. Het oordelen over het handelen van de officier van justitie valt buiten de toezichtbevoegdheid van de Inspectie.

---

[167] Art. 65 lid 1 Politiewet 2012.
[168] Zie https://www.inspectie-jenv.nl/Publicaties/toetsingskaders/2022/07/12/toetsingskader-hackbevoegdheid-2022
[169] *Kamerstukken I*, 2017/18, 34372, nr. G, p.21
[170] Artt. 132a en 148 Sv.
[171] Instructie voor de inzet van de bevoegdheid ex. artt. 126nba, 126uba, 126zpa en 126ffa Sv (2021I002)
[172] Art. 12 lid 2 Politiewet 2012.

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.[173] De Inspectie heeft in 2022 geen melding hoeven doen van mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie.

Indien de Inspectie constateert dat de politie regels schendt rond de bescherming van persoonsgegevens, kan zij de Autoriteit Persoonsgegevens (AP) informeren.[174] De Inspectie heeft in 2022 geen dergelijke melding hoeven doen bij de AP.

[173] *Kamerstukken II* 2016/17, 34372, nr.6, p. 83.
[174] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 83.

Bijlage C: 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	Het Openbaar Ministerie
PG-HR	Procureur-generaal bij de Hoge Raad der Nederlanden
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Bijlage D: Hoor- en wederhoortabel

Nr.	Inzagepartij	Hoofdstuk/ paragraaf	Te corrigeren tekst (eerste…laatste woord)	Argumentatie/onderbouwing van uw reactie	Reactie Inspecties
1	Politie: Digit	Inhoudsopgave		In het verslag wordt nergens verwezen naar het bestaan van de wederhoortabel. De wederhoortabel zou als bijlage C opgenomen kunnen worden. In de inhoudsopgave zou hier naar kunnen worden verwezen.	Overgenomen. De wederhoortabel is opgenomen als bijlage in het rapport. De wederhoortabel wordt in het kader van de navolgbaarheid en transparantie samen met het verslag aangeboden en gepubliceerd. Een verwijzing naar de aanwezigheid van deze tabel als bijlage is in de inhoudsopgave opgenomen.
2	Politie: Digit	Hoofstuk 2, paragraaf 2.2.1, eerste alinea, p. 11	De…gevallen.	In de parlementaire geschiedenis wordt gesproken over uiterste gevallen en niet uitzonderlijke gevallen. Zie kamerstukken II, 2016–2017, 34 372, nr. 23 en p. 15 van de Nota van Toelichting bij het Bogw. Daarnaast wordt in de huidige tekst onvoldoende tot uitdrukking gebracht dat de inzet van commerciële binnendringsoftware steeds per zaak wordt getoetst. Deze toetsing wordt in eerste instantie gedaan door de politie en de landelijk officier voor *digital intrusion* en daarna door het Centrale Toetsings Commissie van het Openbaar Ministerie.	Overgenomen. Per abuis is de inzet van commerciële software in 'uiterste gevallen' en de 'uitzonderingsgevallen' van het achterwege blijven van de keuring met elkaar gemengd. De paragraaf is aangepast. Aangevuld is dat de uiteindelijke besluitvorming over de inzet van commerciële binnendringsoftware in een zaak bij het OM ligt.
3	Politie: Digit	Hoofstuk 2, paragraaf 2.2.1,tweede alinea, p. 12	Dit…uitgangspunt.	Met deze zin wordt de suggestie gewekt dat dit van toepassing is op alle inzetten van de bevoegdheid ex art. 126nba Sv. Dit is niet het geval. Het in deze paragaaf beschreven gebruik van een niet-vooraf gekeurd technisch hulpmiddel geldt alleen voor een specifieke categorie inzetten. Voor deze categorie inzetten	Overgenomen. Alhoewel er al aangegeven was dat het om het merendeel van de zaken ging en dus niet alle inzetten, is expliciet gemaakt dat het hier gaat om de zaken waarbij sprake is van inzetten op een mobiele telefoon (de betreffende specifieke categorie). Dat commerciële software wordt gebruikt in

				is geen vooraf goedgekeurd technisch hulpmiddel beschikbaar.	dergelijke zaken is reeds openbaar gemaakt in het WODC-rapport. Voor deze software is door het OM bepaald dat het een naar zijn aard niet te keuren hulpmiddel betreft. Dit maakt dat zoals de politie in haar reactie aangeeft dat bij deze categorie van inzetten sprake is van standaardpraktijk waarbij wordt gewerkt met een niet goedgekeurd technisch hulpmiddel. Deze categorie van inzetten betreft het merendeel van de zaken in 2022. Dit is door de Inspectie ook verduidelijkt in het algemeen beeld.
4	Politie: Digit	Hoofstuk 2, paragraaf 2.2.2, eerste alinea, p. 13	Daarbij…onregelmatigheden.	De wijze waarop dit wordt geformuleerd impliceert dat het hier gaat om een verplichting die voortvloeit uit het rechtskader. Dat is niet het geval.	De formulering is aangepast. Er is verduidelijkt dat het uitwerken van gebruikssituaties een randvoorwaarde is om effectief invulling te geven aan de vereisten uit het besluit dat onregelmatigheden moeten kunnen worden vastgesteld op basis van logging. Als niet gedefinieerd is welke gebeurtenissen als een onregelmatigheid beschouwd worden, bestaat het risico dat het optreden daarvan niet gesignaleerd wordt omdat de inrichting van logging daarin niet voorziet. Zie tevens reactie #25.
5	Politie: Digit	Hoofstuk 2, paragraaf 2.2.2, tweede alinea, p. 13	Ook…logbestanden.	De wijze waarop deze zin is geformuleerd impliceert dat er geen doorlopende en automatische vastlegging van gegevens in logbestanden plaatsvindt. Dat is niet het geval. Door de politie worden wel doorlopend en automatisch gegevens vastgelegd in logbestanden.	De formulering in deze paragraaf is aangescherpt. Deze paragraaf betreft de bevinding dat de doorlopende en automatische logging vooral is ingericht op basis van wat technisch standaard voorhanden is. De logging zou echter moeten worden ingericht op basis wat aan de hand van een risicoanalyse nodig is en wat volgt als vereiste uit het Besluit. Het

					risico bestaat dat de aanwezige doorlopende en automatische logging onvoldoende voorziet en effectief is gelet op het doel en gebruik van de logging. Zie tevens reactie bij #4.
6	Politie: Digit	Hoofdstuk 2, paragraaf 2.2.4, vijfde alinea, p. 15	Het…kennisname.	Deze zin impliceert dat het risico van het verkrijgen van fysieke toegang gelijk staat aan kennisname van potentiële gevoelige informatie. Dit is niet zondermeer het geval.	Beperkte aanpassing. De zin waarop de reactie van de politie betrekking heeft, is losgekoppeld van de passage over de autorisaties voor fysieke toegang. Daarmee wordt benadrukt dat het autorisatie- en toegangsbeheer betrekking heeft op zowel logische als fysieke toegangsbeveiliging. Op basis van een risicoanalyse zal DIGIT moeten vaststellen welke maatregelen in samenhang getroffen moeten worden om dit risico te beperken. Het inrichten en effectueren van autorisatie- en toegangsbeheer op het gebied van logische- en fysieke toegang zijn basismaatregelen.
7	Politie: Digit	Hoofdstuk 3, p. 18	Tekst in het kader.	De stelligheid van de huidige tekst doet geen recht aan de inspanning en vooruitgang die door de politie is bewerkstelligd. In dit domein heeft de wetgever zaken op basis van een theoretisch kader minutieus geregeld. Daarbij zijn onderdelen van geformuleerde rechtsregels soms contrair. Door zowel het WODC als de PG bij de Hoge Raad wordt dit beschreven. Evenals dat de ervaringen in de uitvoeringspraktijk soms vragen om andere oplossingen die evengoed recht doen aan de uitgangspunten die de wetgever heeft gehanteerd en daarmee rechtmatig zijn.	In het verslag wordt geconcludeerd dat veel van onze bevindingen over 2022 gelijk zijn aan de bevindingen waarover is gerapporteerd in de eerdere drie verslagjaren. In het eerste verslagjaar heeft de Inspectie begrip getoond dat het voor de politie een nieuwe bevoegdheid betrof en dat het technisch team van de politie in opbouw was. In de jaren daarna is het uitblijven van verbeteringen als risico benoemd. Over de onderwerpen die onderdeel maken van de conclusie is ieder jaar gerapporteerd. Het op orde brengen van de logging, de kwaliteitszorg, interne controle en het aantoonbaar op niveau brengen van informatiebeveiliging zijn als vast agendapunt

					in elk overleg met DIGIT besproken. Hiervan is telkens door DIGIT bevestigd dat door een andere prioriteitstellingen mede gelet op capaciteitsgebrek er onvoldoende invulling en opvolging aan deze verbeterpunten is gegeven. De Inspectie concludeert dan ook dat op deze onderwerpen onvoldoende vooruitgang in het verbeteren is geboekt. In de passage is toegevoegd dat hiervan sprake is ondanks de inspanning die daartoe door DIGIT geleverd is. Daarnaast werkt de wederhoorreactie de indruk dat bij deze onderwerpen sprake is van andere geïmplementeerde oplossingen die eveneens recht doen aan de door de wetgever gestelde uitgangspunten. Hiervan is naar oordeel van de Inspectie op de hiervoor benoemde onderwerpen geen sprake. Daar waar het de inzet van commerciële software betreft, is door ons spanning met de praktijk gesignaleerd. Met betrekking tot de contraire rechtsregels: in de bevindingen is aandacht gegeven aan deze constateringen in relatie tot het vernietigen van gegevens. Het feit dat deze rechtsregels door zowel het WODC als de PG als contrair worden beschreven, laat echter onverlet dat de basis van de systemen in orde moeten zijn. Dit betekent bijvoorbeeld dat de instructies, beleid en systemen zodanig zijn ingericht dat alleen noodzakelijke gegevens kunnen worden overgedragen en indien het nodig wordt geacht gegevens te verwijderen, dat dit ook snel uitvoerbaar is. Dit is verwerkt naar aanleiding van de wederhoorreactie #12 en #13.

					Het toezicht van de Inspectie ziet, zoals door de wetgever gevraagd, toe op de naleving van de door de wetgever gestelde regels en uitgangspunten. Zolang deze regels ongewijzigd blijven, is het geldende rechtskader hetgeen waar de Inspectie aan dient te toetsen.
8	Politie: Digit	Hoofdstuk 3, laatste alinea, p. 18	Tevens…kwetsbaar heden.	In de parlementaire geschiedenis wordt gesproken over uiterste gevallen en niet uitzonderlijke gevallen. Zie kamerstukken II, 2016–2017, 34 372, nr. 23 en p. 15 van de Nota van Toelichting bij het Bogw.	Zie reactie bij #2.
9	Politie: Digit	Hoofdstuk 3, laatste alinea, p. 18	Van…geworden.	Met deze zin wordt de suggestie gewekt dat hier sprake is van een door de Inspectie geconstateerde afwijking. Dit is niet het geval. Het niet achteraf keuren van een technisch hulpmiddel berust op een beslissing van de officier van justitie om toepassing te geven aan artikel 21 lid 4 Bogw. De Inspectie is herhaaldelijk over deze beslissing geïnformeerd. Daarbij wekt de zin de suggestie dat dit van toepassing is op alle inzetten van de bevoegdheid ex art. 126nba Sv. Dit is evenmin het geval. De beslissing van de officier van justitie om toepassing te geven aan artikel 21 lid 4 Bogw geldt alleen voor een specifieke categorie inzetten. Voor deze categorie inzetten is geen vooraf goedgekeurd technisch hulpmiddel beschikbaar.	De tekst is verduidelijkt. De wetgever heeft als uitgangspunt gesteld dat indien gebruik wordt gemaakt van een technisch hulpmiddel, dit hulpmiddel vooraf moet zijn gekeurd. Zie Kamerstuk 34 372 nr. 3 p.14. In uitzonderingssituaties kan keuring van een technisch hulpmiddel geheel achterwege blijven. De Inspectie heeft met een aanpassing verduidelijkt dat bij de inzet van een commerciële technisch hulpmiddel dat in het merendeel van de zaken in 2022 is ingezet, niet tegenmoet gekomen wordt aan deze uitgangspunten. Het belang dat de wetgever stelt aan de inzet van een goedgekeurd technisch hulpmiddel heeft de Inspectie in hoofdstuk 2 benoemd. De Inspectie signaleert daarbij dat de werkwijze van het inzetten van een niet goedgekeurd technisch hulpmiddel standaardpraktijk geworden. Hierbij is tevens beschreven dat het niet vooraf en afzien van de

					keuring een beslissing is van de officier van justitie. De Inspectie acht het van belang deze praktijk te schetsen om input te leveren voor de gesprekken over dit onderwerp. Zie reactie bij #3 m.b.t. de inzet voor specifieke categorieën.
10	Politie: Digit	Hoofdstuk 3, eerste alinea, p. 19	De…bevel.	In het Besluit onderzoek in een geautomatiseerd werk en de bijbehorende nota van toelichtingen wordt logging niet gekoppeld aan het controleerbaar maken van de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel.	Niet overgenomen. Tijdens de parlementaire behandeling is aangegeven dat *er wordt voorzien in de geautomatiseerde vastlegging van gegevens over de uitvoering van de onderzoekshandelingen (logging) met het oog op de controle op de uitvoering van de bevoegdheid zodat zowel tijdens het onderzoek als op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel.* Zie kamerstuk 34 372 Nr. D, p. 6 en kamerstuk 34 372 Nr. 3 memorie van toelichting p.31 met een gelijke strekking. Volledigheidshalve is in hoofdstuk 2.2.2 een voetnoot met deze verwijzing opgenomen.
11	Politie: Digit	Hoofdstuk 3, vierde alinea, p. 19	De…uitvoering.	Deze zin impliceert dat bij de uitvoering van de bevoegdheid ex art. 126nba Sv geen enkele vorm van kwaliteitszorg plaats vindt. Dat is niet juist. De bevindingen van de Inspectie zien toe op de mate van aantoonbaarheid van die kwaliteitszorg.	Geen aanpassing. De Inspectie geeft in deze passage al voldoende aan dat er kleine stapjes zijn gezet en soms in de praktijk ook zijn toegepast. De Inspectie concludeert dat sprake is van een versnipperde aanpak en inrichting en dat er in 2022 ondanks toezeggingen onvoldoende uitvoering is gegeven aan het verder inbedden daarvan. Dat inrichten en inbedden moet zich niet beperken tot de aantoonbaarheid, maar behoort toegepast te worden in alle fasen van de uitvoering.

12	Politie: Digit	Hoofstuk 3, tweede alinea, p. 20	Gegevens…vernietigd. en De…vernietigd.	Uit art. 126aa van het Wetboek van Strafvordering en het Besluit vernietigen en bewaren niet-gevoegde stukken volgt niet dat geheimhoudersgegevens onmiddellijke moeten worden vernietigd. De weergave van regelgeving door de Inspectie is hier onjuist.	De bevindingen rondom vernietiging en omgang met geheimhoudersinformatie is naar aanleiding van de wederhoorreactie door de Inspectie opnieuw tegen het licht gehouden en daarop aangepast. Het juridisch kader is hierbij uitgebreider beschreven. Ook is een duidelijker onderscheid gemaakt tussen het herkennen van dergelijke gegevens en het kunnen vernietigen van deze gegevens. Hierbij heeft de Inspectie omschreven welke taken en verantwoordelijkheden op grond van het besluit bij het technisch team liggen en welke rol de officier van justitie heeft.
13	Politie: Digit	Hoofdstuk 3, p. 20	Gehele tekst bij bulletpoint "De vernietiging van geheimhoudersgegevens vindt niet plaats.	In deze gehele alinea wordt onvoldoende tot uitdrukking gebracht dat de politie hier wordt geconfronteerd met tegenstrijdige regelgeving. De politie handelt hierin conform de aanwijzingen die haar door de officier van justitie zijn gegeven.	De passages rondom vernietiging en omgang met geheimhoudersinformatie zijn herzien en aangepast. De reactie van de politie in de hoor- en wederhoortabel is opgenomen. Zie tevens verwerking reactie #12.
14	Politie: Digit	Bijlage A, paragraaf A2, tweede alinea p. 26	Twee…(NCSC).	In de huidige tekst ontbreekt de informatie dat de politie aan het NCSC heeft gevraagd terug te koppelen of melding aan de leverancier/producent plaatsgevonden had. Deze terugkoppeling is gegeven.	Overgenomen. Passage toegevoegd.
15	Politie: Digit	Bijlage A, paragraaf A2, tweede alinea p. 26	Deze…leverancier/producent.	Uit de parlementaire behandeling volgt niet welke procesgang de politie moet volgen voor melden van een onbekende kwetsbaarheid, noch dat dit rechtstreeks bij de producent moet. De wetgever gebruikt op sommige plekken het woord 'direct'. Dat lijkt ze niet te doen als synoniem voor 'rechtstreeks', maar als synoniem voor 'terstond'. De vaststelling dat de	Overgenomen. Passage verwijderd.

				politie hier afwijkt van hetgeen in de wetsgeschiedenis is beschreven, is onjuist.	
16	Politie: Digit	Bijlage A, paragraaf A2, laatste alinea p. 26	Daarnaast…kwetsbaarheden.	In het verslag wordt reden van wetenschap voor de kwalificatie *"zeer waarschijnlijk"* niet onderbouwd, terwijl de Inspectie meerdere keren benadrukt dat de software ook voor haar een black-box is en ze dus geen inzicht heeft in de werking of af-/aanwezigheid van onbekende kwetsbaarheden.	Het klopt dat de Inspectie evenals de politie geen inzicht heeft in de exacte werking van deze software en van welke al dan niet onbekende kwetsbaarheden deze software gebruikmaakt. Gelet op de aard van deze software kan echter niet worden uitgesloten dat deze software gebruikmaakt van een of meerdere onbekende kwetsbaarheden om binnen te dringen. De Inspectie heeft de kwalificatie aangepast.
17	Politie: Digit	Bijlage A, paragraaf A4, eerste alinea, p. 32	Net…leverancier.	Net als in 2020 en 2021 geldt in 2022 dat de software en servers in eigendom en beheer zijn van de politie. Toegang voor de leverancier wordt specifiek en uitsluitend door de politie verleend voor onderhoud en technisch beheer door de leverancier. Hierover zijn dwingende juridische afspraken gemaakt.	De wederhoorreactie benoemt dat de politie toegang verleent aan de leverancier. Hiermee wordt de indruk gewekt dat de leverancier deze mogelijkheid standaard niet heeft. Dit is niet het geval. De politie verleent toestemming voor de leverancier en geen toegang. Volledigheidshalve is in de paragraaf toegevoegd dat contractueel is afgesproken dat de leverancier uitsluitend inlogt op de servers na toestemming van de politie maar dat de politie de toegang niet technisch kan controleren of beperken. Deze context was al opgenomen bij de inzet van het commerciële technisch hulpmiddel in een ander deel van het verslag. Het beheer van de software door de politie betreft het functioneel beheer, zoals het aanmaken van onderzoekszaken en accounts voor opsporingsambtenaren van DIGIT. Dat is

					echter niet waar deze bevinding en het risico over gaat.
18	Politie: Digit	Bijlage A, paragraaf A4, eerste alinea, p. 32	Naast…uitgevoerd.	Voor de volledigheid zou vermeld moeten worden dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor commerciële software. Dit is in het verslag van de Inspectie over 2021 wel benoemd (p. 23).	Deze context is al opgenomen in een ander deel van het verslag bij de inzet van het commerciële technisch hulpmiddel op pagina 37. Deze passage is volledigheidshalve ook toegevoegd bij de software voor het binnendringen.
19	Politie: Digit	Bijlage A, paragraaf A4, derde alinea, p. 33	De…is.	Deze signalering bevat een (impliciet) oordeel over het handelen van de officier van justitie. Bovendien wordt met deze zin de suggestie gewekt dat dit van toepassing is op alle inzetten van de bevoegdheid ex art. 126nba Sv. Dit is niet het geval. De beschreven beslissing geldt alleen voor een specifieke categorie inzetten. Voor deze categorie inzetten is geen vooraf goedgekeurd technisch hulpmiddel beschikbaar.	Er is in deze passage verduidelijkt dat het om een specifiek deel van de zaken gaat en dus niet om alle inzetten van de hackbevoegdheid. Deze specifieke categorie van inzetten betreft - ook in 2022 - echter wel het overgrote deel van de zaken. De Inspectie beperkt zich tot een signalering dat het achterwege blijven van de keuring daarmee geen uitzondering, maar standaardpraktijk geworden is. Hiermee wordt geen (impliciet) oordeel gegeven maar wel een beeld geschetst van de praktijk van de hackbevoegdheid. De Inspectie acht het van belang dit beeld te geven gelet op de ontwikkelingen op dit onderwerp. Zie reactie bij #3 m.b.t. de verwerking van de opmerking over de inzet voor specifieke categorieën.
20	Politie: Digit	Bijlage A, paragraaf A4, tweede alinea, p. 34	De…ingezet.	Het oordeel over of en in welke mate de waarborgen afdoende zijn, is in het Nederlandse strafproces voorbehouden aan de rechter en (voorafgaand daaraan) aan de oordeelsvorming van de officier van justitie.	De zinsnede met betreffende woordkeuze is verwijderd. De Inspectie is zich bewust van de reikwijdte van haar toezicht en de rol van de rechter. De bevindingen over dit onderwerp vallen binnen de reikwijdte van het toezicht. Een voorbeeld hiervan is het ontbreken van een controleerbare duiding en appreciatie van

				Dit valt buiten de reikwijdte van het toezicht van de Inspectie. De conclusies betreffende de toereikbaarheid van de waarborgen vallen niet binnen de scope van het verslag en moeten daarin niet worden opgenomen. Daarbij lijkt de Inspectie in de beoordeling van de test- en verificatieopstelling vooral vanuit een technisch perspectief te redeneren zonder zich rekenschap te geven van de wijze waarop in het strafproces door de rechter appreciatie van (de betrouwbaarheid van) bewijsmiddelen plaatsvindt. Bovendien doet de woordkeuze geen recht aan de inspanningen van de politie verricht om te voldoen aan de kaders die de wetgever heeft gesteld.	testresultaten. Dit betreft immers de praktijk van DIGIT Daarnaast geeft de Inspectie aan dat naast de test- en verificatieopstelling ook sprake is van andere maatregelen. Deze maatregelen kunnen ook bij de tactische teams getroffen zijn. De Inspectie geeft geen oordeel over dit samenstel van maatregelen. Zowel de politie als het OM geven aan dat een samenstel van waarborgen ervoor moet zorgen dat de betrouwbaarheid van gegevens in voldoende mate gewaarborgd is. De Inspectie heeft in de afsluitende alinea al benoemd dat het oordeel of en in welke mate het samenstel van waarborgen afdoende is in het strafproces uiteindelijk voorbehouden is aan de rechter.
21	Politie: Digit	Bijlage A, paragraaf A4, vierde alinea, p. 34	Gelet…waarborgen.	Het oordeel over of en in welke mate de waarborgen afdoende zijn, is in het Nederlandse strafproces voorbehouden aan de rechter en (voorafgaand daaraan) aan de oordeelsvorming van de officier van justitie. Dit valt buiten de reikwijdte van het toezicht van de Inspectie. De conclusies betreffende de toereikbaarheid van de waarborgen vallen niet binnen de scope van het verslag en moeten daarin niet worden opgenomen.	Geen aanpassing. Zie tevens reactie bij #20. De Inspectie geeft hier geen oordeel van de praktijk, maar signaleert hier ("merkt op" en "onvoldoende lijkt").
22	Politie: Digit	Bijlage A, paragraaf A4, tweede alinea, p. 36	Deze…consequent.	Het oordeel of er sprake is van een technisch hulpmiddel, valt buiten de reikwijdte van het toezicht door de Inspectie en is voorbehouden	De passage over de definitie van een technisch hulpmiddel is aangepast. Er is explicieter gemaakt dat de besluitvorming over de inzet door de officier van justitie plaatsvindt op basis van een advies van het technisch team van

				aan de oordeelsvorming van de officier van justitie.	DIGIT. De nadruk is gelegd op de constatering dat DIGIT in twee gevallen aan de Inspectie niet duidelijk heeft kunnen maken wat de (ontwerp)overwegingen zijn geweest om het transport naar de technisch infrastructuur niet te automatiseren. Indien daarvan wel sprake was geweest, was namelijk sprake geweest van een technisch hulpmiddel waarbij in beginsel de weg voor keuring bewandeld moet worden. De signalering dat in een soortgelijke situatie door de officier van justitie geoordeeld is dat de ingezette software een technisch hulpmiddel is, is zonder waardeoordeel opgenomen.
23	Politie: Digit	Bijlage A, paragraaf A4, p. 37	Werkzaamheden…hulpmiddel.	Voor een volledig beeld zou in dit deel van de bevindingen benoemd moeten worden dat er contractuele en procedurele afspraken met de leverancier zijn gemaakt over toegang tot componenten van het technisch hulpmiddel voor onderhouds- en beheerswerkzaamheden. De leverancier vraagt altijd vooraf toestemming voordat de leverancier activiteiten uitvoert. Voordat toestemming wordt verleend wordt door de politie beoordeeld of die werkzaamheden plaats kunnen vinden.	Niet overgenomen. In de alinea waar deze reactie betrekking op heeft, is al aangegeven dat de toegangsbeperking middels een contractuele afspraak ingeregeld is en dat de Inspectie voorbeelden heeft gezien dat de leverancier om toegang vraagt. Zoals aangegeven is het echter voor de Inspectie (en de politie) niet technisch te controleren of deze toestemming altijd door de leverancier gevraagd wordt. Zie tevens reactie #17.
24	Politie: Digit	Bijlage A, paragraaf A4, eerste alinea, p. 38	De…opgeslagen.	Met deze zin wordt onvoldoende genuanceerd dat er een onderscheid bestaat tussen het tijdelijk aanwezig zijn van onderzoeksgegevens op het technisch hulpmiddel en de uiteindelijke vastlegging van de onderzoeksgegevens op de servers (technische infrastructuur) van het technisch team.	De Inspectie heeft dit verduidelijkt door aan te geven dat toegang tot de bedoelde omgeving beperkt is tot enkele medewerkers van DIGIT. De leverancier heeft geen toegang tot deze specifieke omgeving. Dit laat onverlet dat onderzoeksgegevens zich ook buiten deze omgeving bevinden waartoe de leverancier toegang kan verkrijgen. De toegang tot deze

				Op de servers (de technische infrastructuur) waar de onderzoeksgegevens permanent / langdurig op worden vastgelegd, heeft alleen het technisch team van de politie toegang. Bovendien is voorgekomen dat gegevens zijn blijven staan op verzoek van de Inspectie om toezicht mogelijk te maken.	onderzoeksgegevens door de leverancier is ook mogelijk voordat deze gegevens door DIGIT permanent worden vastgelegd. De Inspectie herkent zich niet in de opmerking dat onderzoeksgegevens op verzoek van de Inspectie moeten blijven staan. Wel is gevraagd om verwijdering af te stemmen met de Inspectie vanwege de aanwezige systeemlogging. Deze systeemlogging is van belang omdat daarmee enige controle plaats kan vinden van uitgevoerde handelingen en het optreden van bepaalde gebeurtenissen. Deze gebeurtenissen worden namelijk niet op andere wijze gelogd. Voorkomen moet worden dat het verwijderen een negatief effect heeft op de volledigheid van deze systeemlogging. De Inspectie zou door DIGIT op de hoogte gesteld worden wanneer verwijdering plaatsvindt zodat systeemlogging veiliggesteld kan worden t.b.v. het toezicht. Zowel het verwijderen als het notificeren van het voornemen om te verwijderen, is niet gebeurd.
25	Politie: Digit	Bijlage A, paragraaf A5, eerste alinea, p. 43	Een…aangetroffen.	De wijze waarop dit wordt geformuleerd impliceert dat het hier gaat om een verplichting die voortvloeit uit het rechtskader. Dat is niet het geval. Uit het rechtskader vloeit niet voort dat de politie moet uitwerken welke gebeurtenissen als 'onregelmatigheid' gelden.	Geen aanpassing. In deze passage is al duidelijk gemaakt wat het belang is en dat de politie aangeeft dat het uitwerken van een onregelmatigheid niet direct voortvloeit uit een wettelijke verplichting. Zie tevens reactie #4.
26	Politie: Digit	Bijlage A, paragraaf A5, derde alinea, p. 44	De…opgetreden.	De huidige tekst wekt de suggestie dat de politie alleen beeldscherm- en toetsaanslagopnamen beschikbaar heeft en gebruikt bij de vaststelling of sprake is van	De tekst is aangevuld door aan te geven dat er naast beeldscherm- en toetsaanslagen ook andere vormen van logging beschikbaar zijn. Daarbij wordt nu verwezen naar een eerdere

				onregelmatigheden. Dat is niet het geval. De politie gebruikt deze twee vormen van logging in combinatie met systeemlogging en autorisatie-/authenticatielogging om tijdens en na een inzet te beoordelen of sprake is van onregelmatigheden in de zin van het Bogw of andere bijzonderheden. Daarnaast wordt tijdens een inzet door een daartoe aangewezen medewerker gemonitord of zich onregelmatigheden of bijzonderheden voordoen.	constatering in het verslag dat voor de inrichting en toepassing van deze logging vooral als uitgangspunt is genomen wat technisch standaard voorhanden is. Uitgangspunt zou echter de vereisten uit het Besluit moeten zijn en de risico's die zijn geïnventariseerd in de praktijk. Tevens is verduidelijkt en aangegeven dat de beschikbare logging door de politie veelal op ad-hoc basis gebruikt wordt om zo zowel tijdens de uitvoering als achteraf toe te zien en eventuele afwijkingen of onregelmatigheden te signaleren. In de daaropvolgende alinea wordt al verwezen naar het belang van het uitwerken hoe invulling wordt gegeven aan de doorlopende en automatische logging en de wijze waarop het optreden van de onregelmatigheden wordt gesignaleerd.
27	Politie: Digit	Bijlage A, paragraaf A5, tweede alinea, p. 45	De…logging.	De huidige tekst wekt de suggestie dat de politie alleen maatregelen treft op de technische infrastructuur en niet daarbuiten. Dat is niet het geval. De bevinding van de Inspectie hebben betrekking op de aantoonbaarheid van een en ander.	De tekst is aangescherpt. In de tekst wordt niet suggereert dat er in het geheel geen maatregelen getroffen zijn buiten de technische infrastructuur. In de daaropvolgende alinea is al aangegeven dat dit vraagt om een vastlegging en uitwerking hoe en waar de doorlopende en automatische logging (per zaak) plaats moet vinden. Pas dan kan door de politie overgegaan worden tot het implementeren van passende maatregelen op de juiste plek en aangetoond worden dat deze maatregelen daadwerkelijk aanwezig zijn om

					de betrouwbaarheid en integriteit van deze logging te waarborgen.
28	Politie: Digit	Bijlage A, paragraaf A7, tweede alinea, p. 50	De…vernietigd.	Uit art. 126aa van het Wetboek van Strafvordering en het Besluit vernietigen en bewaren niet- gevoegde stukken volgt niet dat geheimhoudersgegevens onmiddellijk moeten worden vernietigd.	De passage rondom vernietiging en omgang met geheimhoudersinformatie is naar aanleiding van de wederhoorreactie aangepast. Zie tevens reactie #12 en #13.

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
Hoge Nieuwstraat 8 | 2514 EL Den Haag
Postbus 20301 | 2500 EH Den Haag
Contactformulier | www.inspectie-jenv.nl

Juli 2023

Aan deze publicatie kunnen geen rechten worden ontleend. Vermenigvuldigen van informatie uit deze publicatie is toegestaan, mits deze uitgave als bron wordt vermeld.