Beschikbaarheid tapsysteem

Onderzoek naar de technische beschikbaarheid van het tapsysteem van de Nederlandse politie over de periode 2012 tot en met juni 2016

Status: Definitief
Datum: 6 december 2017
Versie: 1.0

Managementsamenvatting

Inleiding

De minister van Veiligheid en Justitie verzocht in februari 2016 de korpschef om de beschikbaarheid van het tapsysteem vanaf 2012 in kaart te brengen.[1] Dit verzoek vloeide voort uit de door de hoogleraren Van Koppen en Jacobs geformuleerde zorg over de technische beschikbaarheid van het tapsysteem. De hoogleraren gaven aan twijfels te hebben bij de gemelde technische beschikbaarheid van het tapsysteem van 99,5%. Dit rapport beschrijft het onderzoek dat zich richt op de periode 2012 tot en met juni 2016 en de uitkomsten daarvan. De Auditdienst Rijk commentarieerde dit onderzoek gedurende de verschillende fasen.

Onderzoeksvragen

Het onderzoek richt zich op de technische beschikbaarheid van het tapsysteem en baseert zich op basis van storingen met (potentieel) dataverlies. Er is dus specifiek gekeken naar technische storingen. Deze onderzoeksafbakening sluit aan bij de tekst van de Minister van 12 februari 2016 waarin hij stelt dat hij de zorg van de hoogleraren serieus neemt. Deze stelden dat zij twijfels hadden bij de genoemde technische beschikbaarheid van minimaal 99,5%. Dit is tevens de wijze van meten zoals die destijds in 2013 heeft plaatsgevonden.
Tijdens het onderzoek bleek dat het tapsysteem geen informatie vastlegt waarmee eenduidig valt vast te stellen of er daadwerkelijk sprake is van dataverlies. We spreken daarom van *(potentieel) dataverlies* als na een tapsysteemstoring dataverlies niet met zekerheid kan worden uitgesloten.
Het onderzoek is na afstemming met het Ministerie van Veiligheid en Justitie uitgewerkt aan de hand van de volgende vier onderzoeksvragen:

1. Hoeveel storingen met dataverlies zijn er per jaar geweest?
2. Wat is op grond van die storingen de resulterende (on)beschikbaarheid van het tapsysteem?
3. In hoeverre hebben de reeds genomen maatregelen effect op de beschikbaarheid van het tapsysteem en op de mogelijkheden om die beschikbaarheid adequaat te monitoren?
4. Welke aanvullende maatregelen kunnen worden genomen om (het monitoren van) de beschikbaarheid te verhogen?

Het onderzoek is dus gericht op het meten van de beschikbaarheid en niet op het vinden en analyseren van de achterliggende (technische) oorzaken van storingen.
De volgende vier paragrafen beantwoorden deze onderzoeksvragen.

1. Hoeveel storingen met dataverlies zijn er per jaar geweest?

Tijdens het onderzoek zijn de storingen in kaart gebracht, die onbeschikbaarheid van (een deel van) het tapsysteem veroorzaakten en hebben geleid tot (potentieel) dataverlies. In het onderzoek is ervoor gekozen om de storingen op basis van de storingsduur[2] te verdelen in drie categorieën[3]: kort, middel en lang.

Van andere, vooraf zinvol geachte indelingen op basis van type tap, bleek tijdens het onderzoek dat deze niet voldoende consequent kunnen worden uitgevoerd. De twee belangrijkste redenen hiervoor zijn (1) het in een aantal gevallen ontbreken van voldoende informatie om het onderscheid te kunnen maken en (2) storingen die zich voordoen in die delen van het tapsysteem waar de verschillende stromen niet van elkaar onderscheidbaar zijn.

Dit resulteert in het volgende overzicht, waarbij 2016 alleen het eerste halfjaar omvat:

[1] Brief van de minister van Veiligheid en Justitie aan de voorzitter van de Tweede Kamer van 12 februari 2016 met kenmerk 706067.
[2] Voor een indeling op basis van impact bleek onvoldoende informatie beschikbaar.
[3] **Kort**: storingen met een duur tot en met 15 minuten, **Middel**: storingen met een duur tussen 16 en 120 minuten, **Lang**: storingen met een duur langer dan 120 minuten. Van elke gevonden storing is de storingsduur vastgesteld in hele minuten.

Jaar	Kort	Middel	Lang	Totaal
2012	37	8	6	**51**
2013	50	3	4	**57**
2014	36	8	7	**51**
2015	19	10	5	**34**
2016 (1e helft)	*6*	*2*	*2*	***10***

Tabel 1 - Aantal gevonden storingen met (potentieel) dataverlies per jaar

Er zijn over de jaren 2012 en 2013 meer storingen gevonden dan bij eerder onderzoek. De belangrijkste reden hiervoor is de uitgebreidheid van het huidige onderzoek: er zijn meer bronnen en tapstromen onderzocht, de reikwijdte betrof het totale tapsysteem en het onderzoek is diepgaander. De totaal benodigde inspanning bleek daarom ook vele malen groter.

2. Wat is op grond van die storingen de resulterende (on)beschikbaarheid van het tapsysteem?

De geïdentificeerde storingen zijn onderzocht om vast te stellen in welke mate de storing resulteerde in onbeschikbaarheid met (potentieel) dataverlies. Deze onbeschikbaarheid is vervolgens per maand en per jaar berekend.
Om meer zicht te krijgen op de verstoringen is de inrichting van het tapsysteem beschouwd als een ketensysteem, waarin verschillende processtappen zijn geïdentificeerd. Op basis van de vervolgens uitgevoerde analyses zijn de situaties vastgesteld waarin storingen kunnen leiden tot onbeschikbaarheid met (potentieel) dataverlies:

1. Bij het **zetten van de tap**: het zetten van taps dan wel het verlengen ervan is niet mogelijk, waardoor gegevens niet getapt worden die bij correcte werking wel beschikbaar zijn[4].
2. Bij **de ontvangst** van de getapte data: gegevens gaan verloren bij het ontvangen van de getapte data door het tapsysteem. Dit betreft het grensvlak van het politietapsysteem met de systemen van de providers die de data getapt hebben en deze vervolgens aan het politietapsysteem aanbieden.
3. Bij de **verwerking** van de getapte data: gegevens gaan verloren tijdens de verwerking van de data en het transport binnen het politietapsysteem.
4. Bij de **opslag** van de getapte data: in de database opgeslagen gegevens gaan verloren.

Beschikbaarheid van het tapsysteem[5]

Onbeschikbaarheid van (delen van) het tapsysteem heeft geleid tot (potentieel) dataverlies tijdens het zetten van taps, de ontvangst en de verwerking van de getapte data. Uit het onderzoek blijkt dat er in de onderzoeksperiode **geen** storingen waren waarbij data in de opslag verloren ging. Onderstaand overzicht, *Tabel 2 - Beschikbaarheid van het tapsysteem per jaar* toont de beschikbaarheid van het tapsysteem voor de categorieën **Tap zetten**, **Ontvangst**, **Verwerking** en **Opslag**. De kolom **Totaal** geeft het percentage van de tijd aan dat het systeem als geheel zonder storingen heeft gefunctioneerd. Het percentage Totaal is de som van de onbeschikbaarheid van de vier categorieën, die vervolgens is afgetrokken van 100%.

Jaar	Tap zetten	Ontvangst	Verwerking	Opslag	Totaal
2012	99,99%	99,08%	99,69%	100%	98,75%
2013	99,87%	99,92%	99,99%	100%	99,77%
2014	99,81%	99,98%	99,53%	100%	99,32%
2015	99,64%	100%	98,68%	100%	98,31%
2016 (1e helft)	*99,98%*	*100%*	*97,38%*	*100%*	*97,37%*

Tabel 2 - Beschikbaarheid van het tapsysteem per jaar

Er zijn over de jaren 2012 en 2013 lagere percentages gevonden dan uit eerder onderzoek naar voren kwam[6]. De belangrijkste reden hiervoor is de uitgebreidheid van het huidige onderzoek: (1) er zijn meer bronnen onderzocht, zoals loggings, de e-mails van medewerkers en het registratiesysteem van de leverancier, (2) alle tapstromen zijn in het onderzoek meegenomen, dus niet alleen spraak, (3) het

[4] Deze situatie is tijdens het onderzoek aangemerkt als een categorie die mogelijk tot dataverlies kan leiden en daarom, met instemming van de opdrachtgever, toegevoegd.
[5] We wijzen erop dat de beschikbaarheidspercentages zijn weergegeven met twee decimalen. De onderbouwing voor deze keuze vindt u in paragraaf 2.2.2. Zie verder de bijlagen B en C voor aanvullende toelichting.
[6] Zie brief van de minister van Veiligheid en Justitie aan de voorzitter van de Tweede Kamer van 17 december 2013.

onderzoek kent een uitgebreidere scope, inclusief het proces van het zetten van taps en (4) het onderzoek is diepgaander uitgevoerd, inclusief een handmatige verificatie van alle door de politie geregistreerde incident tickets.

Het aantal storingen over deze jaren ligt hoger dan in het vorig onderzoek. Dit heeft een negatief effect op de beschikbaarheidscijfers. Er zijn met name veel relatief korte storingen in beeld gekomen.
Het ongunstige beeld over 2015 en de 1e helft 2016 wordt veroorzaakt door één zeer langdurige storing rond de jaarwisseling waarbij een deel van de metagegevens van een beperkt deel van het tapverkeer verloren is gegaan. De aanvoer van de *content* werd door deze storing niet verstoord. Mede daarom is de storing zelf lang onopgemerkt gebleven.

3. In hoeverre hebben de reeds genomen maatregelen effect op de beschikbaarheid van het tapsysteem en op de mogelijkheden om die beschikbaarheid adequaat te monitoren?

In de afgelopen jaren nam de politie meerdere maatregelen ter verbetering van het tapsysteem. Deze zijn veelal niet specifiek gericht op hogere beschikbaarheid van het tapsysteem. Een deel betreft de professionalisering van het beheer in bredere zin. Een aantal maatregelen is recent (april 2016) ingevoerd of afgerond. In dit onderzoek is het daarom niet mogelijk gebleken om een voldoende onderbouwde uitspraak te doen over het directe effect dat de uitvoering van deze maatregelen heeft op de beschikbaarheid.
Wel zijn er twee indicaties van het verbeterde tapsysteembeheer te noemen:

- De dalende trend in het aantal storingen;
- De sterk gestegen beschikbaarheid van logbestanden.

Dit laatste is een indicatie dat het loggingsproces beter is ingericht dan wel beter wordt uitgevoerd. Anderzijds biedt een groter aantal bruikbare logbestanden betere mogelijkheden om de performance van het tapsysteem gestructureerd te onderzoeken en in kaart te brengen.

4. Welke aanvullende maatregelen kunnen worden genomen om (het monitoren van) de beschikbaarheid te verhogen?

Het onderzoek is gericht op meting van de beschikbaarheid en niet op het vinden en analyseren van de achterliggende (technische) oorzaken van storingen.

Op basis van hetgeen de onderzoekers tijdens dit onderzoek zijn tegengekomen en vanuit hun ICT-expertise, adviseert het onderzoeksteam om op een aantal punten aanvullende maatregelen te treffen.

- **Ketenmonitoring**: beschouw het tapsysteem als een ketenproces en richt de monitoring en logging ook zodanig in.
- **Logging en monitoring**: breid de mogelijkheden uit van logging en monitoring ten behoeve van zowel het technische beheer als betere managementinformatie. Voor de korte termijn kunnen de dagelijks gegenereerde logbestanden structureel worden onderzocht. Dit levert per direct al meer inzicht op.
- **Meet in data**: meten in data, bij voorkeur in geordende data, zoals gesprekken en berichten, creëert meer inzicht in de technische beschikbaarheid van het tapsysteem. Dit is echter technisch complex, daarmee vermoedelijk kostbaar en naar huidig inzicht voor de opsporing van beperkt belang.
- **Redundantie**: identificeer single points of failure en evalueer in hoeverre deze moeten worden weggenomen.
- **Graceful shutdowns**: gebruik componenten die de mogelijkheid bieden om zonder verlies van data af te sluiten en opnieuw op te starten (graceful shutdown).
- **Professionaliseer beheerprocessen**: met name de structurele beheerprocessen zoals configuratie-, probleem-, licentie-, capaciteits- en wijzigingsbeheer behoeven versterking. Het onderzoeksteam onderschrijft de beweging die is ingezet om het beheer en de beheerprocessen onder te brengen bij de IV-organisatie van de politie.
- **Stap voor stap**: begin in het nieuw te verwerven systeem met een basisinvoering van het referentiekader en voer daarmee een nulmeting uit. Gebruik dit als startpunt van een proces dat leidt tot verbetering en uitbreiding.

Kijk bij de voorgestelde maatregelen met name naar het nieuw te verwerven systeem. Omdat de levensduur van het huidige systeem ten einde loopt, zijn investeringen daarin niet zinvol meer.

Beschikbaarheid: anders meten

Het onderzoeksteam heeft geconstateerd dat het lastig is om de technische onbeschikbaarheid van het tapsysteem te meten op basis van storingstijd en dat de storingstijd alleen weinig tot geen exacte informatie geeft over de omvang van het dataverlies die wordt geleden. Het team is van mening dat meer waarde moet worden gehecht aan metingen op basis van de verwerkte tapdata. Het meten van input en output in data, bij voorkeur in geordende data (zoals gesprekken en berichten), bij alle schakels binnen de tapketen, verheldert de werking van elke schakel op een manier die veel dichter bij de toepassing en het gebruik van tappen staat, dan het meten en zichtbaar maken van de technische beschikbaarheid van de onderliggende IT-systemen doet.

Een metafoor maakt dit wellicht duidelijker: voor de beschikbaarheid van het openbaar vervoer in Nederland is een halve dag storing op het traject Groningen-Roodeschool, gemeten in *tijd*, ernstiger dan een storing van een uur tussen Amsterdam en Utrecht. Maar gemeten naar het aantal getroffen reizigers zal de tweede storing waarschijnlijk veel meer impact hebben. Dit geldt ook voor het tapsysteem.

Inhoudsopgave

1. Inleiding tot het onderzoek

1.1. Aanleiding

Op 12 februari 2016 stuurde de minister van Veiligheid en Justitie (de minister) een brief aan de Tweede Kamer[7] waarin hij de Kamer onder meer informeerde over de uitkomst van het gesprek over het onderzoeksrapport Interceptiefaciliteit[8] tussen de Auditdienst Rijk (ADR) en de hoogleraren Van Koppen en Jacobs. In de brief meldt de minister dat hij de zorg van de hoogleraren over de technische beschikbaarheid serieus neemt en de korpschef heeft verzocht om de beschikbaarheid van het tapsysteem vanaf 2012 tot heden in kaart te brengen. De ADR commentarieerde het onderzoek. Dit rapport beschrijft dit onderzoek en de uitkomsten ervan.

1.2. Context

De Afdeling Interceptie en Sensing (I&S) van de Landelijke Eenheid (LE) verzorgt op dit moment de interceptie voor de politie, de Rijksrecherche, de bijzondere opsporingsdiensten en de Koninklijke Marechaussee. Zowel de interceptie zelf als de benodigde technische infrastructuur (aangeduid als de interceptiefaciliteit of het tapsysteem) is complex. Naar aanleiding van de rechtszaak tegen Van Rey in 2013 bleek dat er in september 2012 een storing plaatsvond die wel door de leverancier van het tapsysteem was opgemerkt en opgelost, maar niet bij de politie geregistreerd stond.
Dit incident gaf voeding aan de door de hoogleraren geuite zorgen. In zijn brief van 12 februari 2016 aan de Kamer gaat de minister in op de twijfels van de hoogleraren bij de door de korpsleiding gemelde technische beschikbaarheid van het tapsysteem. De minister geeft in de brief aan dat hij de zorgen van beide hoogleraren zeer serieus neemt. Hij heeft daarom *'de korpschef gevraagd de beschikbaarheid van het tapsysteem vanaf 2012 tot heden in kaart te brengen'.* De minister vermeldt in de brief verder dat '*uit een eerste analyse blijkt dat bij herbeoordeling van de destijds gebruikte gegevens geen zekerheid kan worden gegeven of de gerapporteerde beschikbaarheid van het tapsysteem juist is. Hiervoor is een uitgebreide analyse noodzakelijk. Het aantal storingen met dataverlies moet uit een systeem worden gehaald dat niet is ingericht voor het ontsluiten van managementinformatie. Deze analyse zal daarom handmatig moeten worden uitgevoerd en zal minimaal een half jaar in beslag nemen.'*

1.3. Opdrachtgeverschap

De opdrachtgever voor het onderzoek is de korpsleiding, in de persoon van de Chief Information Officer (CIO). Namens de leiding van de Landelijke Eenheid is het hoofd Operatiën de opdrachtnemer. Hij fungeert tevens als gedelegeerd opdrachtgever richting de onderzoeksleider.

1.4. Onderzoeksteam

Het onderzoek is uitgevoerd door een onderzoeksteam bestaande uit vier leden en een onderzoeksleider, allen extern. De onderzoeksleider is ingehuurd van het ICT-adviesbureau Verdonck, Klooster & Associates (VKA). Bij de werving van het onderzoeksteam zijn kandidaat-teams beoordeeld op diepgaande ICT-kennis, ervaring met functioneel beheer (IV/IM), ordentelijke verslaglegging, projectmanagement en onderzoek. Bij de selectie van het team is verder gekeken naar zo veel mogelijk complementaire kennis en ervaring. Er is ten slotte uitdrukkelijk gekozen voor een team met specialistische kennis van en ervaring met (digital) forensic accounting. Alle teamleden zijn voorafgaande aan het onderzoek op het vereiste niveau gescreend.

1.5. Onderzoeksvragen

Zoals in de inleiding aangegeven, is de concrete vraag van de minister aan de korpschef om *'de beschikbaarheid van het tapsysteem vanaf 2012 tot heden in kaart te brengen'*. In overleg met het

[7] Brief van de minister van Veiligheid en Justitie aan de voorzitter van de Tweede Kamer van 12 februari 2016 met kenmerk 706067.
[8] Rapportage onderzoek interceptiefaciliteit, ADR/2014/1470, 9 december 2014, door de minister van Veiligheid en Justitie aangeboden aan de Tweede Kamer op 6 februari 2015, kenmerk 605974.

departement is, voorafgaande aan het feitelijke onderzoek, deze vraag nader gedefinieerd[9] en verdeeld in vier deelvragen:

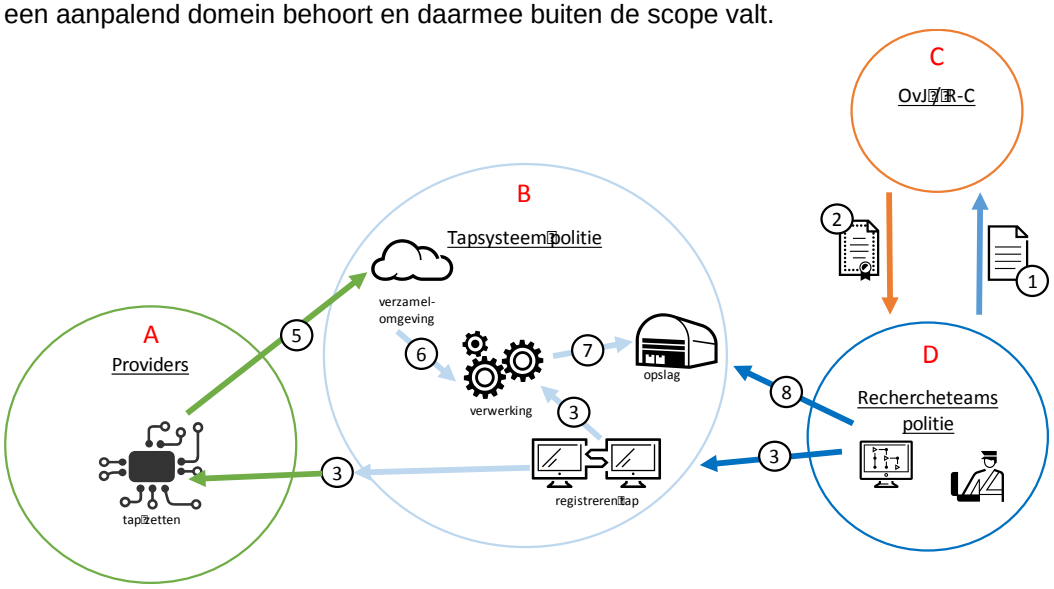
1. Hoeveel storingen met dataverlies zijn er per jaar geweest?
2. Wat is op grond van die storingen de resulterende (on)beschikbaarheid van het tapsysteem?
3. In hoeverre hebben de reeds genomen maatregelen effect op de beschikbaarheid van het tapsysteem en op de mogelijkheden om die beschikbaarheid adequaat te monitoren?
4. Welke aanvullende maatregelen kunnen worden genomen om (het monitoren van) de beschikbaarheid te verhogen?

1.6. Reikwijdte en beperkingen

Het onderzoek richt zich op de onderdelen van het tapsysteem binnen het politiedomein. Zie ook *Figuur 1 - Reikwijdte van het onderzoek*. De reikwijdte van het onderzoek met betrekking tot storingen is als volgt afgebakend[10]: Overwegend dat de hoogleraren hun zorg formuleerden over de technische beschikbaarheid van het systeem, is tot de volgende afbakening besloten:

- De storing doet zich voor binnen de technische infrastructuur (hard- en software) van de politie.
- De storing heeft geleid tot onbeschikbaarheid met (potentieel) dataverlies.
- Er is sprake van (potentieel) dataverlies als:
    - potentiële gegevens niet worden ingewonnen, omdat taps niet kunnen worden gezet (of verlengd). Dit komt overeen met stap 3 in Figuur 1;
    - gegevens die door een provider correct zijn getapt en aangeboden niet of niet goed worden ontvangen door het tapsysteem. Dit komt overeen met stap 5 in Figuur 1;
    - gegevens binnen het tapsysteem tijdens de verwerking of het transport onherstelbaar verloren gaan. Dit komt overeen met stap 6 in Figuur 1;
    - opgeslagen gegevens onherstelbaar verloren gaan. Dit komt overeen met stap 7 in Figuur 1.
- De storing doet zich voor op de systemen die zijn betrokken bij het tapproces, van het zetten van een tap tot de opslag van de verkregen tapgegevens.
- Storingen hebben betrekking op de periode van 2012 tot en met juni 2016.

Schematisch ziet het landschap er als volgt uit. Binnen de reikwijdte van het onderzoek vallen de omgevingen binnen de grote cirkel (B), Tapsysteem politie.
NB: De stappen 3 en 5 hebben componenten waarvan een deel wel binnen de scope valt en een deel bij een aanpalend domein behoort en daarmee buiten de scope valt.



Figuur 1 - Reikwijdte van het onderzoek

Buiten de reikwijdte van het onderzoek vallen alle verstoringen die geen technische oorzaak hebben binnen de infrastructuur van de politie, zoals:

[9] Outline Onderzoeksopdracht analyse van de beschikbaarheid van het tapsysteem van 2012 tot heden, versie 1.1 van 16 maart 2016
[10] Zie voor een gedetailleerde uitwerking Bijlage A

- Handelen door personen, met name het foutief invoeren van een te tappen nummer. Handelingen waardoor het systeem niet meer conform de specificaties functioneert, vallen uiteraard wel binnen de scope van dit onderzoek.
- Vooraf gepland onderhoud, voor zover het onderhoud binnen de aangekondigde tijden is uitgevoerd[11].
- Verstoringen bij het uitwerken van de getapte data door de rechercheteams (stap 8), omdat data die bij die storingen verloren kan gaan, altijd weer kan worden hersteld vanuit de opslag en dus nooit tot definitief dataverlies kan leiden.
- Verstoringen binnen het domein van de providers.

In Bijlage A is een meer gedetailleerde beschrijving van de reikwijdte opgenomen.

Het onderzoek is gericht op meting van de beschikbaarheid en niet op het vinden en analyseren van de achterliggende (technische) oorzaken van storingen, de betrokken verantwoordelijkheden of het vaststellen van eventuele schuld van personen en/of partijen.
De aanbevelingen zijn om die reden vooral gebaseerd op wat de onderzoekers zijn tegengekomen tijdens het onderzoek, in combinatie met hun eigen kennis van ICT-systemen en –processen. Daarnaast speelt mee dat het huidige systeem binnen afzienbare tijd zal worden vervangen, waardoor aanbevelingen voor systeemspecifieke (en vermoedelijk tijdrovende of kostbare ingrepen) weinig rendement zullen opleveren.

1.7. Activiteiten

Voor het onderzoek naar de (on)beschikbaarheid van het tapsysteem zijn de volgende activiteiten uitgevoerd[12]:

- Het bestuderen van relevante documenten.
- Het interviewen van politiemedewerkers.
- Het interviewen van medewerkers van de tapsysteemleverancier.
- Het opstellen van een gedetailleerde weergave van het tapsysteem.
- Het analyseren van de e-mailboxen van de betrokken politiemedewerkers met als doel het vinden van aanvullende informatie over in de tickets gevonden storingen en het zoeken naar niet-geregistreerde storingen.
- Het analyseren van beschikbare processen verbaal.
- Het identificeren van logging.
- Het analyseren van logging en andere beschikbare systeemdata.
- Het analyseren van de door de politie geregistreerde incidenten.
- Het analyseren van de door de leverancier geregistreerde incidenten.
- Het opstellen van een nieuw referentiekader met een gedifferentieerde set van beschikbaarheidsnormen.
- Het analyseren en evalueren van de bevindingen ter beantwoording van de onderzoeksvragen.
- Het afstemmen en toetsen van de feitelijke bevindingen met betrokkenen binnen de politie.
- Het afstemmen van de resultaten met de opdrachtgevers.

1.8. Leeswijzer

Dit rapport kent een gelaagdheid die is bedoeld om lezers met verschillende behoeften aan detailinformatie tegemoet te komen. Voor lezers die kernachtig kennis willen nemen van de onderzoeksresultaten is de *Managementsamenvatting* van het onderzoek en de onderzoeksresultaten bedoeld. Hoofdstuk 2, *Beantwoording van de onderzoeksvragen*, bevat de nadere en meer gedetailleerde uitwerking van het onderzoek. Lezers die geïnteresseerd zijn in een verdere verdieping en de achtergronden van het onderzoek, vinden deze in de bijlagen. Lezers die het rapport inclusief de bijlagen integraal lezen, zullen door deze gelaagdheid sommige teksten en informatie meer dan eens in verschillende mate van detail tegenkomen.

[11] Hoewel bij onderhoud het tapsysteem mogelijk niet, dan wel niet volledig, beschikbaar is, is er geen sprake van een storing. Binnen de ICT-sector is het gebruikelijk dat niet-beschikbaarheid als gevolg van vooraf gepland onderhoud niet wordt meegeteld als onbeschikbaar bij het berekenen van de beschikbaarheid van systemen en diensten.
[12] De stappen gericht op het verzamelen en analyseren van de storingsgegevens hebben plaatsgevonden in de periode juni tot en met november 2016. Aansluitend is in overleg met betrokkenen een nadere analyse van en verificatie op de verzamelde gegevens uitgevoerd in de periode tot en met november 2017.

2. Beantwoording van de onderzoeksvragen

2.1. Onderzoeksuitvoering

Alvorens in te gaan op de beantwoording van de onderzoeksvragen, wordt eerst een beeld geschetst van het tapsysteem en de keten van processtappen die tappen mogelijk maakt. Ook wordt uitgelegd hoe de onderzoekers met de term dataverlies omgingen. Het is belangrijk om hiervan kennis te nemen, aangezien dit verklaart waarom het onderzoeksteam bepaalde keuzes maakte bij het weergeven van de beschikbaarheid.

2.1.1. *Onderzoeksobject*

In 2011 vernieuwde de politie het tapsysteem. Het betreft een complexe ICT-infrastructuur (hardware) met net zo complexe software. Door de technologische ontwikkelingen op het gebied van telecommunicatie is het tapsysteem bovendien voortdurend onderhevig aan veranderingen. Een goed voorbeeld is de nieuwe Europese interceptiestandaard (ETSI 232), die eind 2013 is ingevoerd. Dit leidde tot grote aanpassingen in de infrastructuur van de telecomproviders en de politie. Tot slot zijn de werking en de effectiviteit van het tapsysteem afhankelijk van de aanleverende (keten)partijen – de telecom-providers – die de door hen getapte data op de juiste manier dienen aan te leveren.

De keten van het tapproces

De huidige inrichting van het tapproces is een complexe keten waarin het tapsysteem slechts een schakel vormt. In elke schakel kunnen verstoringen leiden tot dataverlies. Soms zijn tapgegevens niet beschik-baar omdat deze simpelweg niet worden getapt (door foutief inregelen en/of verstoringen binnen andere domeinen in de keten). Providers kunnen een storing binnen hun domein hebben, waardoor zij tapgege-vens niet aan het tapsysteem (kunnen) afleveren. Tot slot kunnen getapte verbindingen wegvallen, omdat het beltegoed op is, de verdachte een ander land binnenrijdt, een schakeling tussen zendmasten niet goed verloopt, et cetera. Dit onderzoek richt zich alleen op de technische infrastructuur van het tapsys-teem die onder de verantwoordelijkheid van de politie valt.

De systemen waarmee tapgegevens worden geanalyseerd, vallen niet binnen de reikwijdte van dit onder-zoek. De reden daarvoor is dat storingen hierin weliswaar kunnen leiden tot tijdelijke niet-toegankelijkheid van tapgegevens, maar nooit tot definitief dataverlies. Het onderzoek is uitgevoerd op basis van de beschikbare informatie uit het incidentregistratiesysteem van de politie, beschikbare e-mailberichten, processen verbaal, beschikbare informatie van de leverancier en beschikbare systeemloggings uit de tapinfrastructuur van de politie. Deze bronnen zijn nader beschreven in Bijlage C, *Bronnen*.

2.1.2. *Storingen met (potentieel) dataverlies*

Een belangrijk criterium bij het bepalen van de beschikbaarheid van het tapsysteem luidt de vraag of er sprake is van dataverlies. In het kader van het onderzoek wordt onder dataverlies verstaan dat gegevens permanent verloren zijn gegaan en niet meer te herstellen vallen. Indien gegevens kunnen worden terug-gezet vanuit tijdelijke opslag of opnieuw kunnen worden verwerkt dan wel gegenereerd, classificeerden de onderzoekers dit niet als dataverlies. Het herstellen van gegevens is vooral mogelijk bij IP-taps, omdat de data daarvan vrijwel direct bij binnenkomst wordt opgeslagen. Spraaktaps daarentegen worden eerst door het geheimhouderfilter (systeem van nummerherkenning) geleid en daarna opgeslagen, waarbij de toegang tot geheimhoudergesprekken door het systeem wordt geblokkeerd en de gesprekken direct na afloop worden vernietigd. Geheimhoudergesprekken zijn gesprekken waarvan ten minste één van de telefoonnummers die bij het gesprek zijn betrokken, voorkomt op de lijst van geheimhouders. Dit heeft tot gevolg, dat dataverlies dat vóór het filter plaatsvindt veelal niet herstelbaar is.
Dataverlies kan binnen de reikwijdte van dit onderzoek optreden op vier momenten in het tapproces:

1. Bij het **zetten** van de tap: als het zetten (instellen) van de tap of het verlengen van bestaande taps niet mogelijk is, is er sprake van potentieel dataverlies, omdat taps pas later kunnen worden gezet of verlengd. Hierdoor worden gegevens niet getapt die bij correcte werking wel beschikbaar zijn[13].

[13] Deze situatie is tijdens het onderzoek aangemerkt als een categorie die mogelijk tot dataverlies kan leiden en daarom, met instemming van de opdrachtgever, toegevoegd.

2. Bij de **ontvangst** van de getapte data: gegevens gaan verloren tijdens het proces van overdracht, waarbij de provider de getapte data correct aanlevert en het tapsysteem van de politie deze data ontvangt.
3. Bij het **verwerken** en **transporteren** van de data: gegevens gaan verloren tijdens het verwerken en transporteren van de ontvangen data binnen het tapsysteem.
4. Bij de **opslag** van de getapte data: opgeslagen gegevens gaan verloren. Dit heeft betrekking op:
    - verstoringen in de eerste opslag. Dit zijn met name fysieke storingen in de databaseserver of logische storingen in (de tabellen van) de database. Hiervoor geldt dat dataverlies in de meeste gevallen kan worden hersteld middels de getroffen back-upmaatregelen.
    - verstoringen in de verdere opslag, meestal onderdeel van de applicatie die de data verder verwerkt en/of analyseert. Bij deze storingen is de data meestal te herstellen.

We hebben in de storingsanalyse deze verliesmomenten binnen het tapproces gebruikt om de categorieën storingen aan te duiden.

Tijdens het onderzoek bleek dat voor een deel van de storingen niet met zekerheid valt vast te stellen of er al dan niet sprake was van dataverlies. We spreken in die gevallen van mogelijk dataverlies. Voor het onderzoek zijn alle storingen, waarbij met zekerheid of mogelijk dataverlies is opgetreden, gekwalificeerd als ‘storingen met (potentieel) dataverlies’.

Storingen binnen de reikwijdte van het onderzoek

Samengevat is het begrip storingen binnen dit onderzoek als volgt afgebakend:

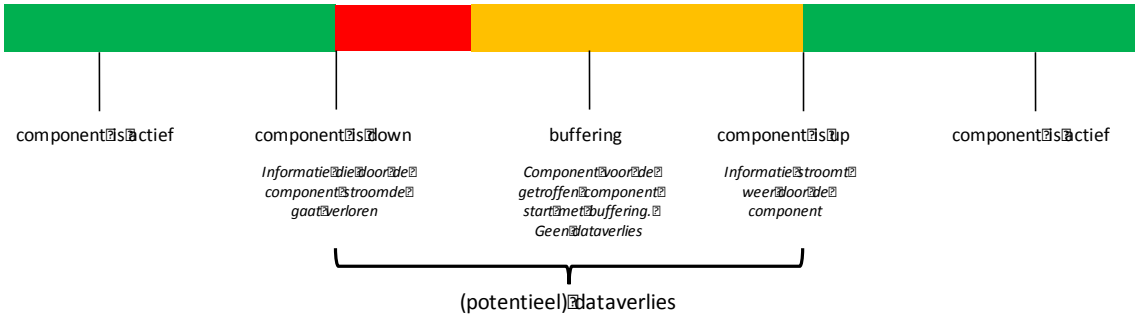
- De storing doet zich voor binnen de technische infrastructuur (hard- en software) van de politie.
- De storing doet zich voor in de systemen die zijn betrokken bij het tapproces, van het zetten van een tap tot de opslag van de verkregen tapgegevens. Zie ook Figuur 1 - *Reikwijdte van het onderzoek*.
- De storing heeft geleid tot onbeschikbaarheid met (potentieel) dataverlies (zie vorige paragraaf).
- Storingen hebben betrekking op de periode van 2012 tot en met juni 2016.

2.1.3. *De duur van het (potentieel) dataverlies*

Als een component binnen de tapinfrastructuur gedurende een zekere tijd niet werkt (onbeschikbaar is), betekent dat niet automatisch dat het (potentieel) dataverlies net zolang duurt. Veelal wordt het (potentieel) dataverlies door buffering beperkt. Het houdt in dat bij uitval van component B zijn voorganger in de keten, component A, de data tijdelijk opslaat (buffert). Zodra component A vaststelt, dat component B weer correct functioneert, stuurt A de tijdelijke gebufferde data alsnog door naar B. Anders dan gewone opslag zijn buffers niet doorzoekbaar en slechts ingericht om gedurende korte tijd data te bewaren. Dat heeft tot gevolg dat het begrip storingstijd in dit onderzoek twee verschillende betekenissen kent, namelijk:

- het aantal minuten dat er een storing is binnen het tapsysteem;
- het aantal minuten (potentieel) dataverlies: dit betreft het aantal minuten dat er daadwerkelijk data verloren kan gaan.

In de onderstaande *Figuur 2 - De duur van (potentieel) dataverlies* is dit grafisch weergegeven. De balk is de tijdlijn en geeft in kleur de status van een component weer. Tijdens de rode en gele periode is de betreffende component niet beschikbaar vanwege een storing (technische onbeschikbaarheid). Echter, alleen tijdens de rode fase kan er sprake zijn van (potentieel) dataverlies. Tijdens de gele fase loopt de buffering bij de voorgaande component en is er feitelijk geen dataverlies meer. Omdat met de huidige loggingsinformatie het exacte tijdstip waarop de buffer start echter niet met zekerheid valt vast te stellen, wordt in het onderzoek de hele storingsperiode (rood en geel) gerekend als storingsduur met (potentieel) dataverlies.



Figuur 2 - De duur van (potentieel) dataverlies

Het daadwerkelijke verlies, dus de **hoeveelheid** gegevens die tijdens een storing verloren gaat, wordt verder bepaald door het tijdstip waarop de storing optreedt. Gedurende de nacht wordt over het algemeen namelijk minder verkeer afgeleverd, omdat er minder activiteit is op de taps. Het is zelfs mogelijk dat er tijdens een storing helemaal geen dataverlies is, als er op het moment van de storing geen actieve data in de door de storing getroffen component aanwezig was. Omdat het tapsysteem hierover geen gegevens registreert, is het feitelijke dataverlies niet structureel vast te stellen. De vastgestelde duur geeft daarmee de duur van het (potentiële) dataverlies. In het onderzoek is ervoor gekozen om de storingen op basis van de gevonden storingsduur te verdelen in drie categorieën: Kort, Middel en Lang. Korte storingen hebben een duur tot en met 15 minuten. De categorie Middel betreft storingen met een duur tussen 16 en 120 minuten en de categorie Lang zijn storingen met een duur langer dan 120 minuten. Van elke gevonden storing is de storingsduur vastgesteld in hele minuten, waar nodig door afronding.

Van andere, vooraf zinvol geachte indelingen op basis van type tap en impact, bleek tijdens het onderzoek dat deze niet voldoende consequent kunnen worden uitgevoerd. De twee belangrijkste redenen hiervoor zijn (1) het in een aantal gevallen ontbreken van voldoende informatie om het onderscheid te kunnen maken en (2) storingen die zich voordoen in die delen van het tapsysteem waar de verschillende stromen niet van elkaar onderscheidbaar zijn.

2.1.4. *Werkwijze beschikbaarheidsanalyse*

Allereerst zijn in de tickets uit het incidentregistratiesysteem van de politie de mogelijke storingen met (potentieel) dataverlies geïdentificeerd. Bij het merendeel van de tickets is vastgesteld dat ze buiten de reikwijdte van dit onderzoek vallen. Dit betreft vooral administratieve meldingen over toegang tot applicaties, hulpverzoeken voor het interpreteren van gegevens en problemen bij de provider, een verdachte die in het buitenland zit, oproeppogingen en dergelijke. Slechts een beperkt percentage van de incidenttickets heeft werkelijk betrekking op een mogelijke storing.

Als tickets een (mogelijke) storing beschreven, is nader onderzoek gedaan op basis van de andere bronnen[14]. Bronnen zijn ingelezen in een specifiek daarvoor ingericht onderzoeksplatform, waarmee alle bronnen met elkaar in verband kunnen worden gebracht, wat analyse van de samenhang van de storingen mogelijk maakt.
Allereerst zijn de storingstabellen van de leverancier vergeleken met de al geïdentificeerde storingen en is het storingsoverzicht aangevuld. Aangetroffen nieuwe storingen zijn toegevoegd. Vervolgens is met het onderzoeksplatform een diepgaande analyse uitgevoerd om vast te stellen welke informatie er over elk van de geïdentificeerde storingen in de verschillende bronnen ter onderbouwing te achterhalen valt. Het storingenoverzicht is hiermee aangevuld. Daarna is een analyse uitgevoerd op de beschikbare logging. Hieruit zijn alle afwijkingen gedestilleerd die duiden op een storing. Deze ‘anomalies’ vergeleken we met de geïdentificeerde storingen en waar nodig verrijkten we het storingsoverzicht. Ontbrekende storingen zijn toegevoegd aan het overzicht.

Tot slot is het resulterende storingsoverzicht opnieuw vergeleken met de informatie in het onderzoeksplatform om de gegevens nogmaals te verifiëren en waar mogelijk verder te verrijken. Een belangrijk doel hierbij was om de duur van elke storing zo exact mogelijk te bepalen en daarmee de onbeschikbaarheidscijfers zo specifiek mogelijk vast te stellen. Met name de beschikbare logging-informatie is een uitstekende bron gebleken om de omvang van een storing nauwkeurig te bepalen. Indien op basis van de bronnen geen uitsluitsel kon worden verkregen over de oorzaak, de aard en/of de omvang van een storing, nam het team op basis van expert opinion een beslissing. Dit betrof zowel beslissingen om een storing wel of niet op te nemen als besluiten over de duur van een storing. Bij deze besluiten zijn vooral de nauwkeurigheid en betrouwbaarheid van de broninformatie meegewogen.

Vervolgens is op basis van het systeemoverzicht en gesprekken met de beheerders van het tapsysteem per systeemcomponent onderzocht en bepaald welke impact de onbeschikbaarheid van die component heeft op de beschikbaarheid van het tapsysteem met betrekking tot het (potentieel) dataverlies. Hierbij is wederom rekening gehouden met de vier categorieën storingen:

- bij tapzetting
- bij ontvangst
- bij verwerking en transport

[14] Zie Bijlage B, ***Aanpak van het onderzoek*** *en* Bijlage C, ***Bronnen***, waarin elk van de bronnen nader wordt beschreven en gekwalificeerd.

- bij opslag

Als uitval van component A leidt tot (potentieel) dataverlies in een van de vier categorieën, dan wordt bij elke storing van component A de storingstijd van die component opgeteld bij de onbeschikbaarheid (in minuten) van de betreffende categorie.
Ten slotte zijn alle storingen nog op samenhang nagelopen aan de hand van twee regels:

1. Storingen die elkaar binnen korte tijd (maximaal één uur) opvolgen en waarbij dezelfde component is betrokken, zijn geteld als een en dezelfde storing, waarbij de storingsduur van beide is opgeteld.
2. Storingen die elkaar in tijd volledig afdekken, deels overlappen dan wel direct op elkaar aansluiten, zijn ongeacht de betrokken componenten als een en dezelfde storing geteld. De duur van de samengestelde storing is bepaald door de totale storingsduur zonder de overlapping dubbel te tellen.

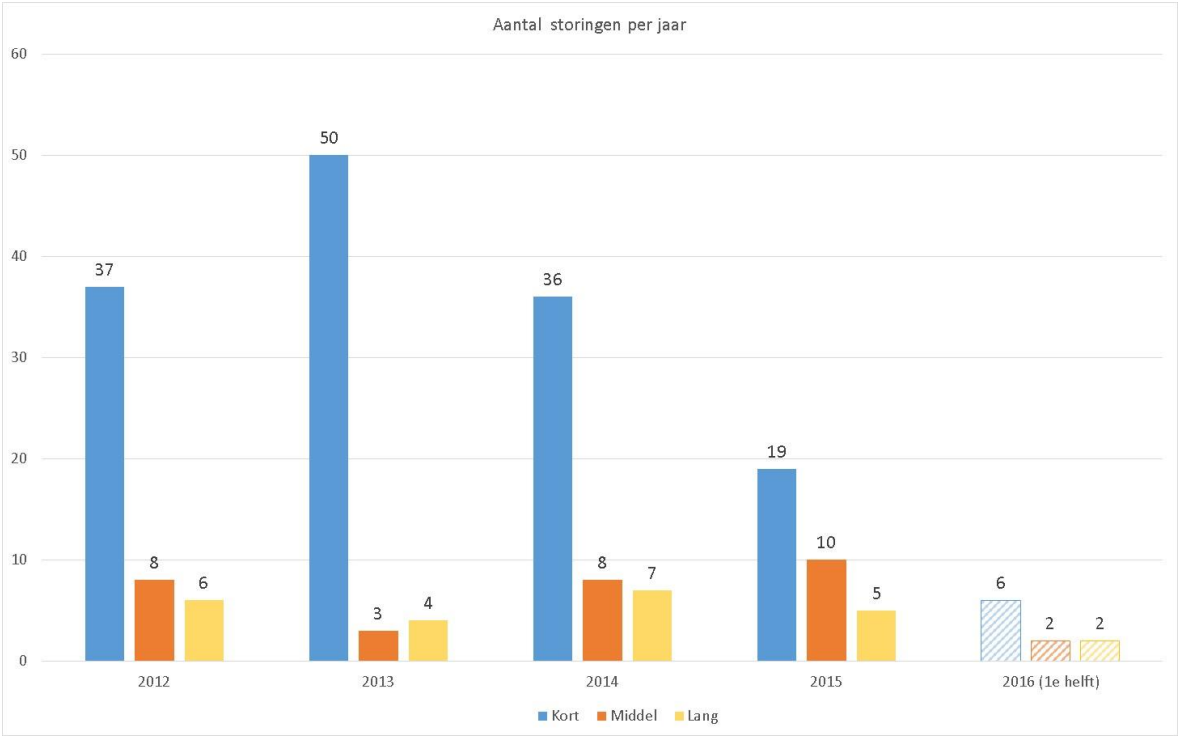
2.2. Beantwoording van de onderzoeksvragen

2.2.1. *Hoeveel storingen met dataverlies zijn er per jaar geweest?*

Op basis van de definitie van storingen met (potentieel) dataverlies, komt het onderzoeksteam tot de volgende storingsaantallen over de onderzoeksperiode. Zie *Tabel 3 - Aantal gevonden storingen met (potentieel) dataverlies per jaar* en Figuur 3 - *Aantal gevonden storingen met (potentieel) dataverlies per jaar (2016 alleen eerste helft)*. Het betreft hier storingen binnen het tapsysteem die (potentieel) data-verlies tot gevolg hadden tijdens de 4,5 jaar van de onderzoeksperiode 2012-2016. Van het jaar 2016 is alleen het eerste halfjaar onderzocht.

Jaar	Kort	Middel	Lang	Totaal
2012	37	8	6	**51**
2013	50	3	4	**57**
2014	36	8	7	**51**
2015	19	10	5	**34**
2016 (1e helft)	*6*	*2*	*2*	***10***

Tabel 3 - Aantal gevonden storingen met (potentieel) dataverlies per jaar



Figuur 3 - Aantal gevonden storingen met (potentieel) dataverlies per jaar (2016 alleen eerste helft)

Er zijn over de jaren 2012 en 2013 meer storingen gevonden dan bij eerder onderzoek. De belangrijkste reden hiervoor is de uitgebreidheid van het huidige onderzoek: er zijn meer bronnen en meer tapstromen onderzocht, de reikwijdte betrof het totale tapsysteem en het onderzoek is diepgaander. De totaal benodigde inspanning bleek daarom ook vele malen groter.

Een aantal storingen in 2014 valt te verklaren uit het feit dat toen de effecten van de invoering van de nieuwe interceptiestandaard zichtbaar werden. Die invoering vond eind 2013 plaats en stelde providers, politie en leverancier voor grote uitdagingen. Gedurende 2014 zijn deze problemen opgelost door het aanpassen van soft- en hardware door alle betrokken partijen. In de praktijk leidde dit ertoe dat systemen op momenten moesten worden herstart, wat resulteerde in onderbreking van actieve tapsessies en het verlies van het restant van de betreffende sessies. De invoering van de nieuwe interceptiestandaard (ETSI-232) was noodzakelijk, omdat de oude standaarden (ETSI-671 en TIIT) niet geschikt zijn voor de interceptie van (mobiele) data en IP-verkeer. De volgende paragraaf gaat in op het effect van de genoemde storingen op de beschikbaarheid van het tapsysteem.

2.2.2. *Wat is op grond van die storingen de resulterende (on)beschikbaarheid van het tapsysteem?*

Op basis van de definitie van storingen met (potentieel) dataverlies, komt het onderzoeksteam tot de volgende beschikbaarheidspercentages[15] over de onderzoeksperiode. Onderstaand overzicht, Tabel 4 - *Beschikbaarheid in percentages per jaar*, toont over 2012 tot en met juni 2016 de jaarlijkse beschikbaarheidspercentages van het tapsysteem. Opvallend is het ontbreken van dataverlies in de opslag. Dit betekent dat als de data eenmaal is opgeslagen, deze in de praktijk niet meer verloren gaat, terwijl dat in de overige onderdelen van het systeem wel het geval kan zijn. Het percentage Totaal is de som van de onbeschikbaarheid van de vier categorieën, die vervolgens is afgetrokken van 100%.

Jaar	Tap zetten	Ontvangst	Verwerking	Opslag	Totaal
2012	99,99%	99,08%	99,69%	100%	98,75%
2013	99,87%	99,92%	99,99%	100%	99,77%
2014	99,81%	99,98%	99,53%	100%	99,32%
2015	99,64%	100%	98,68%	100%	98,31%
2016 (1e helft)	*99,98%*	*100%*	*97,38%*	*100%*	*97,37%*

Tabel 4 - Beschikbaarheid in percentages per jaar

Er zijn over de jaren 2012 en 2013 lagere percentages gevonden dan uit eerder onderzoek naar voren kwam[16]. De belangrijkste reden hiervoor is de uitgebreidheid van het huidige onderzoek: (1) er zijn meer bronnen onderzocht, zoals loggings, de e-mails van medewerkers en het registratiesysteem van de leverancier, (2) alle tapstromen zijn in het onderzoek betrokken, dus niet alleen spraak, (3) het onderzoek kent een uitgebreidere scope, inclusief het proces van het zetten van taps en (4) het onderzoek is diepgaander uitgevoerd, inclusief een handmatige verificatie van alle door de politie geregistreerde incident tickets.

Het aantal storingen over deze jaren ligt hoger dan in het vorig onderzoek. Dit heeft een negatief effect op de beschikbaarheidscijfers. Er zijn met name veel relatief korte storingen in beeld gekomen.

De achterblijvende percentages in 2015 en 2016 worden in overwegende mate veroorzaakt door één langdurige storing, die begon op 28 december 2015 en doorliep tot op 5 januari 2016. Het betrof een incident waarbij verlies van een deel van de metagegevens voor een beperkt deel van de sessies optrad. De aanvoer van de *content* werd door deze storing niet verstoord. Mede vanwege dit geringe effect op de dienstverlening is deze storing in het weekeinde van de jaarwisseling pas laat opgemerkt en opgelost,

[15] We wijzen erop dat de beschikbaarheidspercentages zijn weergegeven met twee decimalen. De keuze voor 2 decimalen komt niet voort uit de mate van exactheid en nauwkeurigheid van de onderliggende bronnen en dientengevolge van deze cijfers, maar is overgenomen van de eerdere opgave van de minister (brief van 17 december 2013 aan de vz. TK) over de jaren 2012 en 2013, die eveneens in twee decimalen nauwkeurig was, en is tevens in overeenstemming met het algemeen voorkomend gebruik in de IT-sector om technische beschikbaarheid met twee decimalen weer te geven. Zie de bijlagen B en C voor verdere toelichting.
[16] Zie brief van de minister van Veiligheid en Justitie aan de voorzitter van de Tweede Kamer van 17 december 2013.

waardoor het in tijd gemeten een extreem grote storing werd. Omdat alleen de eerste helft van 2016 is onderzocht, is de invloed van deze storing bij het berekenen van de beschikbaarheid in 2016 relatief groot.

2.2.3. *In hoeverre hebben de reeds genomen maatregelen effect op de beschikbaarheid van het tapsysteem en op de mogelijkheden om die beschikbaarheid adequaat te monitoren?*

In dit onderzoek beschouwden we de door de minister genoemde maatregelen, die daadwerkelijk binnen de onderzoeksperiode zijn genomen en die van invloed (kunnen) zijn op de beschikbaarheid van het tapsysteem. Het betreft de volgende maatregelen:

1. Aanscherping van de procedures: dit betreft de instructies voor het melden van storingen van de tapmodule aan de eindgebruikers en het opstellen van processen verbaal. Tevens is het toezicht op de naleving van de instructies verscherpt. De nieuwe procesbeschrijving 'Incidentmanagement I&S' is in juni 2014 opgeleverd. In 2015 is de volledige uitwerking afgerond met een actualisatie van het (in juni 2014 vastgestelde) proces. De onderliggende werkinstructies zijn vervolgens uitgewerkt. De invoering van het geactualiseerde proces en de werkinstructies zijn aan het einde van het eerste kwartaal van 2016 afgerond.
2. Overdracht beheer: dit betreft de beheeroverdracht van het tapsysteem van de Afdeling I&S (Landelijke Eenheid) aan de ICT-organisatie van de politie. Deze maatregel startte versneld in februari 2016. Gezien de startdatum zou het eerste effect mogelijk zichtbaar kunnen zijn vanaf maart of april 2016, afhankelijk van de exacte uitvoering en timing van de overdracht. Aangezien de onderzochte periode tot en met juni 2016 loopt, is er onvoldoende statistische onderbouwing voor steekhoudende conclusies.
3. Invoeren beheerkalender: dit betreft het opstellen van een beheerkalender met kritieke beheerhandelingen. De kalender is aan het einde van het eerste kwartaal 2016 ingevoerd. Ook van deze maatregel is de meetperiode te kort voor een voldoende betrouwbare duiding van het effect ervan.

Ad 1: In juni 2014 zijn de procedures voor het melden van storingen aan het tapsysteem aangepast en is het toezicht op de naleving van de instructies verscherpt. Onderdeel van deze maatregel is dat alleen medewerkers van het frontoffice nieuwe incidenttickets mogen aanmaken. In welke mate deze maatregel exact van invloed is op de beschikbaarheid van het tapsysteem valt niet te duiden, omdat de maatregel niet direct ingrijpt op de beschikbaarheid zelf. Er is wel een constante daling van het aantal incidenttickets zichtbaar, die mogelijk mede het gevolg is van deze maatregel. Verder heeft het onderzoeksteam waargenomen dat de kwaliteit van de eerste ticketvastlegging is verbeterd. Met name doordat het frontoffice nu veel consequenter alle relevante velden invult, wat eerder regelmatig niet gebeurde. Ten slotte zorgt deze aanpak voor meer eenduidigheid in de beschrijvingen van de incidenten en is er een betere coördinatie bij meervoudige meldingen van dezelfde storing. Tijdens het onderzoek is onvoldoende informatie aangetroffen voor een nadere kwantitatieve en kwalitatieve duiding van het effect dat deze maatregel sorteert, mede omdat de volledige invoering pas per april 2016 afgerond is. Waarbij opgemerkt dient te worden dat de cijfers voor mei en juni 2016 qua aantal storingen (beide één) en storingstijd (respectievelijk drie en twee minuten) voor beide maanden uitstekend te noemen zijn.

2.2.4. *Tussenbalans*

Om de laatste onderzoeksvraag naar de mogelijke aanvullende maatregelen te kunnen beantwoorden, is het van belang om stil te staan bij wat kan worden opgemaakt uit de bevindingen tot nu toe.

- Het aantal storingen per jaar vertoont vanaf 2013 een dalende trend, zoals valt op te maken uit *Tabel 3 - Aantal gevonden storingen met (potentieel) dataverlies per jaar* en Figuur 3 - *Aantal gevonden storingen met (potentieel) dataverlies per jaar (2016 alleen eerste helft)*.
- Ook de beschikbaarheid van bruikbare logbestanden toont een stijgende lijn, wat tevens een indicatie is van verbetering van de beheersituatie.
- Het beschikbaarheidspercentage per jaar kent niet zo'n positieve trend. Met name de langdurige verstoring rond de jaarwisseling 2015-2016 (zie paragraaf 2.2.2., laatste alinea) haalt het percentage in beide jaren fors omlaag. Omdat slechts de helft van 2016 is onderzocht, heeft deze storing relatief grote invloed bij het berekenen van het beschikbaarheidspercentage 2016.
- Voor de gemeten beschikbaarheid speelt ten slotte de wijziging van de interceptiestandaard, die eind 2013 is doorgevoerd, een negatieve rol. Diverse storingen zijn daaraan gerelateerd.

- De mate van dataverlies bij storingen valt binnen het huidige tapsysteem vaak niet exact vast te stellen, simpelweg omdat het tapsysteem hierover geen informatie registreert. Veelal is het alleen mogelijk om de storingsduur vast te stellen. Daarbij blijft bij een deel onduidelijk of er tijdens de storing daadwerkelijk data op de betreffende component verloren is gegaan en zo ja, hoeveel. We spreken daarom van (potentieel) dataverlies.
- Door het ontbreken van feitelijke informatie over de mate van dataverlies, bestaat er geen mogelijkheid om storingen te wegen op basis van hun feitelijke impact. Dat betekent dat elke storing naar rato van de storingsduur is meegeteld, ongeacht de impact van die storing in termen van dataverlies.

2.2.5. *Welke aanvullende maatregelen kunnen worden genomen om (het monitoren van) de beschikbaarheid te verhogen?*

Zoals eerder vermeld, is het uitgevoerde onderzoek primair gericht op het vaststellen van de beschikbaarheid van het tapsysteem gedurende de onderzoeksperiode en niet op het vinden en analyseren van de achterliggende (technische) oorzaken van storingen of op het zoeken naar mankementen of zwakheden in het systeem. De aanbevelingen zijn om die reden gebaseerd op wat de onderzoekers zijn tegengekomen tijdens het onderzoek, in combinatie met hun eigen kennis van ICT-systemen en –processen. Hierbij speelt mee dat het huidige systeem binnen afzienbare tijd zal worden vervangen, waardoor aanbevelingen voor systeemspecifieke (en vermoedelijk tijdrovende of kostbare) ingrepen weinig rendement zullen opleveren. Met bovenstaande in het achterhoofd zijn het team tijdens het onderzoek zaken opgevallen, die verbeterd kunnen worden en die in deze paragraaf als mogelijke verbetermaatregelen zijn beschreven.

Het tapsysteem wordt gekenmerkt door een complexe ICT-infrastructuur met ingewikkelde software en daaromheen een keten met meerdere partijen. De beschikbaarheid van het tapsysteem beter monitoren, kan in belangrijke mate bijdragen aan het sneller duiden van de oorzaak van (gepercipieerde) onbeschikbaarheid. Dit draagt er vervolgens mogelijk aan bij dat de verantwoordelijke partij sneller kan reageren of zelfs anticiperen om een probleem (voortijdig) weg te nemen en dataverlies te voorkomen dan wel te beperken. Het onderzoeksteam is van mening dat de hieronder voorgestelde maatregelen naar verwachting bijdragen aan het verhogen van de beschikbaarheid en het verbeteren van het monitoren en loggen ervan. Hierbij is niet gekeken naar de met deze maatregelen gemoeide kosten.

Draag zorg voor ketenmonitoring

Zoals beschreven maakt het tapsysteem onderdeel uit van een complexe keten. Het monitoren en doormeten van de keten kan beter inzicht geven in toekomstige storingen of de oorzaak van een storing. Door elke stap in de keten te meten en de metingen te vergelijken, kunnen verschillen (zoals het verlies van data) sneller worden opgemerkt, zodat herstelacties eerder kunnen worden opgestart. Op deze manier houdt de beheerorganisatie meer inzicht in de keten en beter zicht op de gemelde incidenten.

Breid de mogelijkheden tot managementinformatie uit in het nieuwe systeem

Het huidige tapsysteem is een opsporingssysteem en dus niet bedoeld om managementinformatie te geven. Een trend in de wereld van dergelijke systemen is echter dat meer en meer stuurinformatie moet kunnen worden aangeleverd. Het zou mogelijk zijn om het aantal meetpunten binnen het systeem uit te breiden, de frequentie van meten te verhogen en zowel op basis van beschikbaarheid als van verwerkte hoeveelheid (input-output) te meten. Denk hierbij aan de actieve taps per tijdinterval, de beschikbaarheid van componenten, het aantal actieve gebruikers, et cetera. Omdat de levensduur van het huidige systeem ten einde loopt, zijn investeringen daarin niet meer zinvol. Voor het te verwerven nieuwe systeem ligt dat uiteraard anders. Het is belangrijk om bij de verwerving en inrichting ervan al vanuit de architectuur structureel aandacht te schenken aan het verkrijgen van dergelijke informatie uit het systeem.

Intensiveer logging en monitoring (gericht op de techniek)

Tijdens het onderzoek is de aanwezigheid van logging op verschillende componenten vastgesteld. Deze logging wordt primair gebruikt om problemen (achteraf) te onderzoeken. De registratie levert waardevolle, relevante en accurate informatie op over het technische systeem, bleek tijdens het onderzoek. Proactieve monitoring helpt bij het voortijdig signaleren van zich aandienende storingen, maar was tijdens de onderzochte periode onvoldoende ingericht. Het verzamelen en aggregeren van loginformatie kan de organisatie en de leverancier helpen bij het sneller en mogelijk voortijdig identificeren van storingen en onderliggende oorzaken. Het is daarom van belang om logging en monitoring uit te breiden. Verder is het belang-

rijk om op gestructureerde wijze en periodieke basis vanuit de logging en monitoring over beheeronderwerpen (waaronder beschikbaarheid) aan het management te rapporteren. Voor de korte termijn kunnen de nu reeds dagelijks in het huidige systeem gegenereerde logbestanden structureel worden onderzocht, bijvoorbeeld op de manier die in het onderzoek is gedaan. Dit levert per direct al meer inzicht op.

Meet in data

Vanuit technisch perspectief kan beter worden gekozen om te meten in termen van hoeveelheden bij voorkeur geordende data **naast** het meten in (storings)tijd. De beschikbaarheid van het tapsysteem kan beter worden uitgedrukt in de hoeveelheid gegevens die succesvol is verwerkt, zoals het aantal minuten en gesprekken (bij spraak) of het aantal MB's (bij data).

Er zijn in principe drie niveaus van meten te onderscheiden die een oplopend mate van detail hebben en die in opvolgende stappen aanvullend zouden kunnen worden geïmplementeerd en dan leiden tot een verhoogd en verbeterd niveau van beschikbaarheidsmetingen:

1. Meten in (storings)tijd: Zoals in dit onderzoek heeft plaatsgevonden. Het geeft alleen informatie over de duur van de technische (on)beschikbaarheid van zowel losse componenten als het volledige systeem;
2. Meten in ruwe data: Dit betreft input-output metingen puur op basis van de hoeveelheden verwerkte data. Dit geeft informatie over het werkelijke verlies aan ruwe data (in megabytes), zowel van losse componenten als over het gehele systeem;
3. Meten in geordende data: Dit betreft het meten van het aantal succesvol getapte dan wel gemiste gesprekken, berichten, sessies en dergelijke voor zover die kunnen worden bepaald. Hiermee wordt, als er bijvoorbeeld gesprekken zijn gemist, exact duidelijk wanneer en welke dat zijn geweest.

Meten in ruwe data en vooral geordende data is binnen het tapsysteem technisch complex. Het huidige tapsysteem is hier totaal niet voor ingericht. Vanwege het gebruik van veel verschillende applicaties, versleuteling en bijvoorbeeld VPN's zal met name IP-data bijzonder lastig te ordenen zijn. Spraak biedt hier vooralsnog meer mogelijkheden. De implementatie ervan vergt forse aanpassingen in het tapsysteem en brengt navenante kosten met zich mee. Naar huidig inzicht is de extra informatie voor de opsporing van beperkt belang.

Redundantie tapsysteem

In het huidige systeem zijn niet alle onderdelen redundant uitgevoerd. Redundantie geeft behalve een hogere beschikbaarheid ook minder of zelfs geen downtime bij onderhoud. Het onderzoeksteam adviseert om te onderzoeken in hoeverre niet-redundante onderdelen redundant te maken zijn. Uiteraard moeten de kosten daarvan worden meegewogen ten opzichte van de te verwachten verbetering van de beschikbaarheid. Een ander belangrijk aspect is uiteraard de nog beperkte levensduur van het huidige systeem. Redundantie moet daarom vooral beschouwd en gewogen worden in de architectuur van het nieuw te verwerven systeem.

Graceful shutdowns

Het onderzoeksteam adviseert te inventariseren in hoeverre apparatuur te gebruiken valt die de mogelijkheid biedt tot een graceful shutdown. Daarbij is het mogelijk om een systeemonderdeel zodanig uit te zetten dat de lopende communicatie correct wordt afgehandeld en waar nodig overgedragen dan wel gebufferd, zonder dat data verloren gaat. Verder adviseert het onderzoeksteam de buffercapaciteit en bufferkwaliteit te verbeteren ter vermindering van het dataverlies. Een belangrijk aspect hierbij is het opstellen en invoeren van een bufferstrategie in de architectuur.

Professionaliseer beheerprocessen op basis van best practises

Bij de analyse van de incidentregistratie is geconstateerd dat de beheermedewerkers als primair doel hebben om de collega's die gebruikmaken van het tapsysteem zo snel mogelijk te voorzien van een oplossing. Er lijkt onvoldoende tijd beschikbaar om aandacht te schenken aan het structureel verhelpen en zelfs voorkomen van terugkerende problemen. Het professionaliseren van die structurele beheerprocessen kan sterk bijdragen aan het terugdringen van het aantal operationele storingen. Het is daarom van belang om voldoende capaciteit en prioriteit toe te kennen aan het professionaliseren van de structurele beheerprocessen zoals configuratie-, probleem-, licentie-, capaciteits- en wijzigingsbeheer. Dit maakt het mogelijk om storingen sneller af te handelen, terugkerende storingen te classificeren als probleem en wijzigingen in de omgeving gecontroleerd door te voeren. Mogelijke methoden hiervoor zijn ITIL v3 en

certificering op basis van ISO 20000-1. Het is tevens belangrijk om de beheerprocessen te ondersteunen met een adequate en representatieve testomgeving. Door het inzetten van een OTAP-straat[17] en met name een goede acceptatieomgeving, kunnen de risico's die met wijzigingen samenhangen worden gereduceerd.

Certificatenbeheer

Gedurende het onderzoek is vastgesteld dat bepaalde jaarlijks terugkerende storingen direct kunnen worden gerelateerd aan het te laat vernieuwen van de benodigde certificaten. Op grond van deze waarneming vermoedt het onderzoeksteam dat het beheer hiervan onvoldoende gestructureerd is ingericht. Voor de continuïteit en stabiliteit van de dienstverlening is het van belang om het gebruik en verwerven van certificaten een structurele plaats te geven en onderdeel te maken van periodieke beheercycli.

Begin eenvoudig in het nieuwe tapsysteem en breid vervolgens uit

Het inrichten van monitoring en logging in een bestaand systeem kan een kostbare operatie betekenen. Voor het huidige tapsysteem lijkt dit niet zinvol. Begin daarom in het nieuw te verwerven systeem met een basisinvoering van het referentiekader en voer daarmee een nulmeting uit. Gebruik de uitkomsten uit de nulmeting als startpunt van een verbeteringsproces met realistische doelen, waarin verbeteringen kunnen worden doorgevoerd en meetpunten stap voor stap toegevoegd.

2.3. Afsluiting

In dit hoofdstuk zijn de gestelde onderzoeksvragen beantwoord. In de bijlagen is een nadere uitwerking van het onderzoek opgenomen.

[17] Een OTAP-straat is de combinatie van een Ontwikkeling-, Test-, Acceptatie- en Productieomgeving die wordt ingezet om de productiecyclus van een systeem (bijvoorbeeld software) vanaf ontwikkeling tot aan de productie op een gestructureerde wijze te beheren waarbij de risico's op operationele verstoringen worden geminimaliseerd.

Bijlagen

De volgende bijlagen maken deel uit van dit rapport:

Bijlage A	Reikwijdte van het onderzoek
Bijlage B	Aanpak van het onderzoek
Bijlage C	Bronnen
Bijlage D	Beschikbaarheid tapsysteem per maand
Bijlage E	Overzicht van figuren en tabellen

Bijlage A Reikwijdte van het onderzoek

Inleiding

Ten aanzien van de reikwijdte is, in overleg met het departement[18], afgesproken, dat het onderzoek zich toespitst op de onderdelen van het tapsysteem binnen het politiedomein. Het onderzoek is gericht op onbeschikbaarheid met dataverlies als gevolg van storingen in het systeem. Er is gekeken naar de aard en omvang waarin dataverlies optreedt in combinatie met de tijdsduur. De onderzochte periode betreft de jaren 2012 tot en met juni 2016. De complexiteit van het tapsysteem vraagt om een meer gedetailleerde beschrijving van de reikwijdte. Hiertoe is een aantal basisvragen gehanteerd:

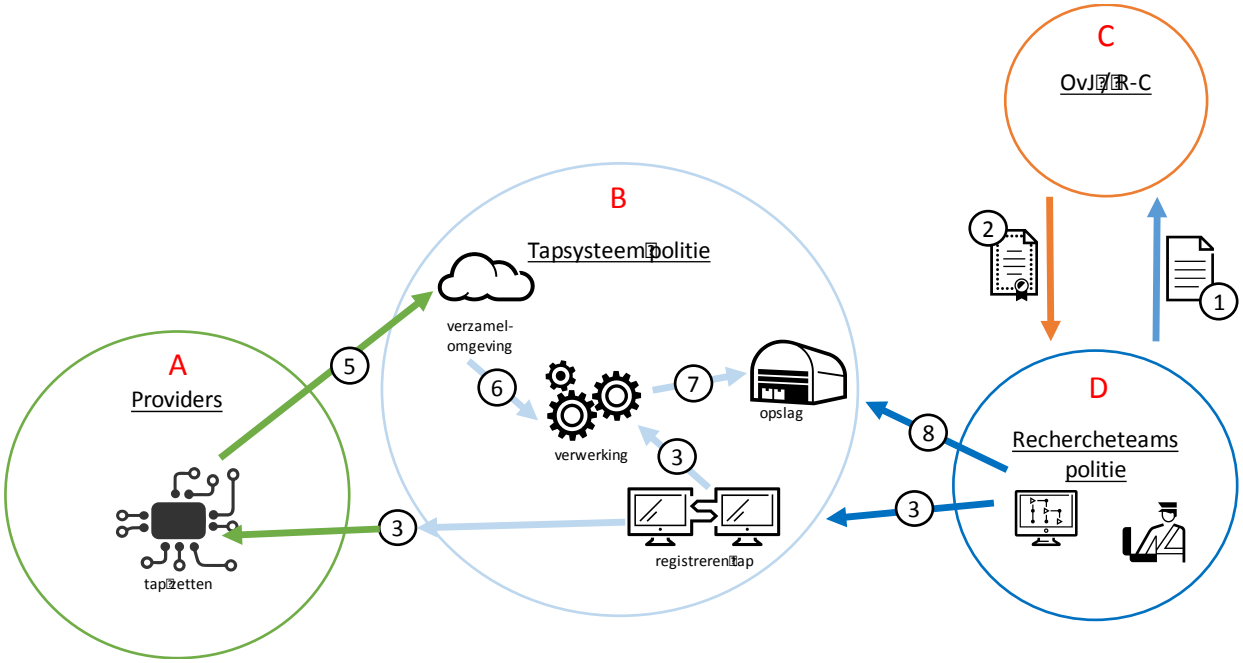
1. Wat behoort wel en niet tot 'het tapsysteem'?
2. Wat behoort wel en niet tot het domein van de politie?
3. Wat is de definitie van beschikbaarheid?
4. Wat is de definitie van dataverlies?

Voor het vaststellen van de onderzoeksreikwijdte zijn in deze bijlage de basisvragen stuk voor stuk uitgewerkt. In de laatste paragraaf van deze bijlage zijn de antwoorden op de vragen geresumeerd en wordt de reikwijdte van het onderzoek naar de beschikbaarheid van het tapsysteem geduid.

NB: Het is voor de lezer van belang te beseffen dat in het spraakgebruik en vooral ook in de media met de term 'tappen' in de meeste gevallen wordt gerefereerd aan het afluisteren van vaste en mobiele telefoongesprekken (spraak). In de praktijk omvat tappen meer dan alleen spraak en wordt ook internetverkeer (vast en mobiel, VoIP en/of data) vaak getapt. Ten slotte is het ook mogelijk om een tap te zetten voor het doorgeven van alleen metagegevens zoals gespreksinformatie. Het uitgevoerde onderzoek betreft alle genoemde soorten taps binnen het tapsysteem.

1. Wat behoort wel en niet tot het tapsysteem?

Het tapsysteem is het technische hart binnen het tapproces. Om een helder beeld te geven van de complexe omgeving waarin het tapsysteem zich bevindt, is de onderstaande, vereenvoudigde weergave van het tapproces opgenomen.



Figuur 4 - Reikwijdte van het onderzoek

[18] Outline Onderzoeksopdracht analyse van de beschikbaarheid van het tapsysteem van 2012 tot heden, versie 1.1 van 16 maart 2016

Dit tapproces bestaat uit de volgende stappen:
1. het rechercheteam dient een tapverzoek in bij de officier van justitie (OvJ) of de rechter-commissaris (RC);
2. de OvJ of RC keurt dit verzoek al dan niet goed[19];
3. bij goedkeuring wordt de tap geregistreerd, de verzamel- en de verwerkingsomgeving ingesteld en de noodzakelijke informatie naar de provider(s) gestuurd;
4. de betrokken providers stellen de tap in;
5. de getapte informatie van alle providers stroomt een centrale verzamelomgeving binnen en wordt voor een deel (niet zijnde spraaktelefonie) voorlopig opgeslagen;
6. de informatie wordt verwerkt;
7. de informatie wordt definitief opgeslagen;
8. het rechercheteam analyseert en verwerkt de getapte informatie in het dossier.

Alleen de technische componenten (hardware/software) maken deel uit van de reikwijdte en zijn dus het onderwerp van dit onderzoek. Tot 'het tapsysteem' behoren in principe alle systemen en componenten die deze processen direct ondersteunen. Het functioneren van de processen en de medewerkers maakt geen deel uit van de reikwijdte van dit onderzoek.

2. Wat behoort wel en niet tot het domein van de politie?

De onderdelen die in het kader van dit onderzoek tot het domein van de politie behoren, zijn de systemen die ingezet worden voor:
- de tapregistratieomgeving (stap 3);
- de verzamelomgeving voor de ontvangst van de data (stap 5);
- de verwerkingsomgeving (stap 6);
- de opslag (stap 7).

Dit houdt het trekken van twee duidelijke grenzen in.
1. De componenten die onder verantwoordelijkheid vallen van de providers, vallen buiten de reikwijdte van dit onderzoek. Dit is in de afbeelding weergegeven met de groene cirkel (A).
2. De componenten, inclusief de toegangsnetwerken, die door politiemedewerkers (de onderzoekteams) en het Openbaar Ministerie (OM) worden gebruikt voor het raadplegen van de tapgegevens (stap 8) vallen buiten de reikwijdte van dit onderzoek. Dit is in het overzicht weergegeven met respectievelijk de donkerblauwe (D) en de oranje cirkel (C).

De reikwijdte van het onderzoek beperkt zich daarmee tot de technische componenten die onder verantwoordelijkheid van de politie vallen, van de registratie van taps via de verzamelomgeving tot en met de opslag, weergegeven in de lichtblauwe cirkel (B).
NB: De stappen 3 en 5 hebben componenten waarvan een deel wel binnen de scope valt en een deel bij een aanpalend domein hoort en daarmee buiten de scope valt.

3. Wat is de definitie van beschikbaarheid?

Een systeem is beschikbaar als het functioneert zoals is beoogd. Uitval beïnvloedt de beschikbaarheid in negatieve zin en komt voor als gedeeltelijke of volledige onbeschikbaarheid van het tapsysteem.

Geplande en ongeplande onbeschikbaarheid

De IT-dienstverlening maakt onderscheid tussen geplande en ongeplande beschikbaarheid. Bij geplande onbeschikbaarheid is sprake van benodigd onderhoud aan systemen en infrastructuur, dat vooraf wordt ingepland in zogenoemde onderhoudsvensters. Het is gebruikelijk om gepland onderhoud buiten de berekening van onbeschikbaarheid te houden. Vaak gaat dit wel gepaard met een vast of een maximum aantal onderhoudsvensters, waarbinnen het onderhoud moet worden uitgevoerd. Binnen dit onderzoek is de keuze gemaakt om de tijd waarin het tapsysteem (deels) niet beschikbaar is vanwege gepland onderhoud binnen de vooraf aangekondigde tijden, niet als onbeschikbaar, maar als beschikbaar te rekenen. Uitloop van onderhoudswerkzaamheden buiten de geplande tijd is wel als onbeschikbaar geduid.

[19] Elke tapopdracht moet vooraf door de RC worden goedgekeurd op voordracht van de OvJ. Alleen een tapopdracht voor het verkrijgen van meta-informatie mag direct zonder tussenkomst van de RC door de OvJ worden uitgevaardigd.

Volledige en gedeeltelijke onbeschikbaarheid

Volledige onbeschikbaarheid betekent dat het tapsysteem in zijn geheel niet beschikbaar is. De kans dat dit gebeurt, is zeer klein, omdat het complete systeem uit veel componenten bestaat en op een aantal cruciale plaatsen redundant is uitgevoerd. Als er sprake is van uitval betreft dat vrijwel altijd slechts een deel van het systeem.

Met gedeeltelijke onbeschikbaarheid wordt de situatie bedoeld waarbij een deel van het tapsysteem niet of niet goed meer werkt. Dit doet zich voor als door een storing de capaciteit van het systeem vermindert (capaciteitsverlies), dan wel de functionaliteit vermindert (functionaliteitsverlies) als er een of meerdere functies uitvallen. Capaciteitsverlies doet zich voor als er in een redundante opstelling één element uitvalt, terwijl de andere, gelijkwaardige elementen blijven functioneren. Bijvoorbeeld als er een probleem optreedt met een specifieke tap of bij de aanlevering van tapgegevens door één provider. Functieverlies doet zich voor als een specifieke functie uitvalt, doordat of een component uitvalt die niet redundant is uitgevoerd, of alle redundante elementen uitvallen die een unieke functie uitvoeren. Voorbeelden van functieverlies zijn de uitval van componenten die spraaktaps decoderen of de uitval van de tapzettingscomponent.

Onbeschikbaarheid in tijd

In de berekening van de beschikbaarheid wordt uitgegaan van de downtime van tapsysteemcomponenten. De netto downtime van een component is niet per definitie gelijk of evenredig aan de duur en/of omvang van het (potentieel) dataverlies dat daarmee wordt veroorzaakt. Veelal wordt het dataverlies door uitval van een component B beperkt, doordat zijn voorganger in de keten, component A, tijdelijk de data opslaat (buffert). Anders dan gewone opslag zijn buffers niet doorzoekbaar en slechts ingericht om gedurende kortere tijd data te bewaren, totdat de verbinding met of de verwerking door component B weer is hersteld. De duur van het (potentieel) dataverlies is daarmee over het algemeen korter dan de duur van onbeschikbaarheid van de betreffende tapsysteemcomponent.

Dat heeft tot gevolg dat het begrip storingstijd in dit onderzoek twee verschillende betekenissen kent in relatie tot onbeschikbaarheid en dataverlies, namelijk:

1. Met minuten onbeschikbaarheid van het tapsysteem wordt bedoeld het aantal minuten dat een of meerdere componenten van het tapsysteem niet conform de specificaties functioneren en er dus sprake is van een technische storing.
2. Met minuten dataverlies wordt bedoeld het netto aantal minuten (de duur) dat er daadwerkelijk data verloren gaat.

Het onderzoeksteam kiest voor de eerste definitie (in hele minuten onbeschikbaarheid) omdat

- geen registratie plaatsvindt van de minuten dat er data verloren gaat;
- ook datataps plaatsvinden die niet in duur uit te drukken zijn, maar eerder in MB's;
- het tijdstip waarop de buffering start niet exact valt vast te stellen.

Het daadwerkelijke verlies aan data in een periode wordt verder bepaald door het tijdstip waarop de storing optreedt. Gedurende de nacht wordt over het algemeen namelijk minder verkeer afgeleverd, omdat er minder activiteit is op de taps.

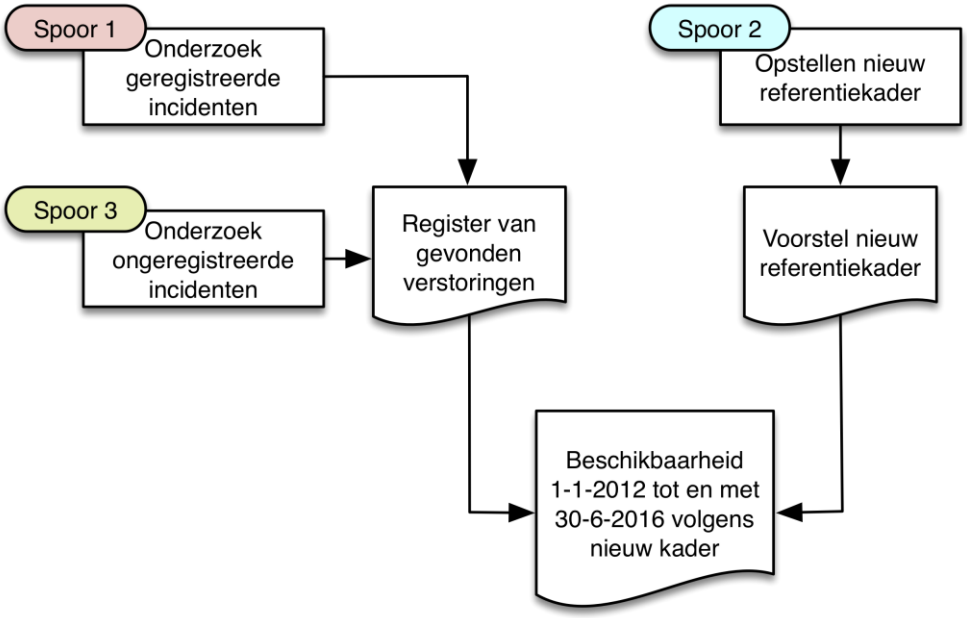
Referentiekader

In zijn brief aan de Tweede Kamer heeft de minister aangegeven dat de beschikbaarheid van het tapsysteem over 2012 99,55% bedroeg en in 2013 (tot 6 december) 99,95%. Deze percentages zijn destijds berekend op basis van de uitval van een deel van de infrastructuur, namelijk het deel voor spraaktaps. In het huidige onderzoek zijn ook de andere onderdelen (data-, metadata- en IP-taps) van het tapsysteem in de berekening meegenomen. Dat is een belangrijke reden dat één enkel percentage voor de totale beschikbaarheid weinig zegt over de performance van het totale tapsysteem. Mede daarom is in dit onderzoek een nieuw referentiekader ontwikkeld dat een beter en genuanceerder beeld kan geven van wat de beschikbaarheid van het tapsysteem is.

Bijlage B Aanpak van het onderzoek

Sporen en producten binnen het onderzoek

Bij aanvang is het onderzoek onderverdeeld in vier sporen, waarvan er drie inhoudelijk en één procesmatig van aard zijn. Deze bijlage beschrijft de inhoud en samenhang van deze sporen. De sporen 1-3 richten zich op het inhoudelijke deel van het onderzoek, spoor 4 bevat de projectactiviteiten. De samenhang tussen de inhoudelijke sporen en producten is op hoofdlijnen weergegeven in *Figuur 5 - Samenhang sporen en producten*.



Figuur 5 - Samenhang sporen en producten bij aanvang onderzoek

SPOOR 1

Inleiding

Spoor 1 van het onderzoek is erop gericht om de incidentregistratie van de politie voor de jaren 2012 tot en met 2016 door te nemen. In dit spoor zijn alle incidentregistraties (OTRS[20]) vanaf 1 januari 2012 tot en met 30 juni 2016 onderzocht en geanalyseerd. De aanpak van spoor 1 is schematisch weergegeven in Figuur 6 - *Overzicht aanpak Spoor 1*.

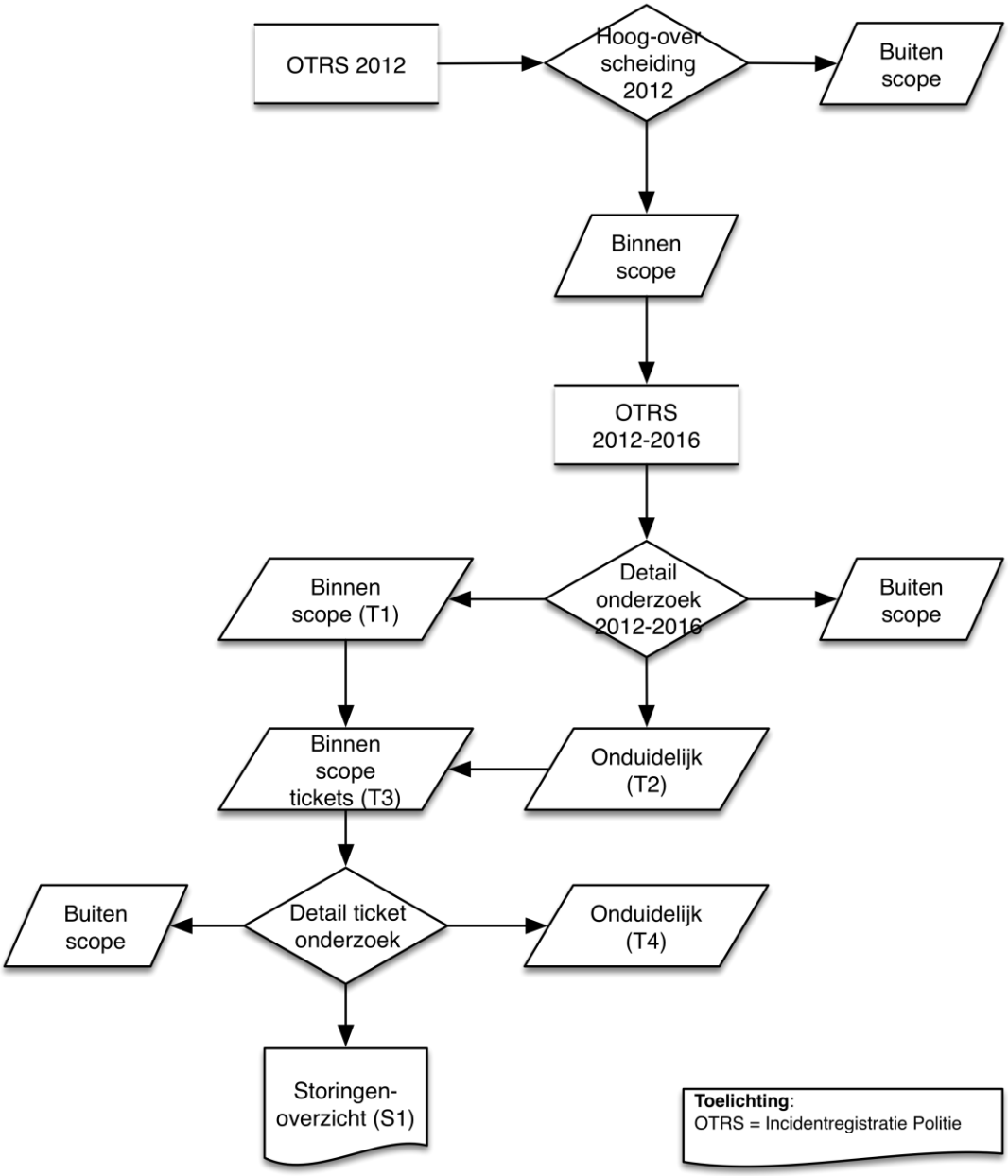
Uitvoering

Alle beschikbare incidenttickets uit de onderzoeksperiode zijn op basis van de datum waarop het ticket is aangemaakt verdeeld over de 54 maanden van het onderzoek. Initieel is elk ticket in 4 stappen[21] onderzocht.

- Stap 1: hoog-over scheiding: het wegfilteren van tickets die zonder nader onderzoek zijn uit te sluiten als storingen
- Stap 2: verificatie van stap 1 op minimaal 10% van de tickets door een tweede onderzoeker
- Stap 3: detailonderzoek van uit de vorige stappen overgebleven tickets door een derde onderzoeker
- Stap 4: verificatie van stap 3 op minimaal 10% van de tickets door een vierde onderzoeker

[20] OTRS: Opensource Ticket Request System

[21] Bij het onderzoeken van de tickets van 2012 bleek dat het efficiënter werkt om de scheiding hoog-over (stap 1) en het detailonderzoek (stap 3) in één slag uit te voeren, gevolgd door één verificatieslag. Deze werkwijze is vervolgens bij het onderzoeken van de tickets vanaf het jaar 2013 toegepast.



Figuur 6 - Overzicht aanpak Spoor 1

Stap 1: hoog-over scheiding

Tijdens stap 1 is het totale aantal tickets in het incidentenregistratiesysteem vergeleken met het vermelde aantal in het projectoverzicht[22]. Vervolgens is per ticket geverifieerd of het ticket binnen of buiten de reikwijdte van het onderzoek valt. Als uitgangspunt hierbij geldt dat alleen bij honderd procent zekerheid dat een storing niet heeft geleid tot dataverlies, is gekozen om deze buiten de reikwijdte van het onderzoek te plaatsen. Bij twijfel is het ticket in onderzoek genomen. De uitkomst van de analyse is geregistreerd en gemotiveerd. Tot slot is gecontroleerd of alle tickets zijn gescheiden (totaal binnen reikwijdte + het totaal buiten reikwijdte = totale aantal tickets van de betreffende maand).

Stap 2: verificatie van stap 1

Tijdens stap 2 is minimaal tien procent van de tickets door een tweede onderzoeker onderzocht. Indien deze een afwijking constateerde, is die afwijking met het projectteam besproken, is indien nodig een aanpak gekozen en gedocumenteerd en zijn alle tickets gecontroleerd op de gekozen aanpak.

[22] Het projectoverzicht is de interne registratie die door het onderzoeksteam is gebruikt, waarin alle projectactiviteiten en de voortgang werden bijgehouden. In het overzicht werden per te onderzoeken maand de aantallen tickets per status bijgehouden.

Stap 3: detailonderzoek van de overgebleven tickets van de vorige stappen door een derde onderzoeker

Tijdens stap 3 is gecontroleerd of het totale aantal tickets met mogelijk dataverlies overeenkomt met dat aantal in het projectoverzicht. De geïdentificeerde tickets (binnen de reikwijdte) zijn in detail nogmaals onderzocht en, indien akkoord, opgenomen in het storingenoverzicht[23]. Tevens is vastgelegd:

- Wat is het incident?
- Wat is de oorzaak?
- Wat is de impact op het systeem en op de dienst?
- Zijn er overige effecten? Zo ja, welke?
- Is er een PV? Zo ja, komt dat overeen met de bevindingen?
- Is er een verbeteringsmaatregel mogelijk?

Tot slot is gecontroleerd of alle tickets zijn onderzocht.

Stap 4: verificatie van stap 3

Tijdens stap 4 is minimaal tien procent van de tickets uit stap 3 door een vierde onderzoeker onderzocht. Bij het constateren van een afwijking is deze met het projectteam besproken, is een aanpak gekozen en gedocumenteerd en zijn alle tickets gecontroleerd op de gekozen aanpak.

Aanpassing procedure

Bij het onderzoeken van de tickets van 2012 bleek dat het efficiënter is om de scheiding hoog-over (stap 1) en het detailonderzoek (stap 3) in één slag uit te voeren, gevolgd door één verificatieslag. Deze werkwijze is vervolgens bij het onderzoeken van de tickets vanaf het jaar 2013 toegepast.

Verificatieslag

Nadat alle maanden zijn geanalyseerd volgens de beschreven procedure, is er een extra verificatieslag toegevoegd, waarbij alle tickets die tot de reikwijdte behoren (T1) en alle tickets met status 'onduidelijk' (T2) zijn samengevoegd tot een nieuwe lijst (T3) en nogmaals met de inmiddels opgedane kennis en ervaring geanalyseerd. Dit heeft geresulteerd in een kleinere lijst onduidelijk (T4) en een storingenoverzicht (S1).

Resultaten

Binnen de incidentregistratie zijn over de periode 1 januari 2012 tot en met 30 juni 2016 in totaal 8360 tickets aangetroffen en onderzocht.
Op basis van het onderzoek vallen 7624 tickets (91,2%) buiten de reikwijdte van het onderzoek, omdat die geen betrekking hebben op een technische storing met (potentieel) dataverlies binnen het domein van de politie. Van 462 tickets (5,5%) is vastgesteld dat die wel betrekking hebben op een dergelijke storing. Bij 274 tickets (3,3%) kon op basis van de informatie in de tickets niet met zekerheid worden vastgesteld of ze wel of niet betrekking hebben op een storing binnen de reikwijdte van het onderzoek. In de onderstaande tabel zijn de aantallen per onderzocht jaar weergegeven. Van het jaar 2016 zijn alleen de gegevens van de eerste helft, van januari tot en met juni meegenomen, waardoor de aantallen lager uitvallen.

Aantal tickets qua impact per jaar					
Totaal	**2012**	**2013**	**2014**	**2015**	**2016** (1e helft)
Totaal aantal tickets					
8.360	2.512	2.358	1.811	1.129	550
100,0%	30,0%	28,2%	21,7%	13,5%	6,6%
Aantal tickets zonder impact					
7.624	2.343	2.121	1.604	1.052	504
91,2%	28,0%	25,4%	19,2%	12,6%	6,0%
Aantal tickets met impact					
462	144	151	122	31	14
5,5%	1,7%	1,8%	1,5%	0,4%	0,2%
Aantal tickets waarvan de impact niet duidelijk is					
274	25	86	85	46	32
3,3%	0,3%	1,0%	1,0%	0,6%	0,4%

Tabel 5 - Analyse van de politie-incidenttickets

[23] Het storingenoverzicht omvat de registratie van alle tijdens het onderzoek gevonden storingen met (mogelijk) dataverlies.

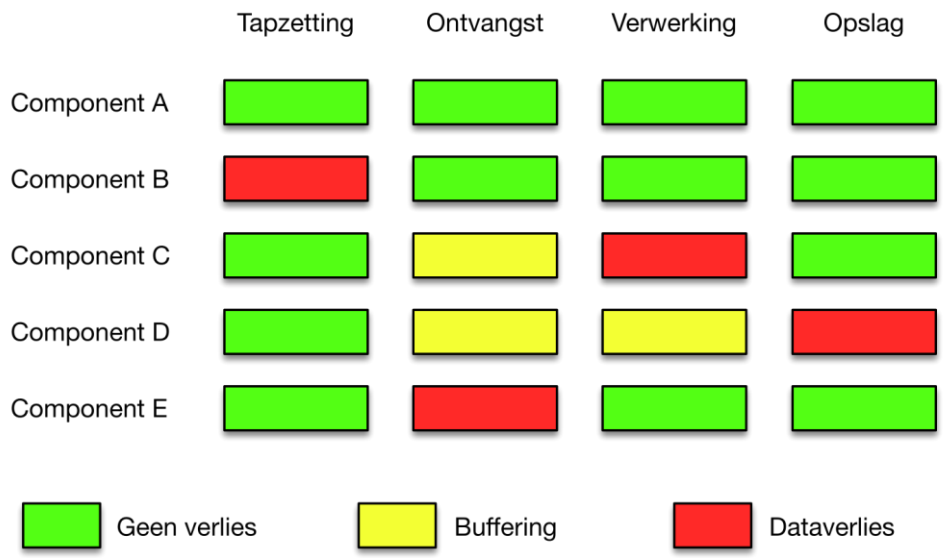
Op basis van de analyses zijn de vier situaties vastgesteld waarin storingen kunnen leiden tot (potentieel) dataverlies:

1. bij het zetten of verlengen van taps;
2. bij de ontvangst van de door de provider getapte data;
3. bij de verwerking en het transport van de data binnen het tapsysteem;
4. bij de opslag van de data.

Het onderscheid is gemaakt omdat het tapsysteem redundantiemaatregelen kent die de beschikbaarheid versterken. De invloed daarvan op de genoemde categorieën kan verschillen. In het onderzoek is daarom per component vastgesteld welke impact de uitval ervan heeft op de beschikbaarheid van de gegevens binnen elk van de categorieën. Door bij alle storingen te duiden welke componenten betrokken zijn, kan vervolgens voor elke storing de onbeschikbaarheid per categorie worden vastgesteld.

Vervolgens zijn alle storingen uit het storingenoverzicht gekoppeld aan een of meerdere componenten (de oorzaak van het incident) van het tapsysteem. Zoals eerder vermeld, is per component in het tapsysteem vastgesteld welke impact die verstoorde component heeft op de beschikbaarheid van het tapsysteem met betrekking tot het verlies van data. Hierbij is de indeling gemaakt naar de vier genoemde categorieën storingen, tapzetting, ontvangst, verwerking en opslag.

Dit heeft geleid tot een Impacttabel. Een klein deel van deze tabel is als voorbeeld weergegeven in *Figuur 7 - Deel van de Impacttabel*. Als een storing in component A leidt tot (potentieel) dataverlies in een (of meer) van de drie categorieën, dan wordt bij elke storing van component A de storingstijd van die component opgeteld bij de onbeschikbaarheid (in minuten) van de betreffende categorie(ën). Op basis daarvan is bepaald wat de impact op de beschikbaarheid in tijd is geweest.



Figuur 7 - Deel van de Impacttabel

Enkele componenten zijn betrokken bij zowel de ontvangst van de getapte data van de providers als bij de verwerking (en het eerste transport) binnen de infrastructuur van de politie. Indien die component uitvalt, wordt de uitvaltijd alleen in de categorie ontvangst meegeteld. De ratio hiervoor is dat gegevens die bij de ontvangst al verloren zijn gegaan, niet in de verwerking nogmaals verloren kunnen gaan. Een andere berekening zou leiden tot dubbeltellingen.

SPOOR 2: referentiekader

Inleiding

Spoor 2 van het onderzoek richtte zich op het opstellen van een referentiekader voor beschikbaarheid. Dit kader is bedoeld om de beschikbaarheid van het tapsysteem volledig weer te geven. Een belangrijke vaststelling van het onderzoeksteam is, dat het tapsysteem en de tapdienst te complex zijn om de beschikbaarheid ervan in één waarde weer te geven en dat het daarom noodzakelijk is om de

beschikbaarheid in een samenhangende set van referentiewaarden uit te drukken. Het referentiekader was bij aanvang van het onderzoek bedoeld om de gevonden (on)beschikbaarheid weer te geven, voor zover daar de data vanuit het bestaande tapsysteem voor beschikbaar was. Zoals eerder vastgesteld, is het huidige systeem niet ingericht voor het opleveren van managementinformatie. Het uiteindelijke beschreven referentiekader kan vanuit de huidige opzet niet worden gevuld en kan derhalve pas na de verwerving van het nieuwe systeem een rol van betekenis spelen. Om die reden is er tijdens het onderzoek voor gekozen om de beschikbaarheid van het tapsysteem niet weer te geven conform het nieuwe referentiekader, zoals bij aanvang van het onderzoek (zie ook Figuur 5 - *Samenhang sporen en producten bij aanvang onderzoek*) wel beoogd werd.

De bij het bepalen van de normen voor het referentiekader meegewogen criteria zijn:
1. De registreerbaarheid van de storingen en eigenschappen en de beschikbaarheid van de benodigde gegevens;
2. De consistentie van het referentiekader;
3. De zeggingskracht en bruikbaarheid van de gekozen normen;
4. De kosten die gepaard gaan met de registratie, verwerking en rapportage, op basis van kennis en ervaring bekeken vanuit de algemene IT-optiek (dus niet specifiek gebaseerd op dit systeem).

Aanpak
Voor het opstellen van het referentiekader zijn drie benaderingen gekozen die uiteindelijk tot één resultaat hebben geleid:
1. De huidige situatie: er is vastgesteld op welke wijze en met welke normen momenteel wordt gewerkt en wat als basis is gebruikt voor het informeren van de minister door de politie;
2. Empirische benadering: op basis van de geregistreerde incidenten is vastgesteld welke verstoringen tot welke onbeschikbaarheid leiden en hieruit is een set vormen van (on)beschikbaarheid afgeleid;
3. Modelmatige benadering: op basis van theorie (bijvoorbeeld ITIL) en de praktijkkennis van het onderzoeksteam in relatie tot vergelijkbare IT-omgevingen is een modelmatig voorstel voor het referentiekader opgesteld.

Storingen kunnen vervolgens op verschillende manieren worden ingedeeld, zoals naar soort storing, naar dienst en/of techniek, naar omvang en naar impact op dienstverlening en eindgebruikers. Het belangrijkste uitgangspunt voor het referentiekader is de focus op de data en het effect op de eindgebruikers.

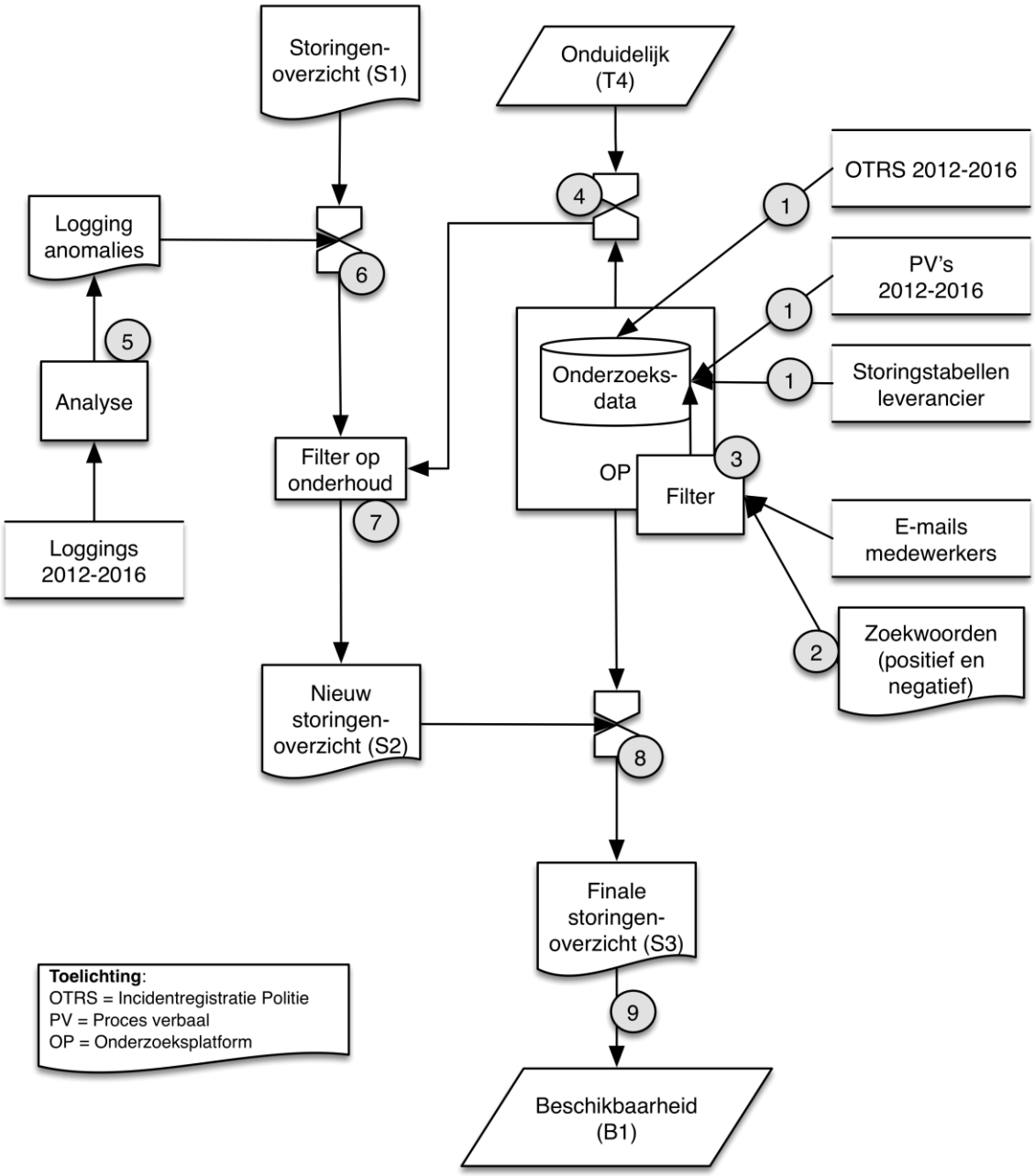
Het referentiekader is als separaat product van het onderzoek opgeleverd.

SPOOR 3: overige, niet door de politie vastgelegde storingen

Inleiding
In spoor 3 van het onderzoek richtte het onderzoeksteam de aandacht op ongeregistreerde storingen (spookstoringen). Het zoeken naar ongeregistreerde storingen vindt zo veel mogelijk geautomatiseerd plaats in andere elektronische bronnen dan de incidentregistratie van de politie. Dit zijn de e-mailboxen van betrokken medewerkers, de PV's, de incidentenregistratie van de leverancier en de systeemloggings. De incidentregistratie van de leverancier is hierbij eerst handmatig geanalyseerd en vervolgens in het geautomatiseerde onderzoeksplatform (OP) opgenomen. Dit onderzoeksplatform maakt het mogelijk om grote hoeveelheden data te verwerken en gestructureerd te doorzoeken.

Hierbij is gezocht naar patronen in het tapsysteem bij geregistreerde storingen. Met de aldus opgebouwde kennis is gezocht naar het bestaan van dergelijke patronen op data en tijdstippen dat geen storing is geregistreerd.

De aanpak hiervan is schematisch weergegeven in *Figuur 8 - Overzicht aanpak Spoor 3*.



Figuur 8 - Overzicht aanpak Spoor 3

Beschrijving aanpak

Bij het onderzoek naar andere storingen dan die in de incidentenregistratie van de politie is gebruikgemaakt van een geautomatiseerd onderzoeksplatform. Hierbij zijn de onderstaande stappen en activiteiten uitgevoerd. De nummers komen overeen met de nummers in het schema van *Figuur 8 - Overzicht aanpak Spoor 3*.

1. Alle data uit de ticketregistratie van de politie, de opgemaakte processen verbaal en de storingstabellen van de leverancier zijn in het platform ingelezen.
2. Er is een lijst met voor het onderzoek relevante zoektermen opgesteld.
3. De lijst met zoektermen is gebruikt als filter bij het inlezen van alle e-mailberichten van alle bij het tapsysteem betrokken politiemedewerkers om zo de inbreuk op de privacy van de betrokken medewerkers zo veel mogelijk te beperken.
4. Het aldus gevulde platform is vervolgens gebruikt om de lijst met onduidelijke incidenten uit spoor 1 (T4) nader te onderzoeken en op te lossen. Incidenten die alsnog als storing zijn geclassificeerd, worden aan het storingenoverzicht toegevoegd.
5. De beschikbare systeemloggings zijn geanalyseerd. Gevonden afwijkingen (anomalies) ten opzichte van het standaardpatroon in de loggings zijn in een apart overzicht opgenomen.

6. Het overzicht met anomalies is vergeleken met het storingenoverzicht (S1), met twee doelen:
    a. Aan de hand van al bekende storingen vaststellen welk soort storing welk patroon in de logging met zich meebrengt;
    b. Onderzoeken of er andere storingen uit de logging zijn dan die al in het storingenoverzicht zijn opgenomen.
7. Alle gevonden storingen (uit stappen 4 en 6) zijn geverifieerd en gefilterd op onderhoud, omdat onderhoud niet meetelt voor onbeschikbaarheid. Het resultaat is een nieuw storingenoverzicht (S2).
8. Dit storingenoverzicht is nogmaals geverifieerd en waar zinvol aangevuld met de data uit het onderzoeksplatform. Het resultaat hiervan is het finale overzicht van gevonden storingen (S3).
9. Op basis van dit finale storingenoverzicht (S3) is de beschikbaarheid van het tapsysteem berekend (B1).

E-mailboxen

De e-mailboxen zijn ingeladen in het onderzoeksplatform. Om een eerste selectie te maken, is ervoor gekozen om een filter te hanteren op de totale set van e-mailgegevens. Het platform is niet in staat om versleutelde berichten te analyseren en laat die berichten daarom geheel buiten beschouwing bij de verdere verwerking en analyse. De termen die in het filter zijn opgenomen, hebben betrekking op de begrippen storing, verstoring, verlies, componenten, operators, leverancier en handelingen die met storing of storingsherstel te maken hebben. Hierbij is vanwege privacyredenen gekozen om niet te filteren op namen van medewerkers. Op basis van deze filtering ontstond de te bevragen gegevensverzameling. Vervolgens zijn de zoekopdrachten uitgevoerd op deze gegevensverzameling.

Processen verbaal

Alle processen verbaal zijn opgehaald uit de betreffende database en inclusief bijlagen ingelezen in het onderzoeksplatform.

Tickets leverancier

De leverancier van het tapsysteem heeft een lijst met incidenttickets (headers) aangeleverd, die handmatig is geanalyseerd en vergeleken met de storingen die in het registratiesysteem van de politie zijn gevonden. In e-mailberichten (zowel intern als met de leverancier) is een aantal storingstabellen aangetroffen die zijn geanalyseerd en gebruikt om het storingsoverzicht aan te vullen en te verrijken. Op basis van de vorige twee stappen zijn alle incidenttickets (headers) van de leverancier gemarkeerd die op een (mogelijke) verstoring duiden. Samen met de leverancier zijn die gemarkeerde tickets geschouwd op basis van registraties uit het ticketsysteem van de leverancier en vervolgens is het storingsoverzicht met de aldus verzamelde informatie aangevuld.

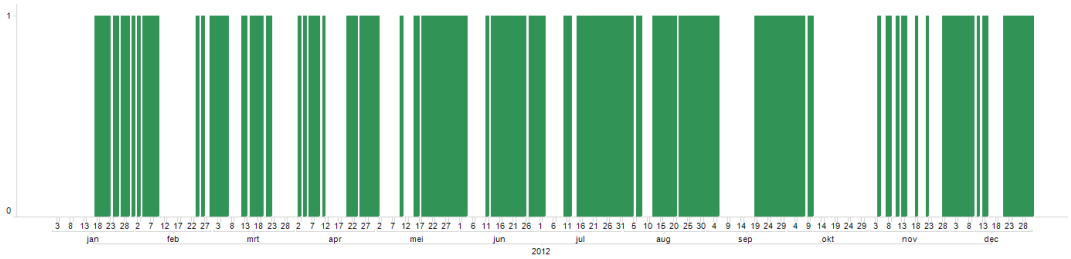
Logging

Binnen het tapsysteem wordt op verschillende plaatsen loggingsinformatie verzameld en weggeschreven. De logging is waardevol, omdat deze geautomatiseerd en gedetailleerd heeft vastgelegd wat er in het tapsysteem is gebeurd. Vanwege de grote omvang van de totale logging kon deze niet worden ingelezen in het onderzoeksplatform. Daarom is gekozen om de logging zelfstandig te analyseren.
De loggings zijn niet compleet. Dit speelt met name bij de files uit de jaren 2012 en 2013. Experts van het Team High Tech Crime en het Nederlands Forensisch Instituut hebben samen met het onderzoeksteam gekeken naar de mogelijkheid tot het alsnog beschikbaar maken van alle loggings. Dit was niet succesvol. In de navolgende Tabel 6 - *Percentages bruikbare loggings per jaar* zijn de percentages per jaar opgenomen van de bruikbare loggings. Er is geen nader onderzoek gedaan naar de oorzaak van de incompleetheid van de loggings, omdat dit niet tot de reikwijdte van het onderzoek behoort.

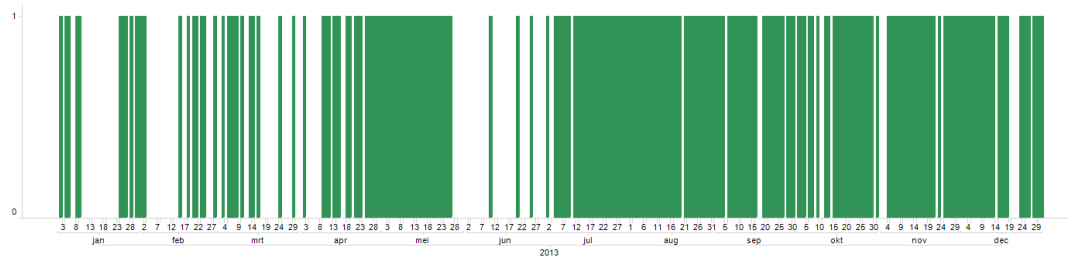
Percentages bruikbare logbestanden per jaar					
Jaar	**2012**	**2013**	**2014**	**2015**	**2016** (1e helft)
% Bruikbaar	54,64%	64,66%	93,97%	95,89%	98,90%

Tabel 6 - Percentages bruikbare loggings per jaar

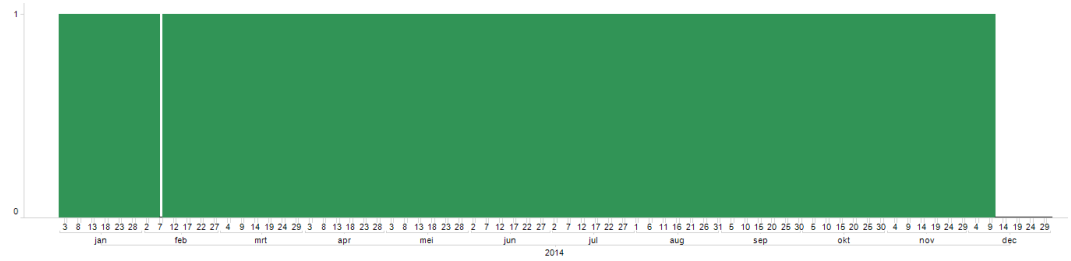
In de onderstaande grafieken is per jaar over de periode 2012 tot en met juni 2016 weergegeven welke logbestanden wel bruikbaar zijn (de groene gedeelten) en welke niet (de witte delen).



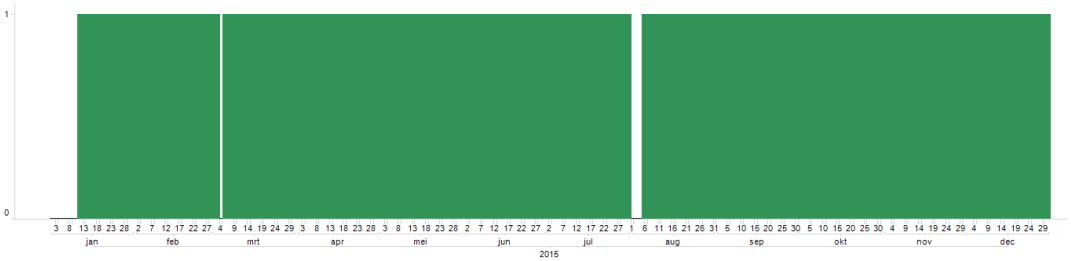
Figuur 9 - Bruikbaarheid logbestanden 2012



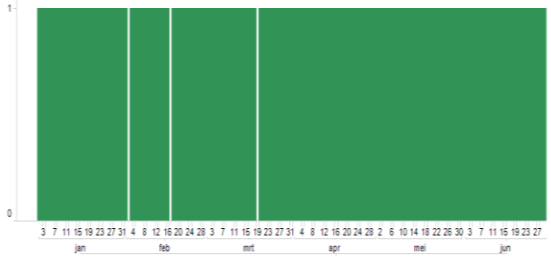
Figuur 10 - Bruikbaarheid logbestanden 2013



Figuur 11 - Bruikbaarheid logbestanden 2014



Figuur 12 - Bruikbaarheid logbestanden 2015



Figuur 13 - Bruikbaarheid logbestanden 2016 (eerste helft)

Bij de analyse is allereerst gekeken naar de omvang van de logbestanden. Elke logfile bevat de log-berichten over een periode van twee uur. Er is een standaard grootte van de logfile als het tapsysteem stabiel draait. Afwijkingen daarvan zijn een sterke aanwijzing voor verstoringen.

Bij een storing zijn drie meldingen in de logging van belang:

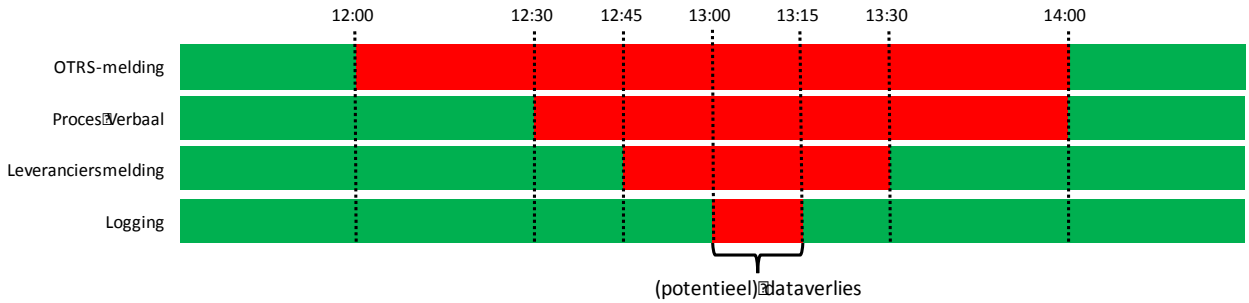
1. Het stoppen van een server. Deze melding wordt alleen gegenereerd als een server op een gecontroleerde manier stopt;
2. Het starten van een server. Deze melding wordt altijd gegenereerd wanneer een server opnieuw wordt opgestart;

3. Het ‘up’ zijn van een server, waarmee de betreffende server meldt dat alles normaal functioneert en er sprake is van een succesvolle herstart.

Voor het onderzoek zijn vooral de start- en upmeldingen van belang, omdat de stopmelding in het geval van een storing niet altijd wordt gedaan, maar soms verloren gaat door de storing zelf.

Het bepalen van de storingsduur

Een belangrijke stap in het proces is de duur van elke storing bepalen. Hiervoor is per storing zo veel mogelijk informatie verzameld uit de verschillende bronnen. Vervolgens is deze informatie per gevonden incident vergeleken en in samenhang beoordeeld. Op basis daarvan stelde het onderzoeksteam een storingsduur in hele minuten vast. Deze storingsduur is de kortste duur waarvan op basis van de beschikbare bronnen is vastgesteld dat die de storing met (potentieel) dataverlies volledig omvat. Oftewel de werkelijke storing kan wel korter, maar nooit langer hebben geduurd dan de door het team vastgestelde storingsduur.
De belangrijkste storingsduurcriteria zijn de nauwkeurigheid en de betrouwbaarheid van de bron. In *Figuur 14 - Voorbeeld gebruik meerdere bronnen*, is een fictief voorbeeld weergegeven van de tijdsinformatie die rond een storing zou kunnen zijn gevonden op zoek naar de aantoonbaar kortste storingsduur (het minimum). In dit voorbeeld zou de storingsduur op vijftien minuten zijn bepaald, omdat de logging de meest betrouwbare, gevonden waarde is. Zou de logging hebben ontbroken, dan zou de qua betrouwbaarheid eerstvolgende waarde, de leveranciersmelding, zijn gebruikt. En zo verder.
De in de figuur getoonde rangschikking is geen vaste rangschikking. Op basis van de gevonden informatie over de betreffende storing en de eigen expert opinion[24] stelde het onderzoeksteam voor elke storing de meest betrouwbare informatie en de uiteindelijke storingsduur per incident vast. Binnen een bron wordt steeds de langste duur gehanteerd waarvoor niet valt uit te sluiten dat er van een storing sprake is (in het voorbeeld 15 minuten).
Zoals elders[25] uitgelegd, is de duur van de storing van de technische component niet per definitie gelijk aan de duur van (potentieel) dataverlies. Zie ook *Figuur 2 - De duur van (potentieel) dataverlies* en de toelichting daarop.



Figuur 14 - Voorbeeld gebruik meerdere bronnen

Inzicht in het tapsysteem

Een belangrijke voorwaarde voor dit spoor is een accuraat inzicht in de technische opbouw en inrichting van het tapsysteem tijdens de onderzoeksperiode (2012-2016). Het resulterende inzicht helpt enerzijds om bij elk incident de impact ervan zo nauwkeurig mogelijk te bepalen. Anderzijds helpt dit inzicht om relevante loggings te lokaliseren. Omdat elk incident en elke logging moet worden gezien in de situatie van het tapsysteem van dat moment, is het noodzakelijk om alle wijzigingen in het systeem gedurende de periode van onderzoek in beeld te hebben.

Er zijn in de periode 2012-2016 verschillende aanpassingen geweest in het tapsysteem. Een ingrijpende wijziging was de uitfasering van het X25-netwerk in combinatie met de ISDN-30 verbindingen voor spraak. De systemen van voor en na deze wijziging zijn voor de spraaktaps dusdanig verschillend, dat met recht van oud en nieuw kan worden gesproken.

[24] Expert opinion verwijst naar het professionele oordeel van de onderzoekers op basis van hun eerder opgedane kennis en ervaring.
[25] Zie paragraaf 2.1.3 in het hoofddocument.

SPOOR 4: projectsturing

Afstemming opdrachtgever

De onderzoeksleider heeft wekelijks afgestemd met de gedelegeerd opdrachtgever. In dit overleg zijn de voortgang, eventuele belemmeringen en de mogelijke beslispunten besproken. De gedelegeerd opdrachtgever is verantwoordelijk voor de afstemming met de interne opdrachtgever, de korpschef.

Afstemming ministerie

Tijdens het onderzoek is er in verschillende samenstellingen afstemming geweest met vertegenwoordigers van het ministerie, de ADR, de korpsleiding, de gedelegeerd opdrachtgever en de onderzoeksleider. Hierbij bracht de onderzoeksleider verslag uit van de voortgang en eventuele issues. Verder zijn de aanwijzingen van de ADR besproken.

Projectaanpak: Agile

Binnen het team is gekozen om te werken op basis van een Agile-aanpak. De belangrijkste overwegingen hiervoor zijn:

- De doorlooptijd, bezetting en het doel van het onderzoek stonden vast, maar de invulling en inrichting niet. Dat vraagt om een flexibele aanpak, zoals met Agile mogelijk is;
- Het was bij aanvang onvoldoende zeker hoeveel inspanning er precies nodig zou zijn voor het analyseren van alle tickets en de andere bronnen. Door te kiezen voor Agile als methodiek kon flexibel worden omgegaan met eventuele onjuiste aannames en inschattingen;
- Bij aanvang bestond er onvoldoende zekerheid of en wanneer enkele bronnen beschikbaar zouden komen. Om toch vanaf het begin effectief te kunnen werken, is een flexibele aanpak cruciaal;
- Meer klassiek vormgegeven onderzoeken starten met een grondig vooronderzoek om onder andere de te onderzoeken omgeving nauwgezet in kaart te brengen en vervolgens de onderzoeksaanpak op basis daarvan vorm te geven. De Agile-aanpak bood de flexibiliteit die nodig is om op korte termijn een grondig onderzoek te verrichten, waarbij essentiële delen uit een klassiek vooronderzoek tijdens het onderzoek ‘on the fly’ zijn uitgevoerd en de uitkomsten ervan in het onderzoek zijn verwerkt;
- Begin 2016 startte de politie met de aanbestedingsvoorbereidingen van het nieuwe tapsysteem. Omdat in een Agile-aanpak conceptrapportages al in een vroeg stadium voor de opdrachtgever beschikbaar kunnen zijn, konden aanbevelingen met betrekking tot het tapsysteem in de eerste versies van de (concept)rapportage meegenomen worden in de aanbesteding;
- De Agile-methodiek biedt de opdrachtgever de mogelijkheid om het onderzoek flexibel aan te sturen, zodat ook bij gewijzigde en onverwachte omstandigheden steeds de optimale strategie kan worden gekozen.

Bijlage C Bronnen

Aantallen

Tijdens het onderzoek zijn diverse bronnen gebruikt. De volgende statistieken geven een beeld van de omvang van deze bronnen:

- 8360 incidenttickets binnen het registratiesysteem van de politie
- 2800 incidenttickets binnen het registratiesysteem van de leverancier
- 984.277 e-mails in 104 mailboxen
- 12,3 TB aan logbestanden
- 11.000 pagina's aan processen verbaal en bijlagen

Tijdens het onderzoek is er geen aanleiding geweest om te twijfelen aan de integriteit van de bronnen. Derhalve is daar geen aanvullend forensisch onderzoek naar gedaan.

Waarde van de bronnen

De aantoonbaarheid van de feiten en bevindingen ten aanzien van de beschikbaarheid moet komen uit de bronnen. Hierbij dient ermee rekening te worden gehouden dat de waarde van een bron voor het onderzoek per bron en per incident verschilt. Zo zal de feitelijke nauwkeurigheid van een interview over een storing die drie tot vier jaar geleden heeft plaatsgevonden, vaak beperkt en daarmee minder waardevol zijn. De aard van de bron bepaalt de informatiewaarde voor het onderzoek. Bij het gebruik van de bronnen is in principe de onderstaande volgorde van (afnemende) waarde gehanteerd, waarbij per geval (storing) op basis van expert opinion van het team een definitieve afweging is gemaakt.

1. De data uit systemen en de loggingen; de aanwezige data is extreem nauwkeurig, zowel in tijd als in event (gebeurtenis). Elke logmelding markeert exact een event met een exacte GMT-tijdsmelding in milliseconden. Niettemin is deze informatie niet volledig in de jaren 2012 en 2013, ondanks intensieve pogingen om die data alsnog te verkrijgen. Over de jaren 2014 tot en met 2016 zijn van vrijwel alle dagen de loggings beschikbaar. In de logbestanden is alle logging verzameld, die de verschillende componenten van het tapsysteem genereren. Echter, niet elke component levert loginformatie aan, wat ook in dat opzicht de logging incompleet maakt.
2. De documentatie over tapsysteem, parameterinstellingen en procedures; het onderzoeksteam beschikte over de documentatie die relevant was voor dit onderzoek.
3. De processen verbaal; de op ambtseed opgemaakte PV's zijn met regelmaat ruim geformuleerd met betrekking tot de (mogelijke) storingstijd, maar geven vaak geen duidelijkheid over de oorzaak van de storing of de relatie tussen het (potentieel) dataverlies en de onbeschikbaarheid van het tapsysteem.
4. De procedurele vastleggingen in de registratiesystemen van de leverancier; de informatie over incidenten is beschikbaar gesteld door de leverancier.
5. De procedurele vastleggingen in de interne registratiesystemen; het incidentregistratiesysteem van de politie is volledig beschikbaar gesteld. De betrouwbaarheid van de informatie wordt bepaald door de kennis van de persoon die de melding maakt. Daarnaast zijn in het systeem veel meldingen aanwezig die niet gerelateerd zijn aan (potentieel) dataverlies veroorzaakt door onbeschikbaarheid van het tapsysteem.
6. De interviews met betrokkenen; de betrouwbaarheid van de informatie wordt bepaald door de kennis die de geïnterviewde over het onderwerp heeft.
7. De informatie in e-mailberichten; de betrouwbaarheid van de informatie wordt bepaald door de kennis die de personen in de communicatie van het onderwerp hebben.

Bij het beoordelen van de waarde van de verschillende bronnen hield het onderzoeksteam rekening met de volgende factoren.

1. **Compleet**: een bron wint aan waarde naarmate de bron completer is. Indien delen ontbreken of niet beschikbaar/leesbaar zijn, dan vermindert de waarde van de bron. Omdat het onderzoek met name gericht is op het vinden dan wel uitsluiten van storingen buiten de incidentregistratie van de politie, is de beschikbaarheid en compleetheid van alternatieve bronnen cruciaal. Het combineren van de verschillende bronnen maakt het mogelijk om broninformatie onderling te versterken en eventuele lacunes in de ene bron te compenseren met informatie uit een andere.

2. **Betrouwbaarheid**: bij elk van de bronnen moet de betrouwbaarheid van de informatie uit de bron worden beschouwd. Hierbij speelt een rol in welke mate de bron authentiek en correct is en wat de kwaliteit van de oorspronkelijk geregistreerde gegevens is.
3. **Duiding** of **zeggingskracht**: de waarde van een bron hangt ook af van zijn duidingskracht: wat betekent de informatie in de bron precies? Zo zegt een startmelding in de log niet dat er een storing is geweest, maar wel dat er een server opnieuw is opgestart. Dit laatste geldt, ondersteund door aanvullende informatie, als een sterke storingsaanwijzing. Een proces verbaal dat een storing beschrijft zonder heldere vermelding van bron, oorzaak of gevolg, biedt vanwege het ontbreken van detailinformatie op zichzelf voor dit onderzoek weinig duiding. Tenzij uit logging blijkt dat een gerelateerd systeem opnieuw opstart.

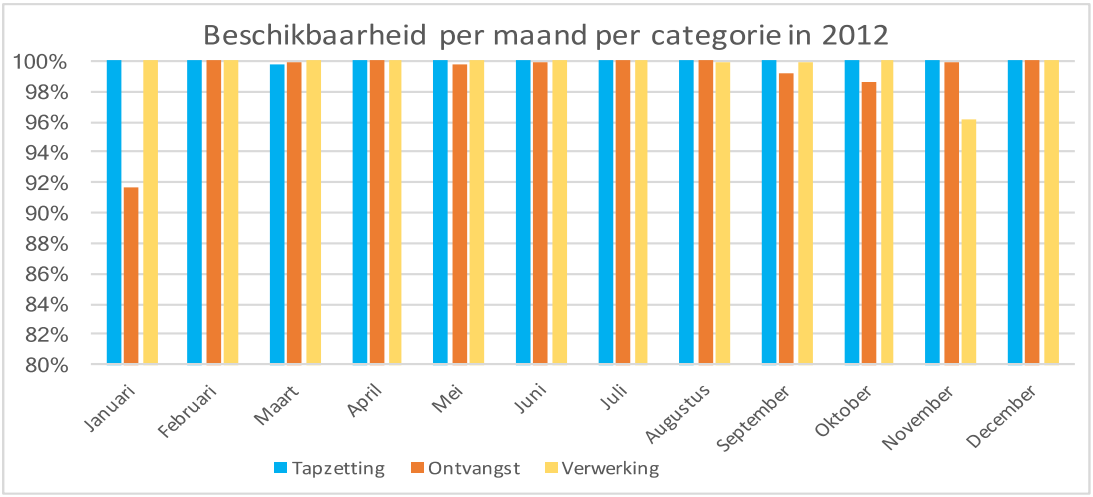
Nauwkeurigheid van de resulterende cijfers

Bij de aanpak van het onderzoek is gekozen voor een benadering waarbij met behulp van de beschikbare bronnen het vinden, identificeren en duiden van zoveel mogelijk incidenten met (potentieel) dataverlies voorop staat. Het was nodig om hiervoor een uitgebreid onderzoek te doen met gebruik van ook andere bronnen dan het tapsysteem zelf, omdat het huidige tapsysteem niet is gebouwd en ingericht om die informatie (eenvoudig) op te leveren. Alle genoemde bronnen hebben bijgedragen aan het inzicht in het aantal verstoringen (en de duur ervan), waarmee de waarde voor de onbeschikbaarheid wordt bepaald, volgens de werkwijze die is beschreven in paragraaf 2.1.4 en in bijlage B. Omdat mogelijk niet alle verstoringen zijn gevonden, is de aldus berekende waarde een minimale waarde voor de onbeschikbaarheid. Door de beschikbaarheid te berekenen als 100% minus de gevonden onbeschikbaarheid, wordt een waarde berekend die de maximale waarde is van de werkelijke beschikbaarheid[26]. Daar staat tegenover dat door de wijze van vaststellen van de duur van het (potentieel) dataverlies, de onbeschikbaarheid juist te ruim gerekend wordt (zie *Figuur 14 - Voorbeeld gebruik meerdere bronnen* en de toelichting daarbij). In het onderzoek zijn de beschikbaarheidscijfers berekend aan de hand van de door de onderzoekers gevonden storingen en aantoonbare minimale storingsduur. Dat laat onverlet dat er meer storingen kunnen zijn geweest, die niet zijn ontdekt, vanwege mogelijke onzuiverheden in de bronnen (niet volledig of niet voldoende nauwkeurig). Dit kan niet met 100% zekerheid worden uitgesloten.

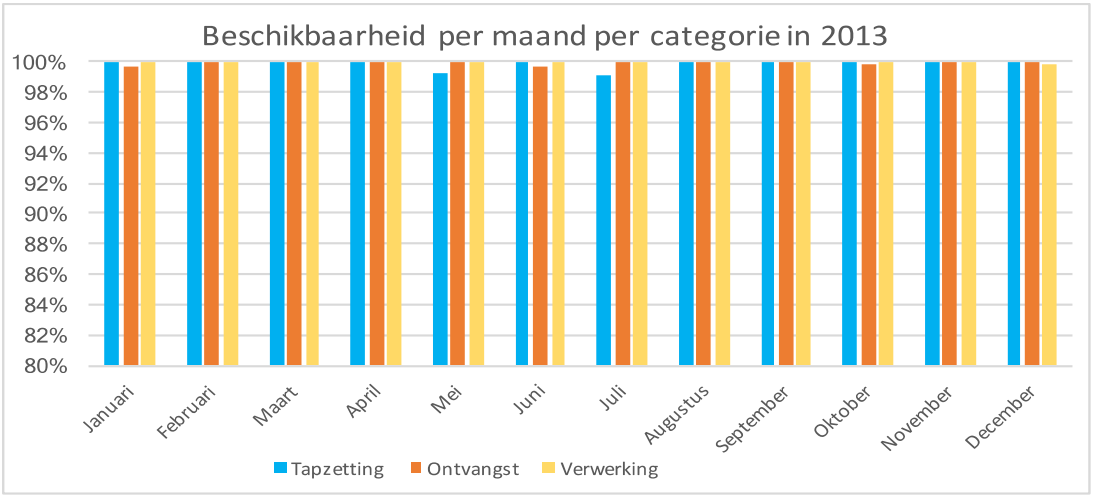
[26] Alleen met behulp van een volledige logging zou ook een betrouwbare minimale waarde voor beschikbaarheid kunnen worden berekend. Op voorwaarde dat de logging compleet is en dat alle componenten van het tapsysteem in de logging zijn opgenomen. Aangezien dat niet het geval is, is deze doorrekening niet gemaakt.

Bijlage D Beschikbaarheid tapsysteem per maand

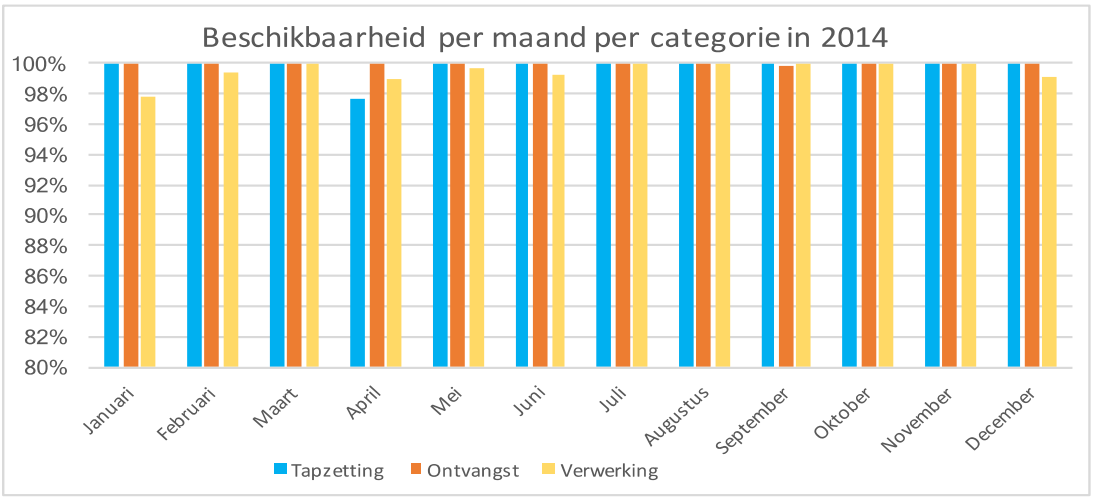
In de volgende vijf grafieken is per kalenderjaar de beschikbaarheid per maand per categorie weergegeven. ‘Opslag’ is niet opgenomen in de grafieken, omdat die over de hele periode honderd procent is gebleken.



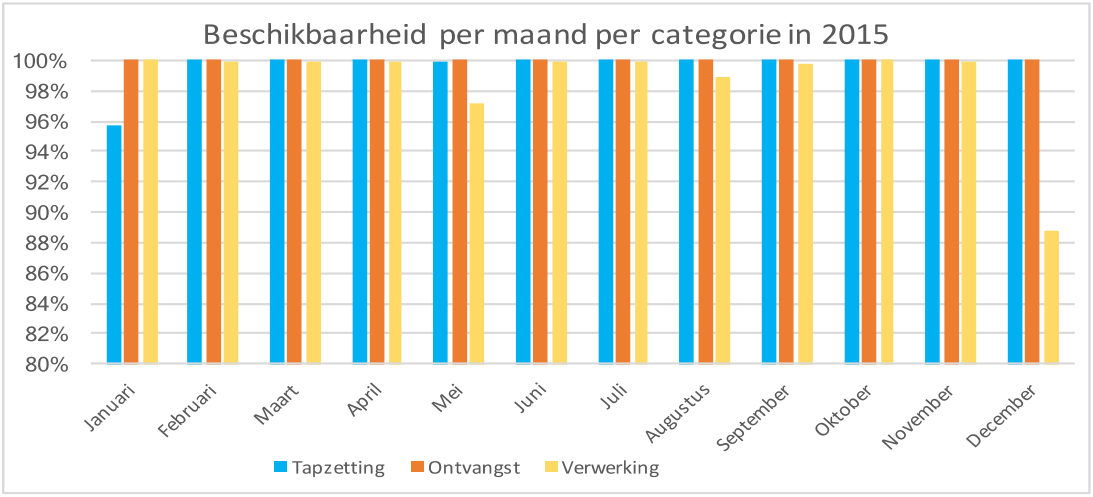
Figuur 15 - Beschikbaarheid per maand per categorie in 2012



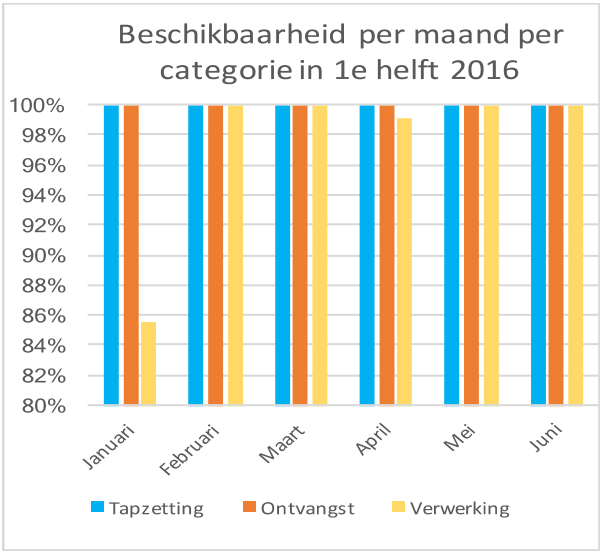
Figuur 16 - Beschikbaarheid per maand per categorie in 2013



Figuur 17 - Beschikbaarheid per maand per categorie in 2014



Figuur 18 - Beschikbaarheid per maand per categorie in 2015



Figuur 19 - Beschikbaarheid per maand per categorie in 1e helft 2016

Bijlage E Overzicht van figuren en tabellen

Figuren

Tabellen