Stratix

Onderzoek “Bewaren Verkeersgegevens door Telecommunicatie-aanbieders”

Eindrapport

Uitgebracht aan het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Justitie

Uitgebracht door:
Stratix Consulting Group B.V.

Schiphol, augustus 2003

Stratix

Samenvatting

Inleiding

De aanslagen in de Verenigde Staten op 11 september 2001 hebben voor veel overheden aanleiding gegeven de mogelijkheden om terrorisme actief te bestrijden, kritisch te bezien, en waar nodig uit te breiden. Ook in Nederland heeft de regering in dit kader een aantal acties uitgezet, samengebracht in het Actieplan Terrorismebestrijding en Veiligheid[1]. Actiepunt 17 hierin luidt:

> **Actie 17:** onderzoek verrichten naar de categorieën gegevens die telecomaanbieders bewaren en de belemmeringen die de opsporings- en I&V diensten ondervinden door de afwezigheid van bewaarplichten voor historische verkeersgegevens. Versterken van mogelijkheden van analyse van internationaal telefoonverkeer (afgestemd met Europese lidstaten).

In dit kader heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Justitie onderzoek laten doen naar een deel van deze vraagstelling, namelijk de categorieën van verkeersgegevens die door de aanbieders bewaard worden. Dit rapport presenteert de resultaten van genoemd onderzoek.

Vraagstelling

De opsporings- en veiligheidsdiensten worden in toenemende mate geconfronteerd met het feit dat verdachten gebruik maken van moderne telecommunicatiediensten. Daarmee ontstaat de noodzaak van het zoeken naar 'digitale' sporen die verdachten achterlaten bij het gebruikmaken van bijvoorbeeld internet- of telefoniediensten. Deze sporen worden, net als meer traditionele sporen, in de opsporing gebruikt om specifieke omstandigheden aan te tonen, die als bewijs of als identificatie kunnen dienen. De vraag is nu, in hoeverre aanbieders van telecommunicatiediensten dergelijke gegevens bewaren en wat de consequenties van een eventuele bewaarplicht zouden zijn.

Om inzicht te krijgen in deze materie worden de volgende specifieke vragen gesteld.

1. *Welke soorten verkeersgegevens worden door de aanbieders bewaard?*
2. *Met welk doel worden deze gegevens bewaard? Gelden daarbij (wettelijke) bewaarplichten?*
3. *Op welke wijze worden deze gegevens bewaard (opslagmethode)?*
4. *Welke soorten verkeersgegevens worden het meest gevraagd door opsporingsdiensten?*
5. *Kan in alle gevallen aan die vraag worden voldaan, zo nee, in welke gevallen niet en wat is daarvan de reden?*
6. *Indien bewaarplichten voor bepaalde soorten verkeersgegevens zouden worden uitgebreid of ingevoerd, wat zijn de gevolgen voor de systemen / bedrijfsvoering?*
7. *Wat zijn de verwachte kosten van het verplicht bewaren van (bepaalde) soorten verkeersgegevens?*

[1] Brief aan de Tweede Kamer "Terroristische aanslagen in de Verenigde Staten", Kamerstukken II 27 925, Nr. 10

Hierbij draait het uitdrukkelijk niet om gegevens betreffende de *gebruiker* van een dienst (zoals naam, adres, woonplaats), noch om de *inhoud* van de communicatie, maar om gegevens over het *gebruik* van netwerken en diensten.

Methode

Het onderzoek werd gestart met een focussessie waarin deelnemers vanuit de opsporing[2] de bepaalden voor welke telecommunicatiediensten het verkrijgen van inzicht in de beschikbaarheid van verkeersgegevens zowel belangrijk als urgent was. Als resultaat hiervan werd het onderzoek gericht op vijf diensten: vaste en mobiele telefonie, internettoegang, e-mail en toegang tot internet via internetcafés. Het onderzoek naar deze diensten is uitgevoerd aan de hand van literatuuronderzoek en gestructureerde interviews met een twaalftal aanbieders van telecommunicatiediensten: één aanbieder van vaste telefonie, drie aanbieders van mobiele telefonie, zeven ISP's, en twee internetcafés.

Bevindingen

Op basis van het onderzoek kan een kwalitatief antwoord op de onderzoeksvragen gegeven worden.

1. *Welke soorten verkeersgegevens worden door de aanbieders bewaard?*

Per dienst zijn, kort samengevat, de volgende gegevens bij de aanbieders beschikbaar:
Vaste telefonie: de onderzochte aanbieder bewaart onder andere de betrokken nummers en datum, tijd, en duur van alle geslaagde, uitgaande gesprekken. Gegevens over inkomende gesprekken vanuit andere netwerken zijn aanwezig, maar moeilijker toegankelijk. Van de niet geslaagde oproepen (onbeantwoord, of in gesprek) worden geen gegevens bewaard.
Mobiele telefonie: de onderzochte aanbieders bewaren onder andere de betrokken nummers, locatie, datum, tijd, en duur van alle geslaagde, uitgaande gesprekken. Bij SMS worden vergelijkbare gegevens bewaard, al ontbreekt in bepaalde gevallen informatie over zender of ontvanger. Gegevens over gesprekken en SMS berichten vanuit andere netwerken zijn bij twee van de drie aanbieder aanwezig. Van de niet geslaagde oproepen (onbeantwoord, of in gesprek) worden geen gegevens bewaard. Bij GPRS (een mobiele dataverbindingsdienst) worden het oproepende nummer en de gebruikte toegangsdienst bewaard, evenals de locatie, datum, tijd, en de hoeveelheid gegevens. Het gebruikte IP adres wordt niet bewaard.
Internet toegangsdienst: de meeste onderzochte ISP's bewaren gegevens van elke toegangsessie. Uit de gegevens valt te herleiden welke gebruiker op welke tijden toegang had tot het internet, en met welk IP adres. Gegevens over de computers en diensten waarmee een gebruiker contact heeft gehad worden in de meeste gevallen niet geregistreerd.
E-mail: de meeste onderzochte ISP's bewaren gegevens betreffende hun e-mail dienst. Sommige ISP's bewaren hierbij slechts het tijdstip van de laatste ophaalsessie per gebruiker, terwijl anderen de afzender, de ontvanger, en het tijdstip van verzending van elk bericht opslaan.
Internetcafés: één van de twee onderzochte internetcafés bewaart in het geheel geen gegevens; de ander bewaart sessiegegevens per werkplek. Het gebruik van internetcafés is anoniem, waardoor er geen gegevens over de gebruiker beschikbaar zijn.

[2] Deelnemers afkomstig uit PIDS, AIVD (voorheen de BVD), Politie, Openbaar Ministerie en Justitie

2. *Met welk doel worden deze gegevens bewaard? Gelden daarbij (wettelijke) bewaarplichten?*

De aanbieders registreren en bewaren verkeersgegevens voor hun bedrijfsoperatie, en met name voor de facturering van de geleverde diensten, voor de bestrijding van fraude en misbruik, voor de technische operatie, en voor de marketing.
De enige bestaande bewaarplicht betreft het anonieme (pre-paid) gebruik van mobiele telefoons, waarbij de aanbieders specifiek omschreven gegevens voor tenminste drie maanden moeten bewaren.

3. *Op welke wijze worden deze gegevens bewaard (opslagmethode)?*

De verkeersgegevens worden in eerste instantie op harde schijf bewaard, en, voor zover zij meerdere maanden bewaard worden, in veel gevallen overgebracht op CD's.

4. *Welke soorten verkeersgegevens worden het meest gevraagd door opsporingsdiensten?*

Van de onderzochte bedrijven blijken de aanbieders van telefonie veel ervaring te hebben met het vorderen van verkeersgegevens door de opsporing, terwijl Internet Service Providers (ISP's) en Internetcafés hier veel minder ervaring mee hebben. Met name bij de ISP's is er echter een toename te verwachten.
Generiek bestaan de gewenste gegevens voor alle telecommunicatiediensten uit de identiteit van de betrokken aansluitingen en gebruikers, en de datum, tijd en (indien relevant) de locatie van een sessie of gesprek. De specifieke gewenste gegevens zijn echter per telecommunicatiedienst verschillend.

5. *Kan in alle gevallen aan die vraag worden voldaan, zo nee, in welke gevallen niet en wat is daarvan de reden?*

De aanbieders van telecommunicatiediensten kunnen een groot deel van de informatie leveren waaraan de opsporingsdiensten behoefte hebben, dankzij de registratie ervan in het kader van de reguliere bedrijfsvoering.
De bewaartermijnen bij de aanbieders worden gedreven door de bedrijfsvoering en variëren van enkele dagen tot enkele maanden, of in sommige gevallen onbeperkt. De opsporingsdiensten geven aan dat om effectief gebruik te kunnen maken van verkeersgegevens, de bewaartermijn ten minste een jaar zou moeten bedragen. Naast het feit dat in veel gevallen de bewaartermijn dus korter is dan de gevraagde termijn, bestaan er nog andere belemmeringen bij het opvragen van gegevens: bepaalde verkeersgegevens zijn überhaupt niet beschikbaar of worden niet geregistreerd; gegevens gaan verloren tijdens de verwerking; en gegevens kunnen zeer moeilijk te leveren zijn als gevolg van intensieve, tijdrovende zoekopdrachten.

6. *Indien bewaarplichten voor bepaalde soorten verkeersgegevens zouden worden uitgebreid of ingevoerd, wat zijn de gevolgen voor de systemen / bedrijfsvoering?*

Om de beschikbaarheid van verkeersgegevens betrouwbaarder en homogener te maken zou een bewaarplicht of zelfs een registratieplicht ingevoerd kunnen worden. De consequenties van dergelijke maatregelen bestaan vooral uit extra investeringen en operationele kosten; een andere consequentie kan zijn dat aanbieders die zich tot nu toe profileren met een duidelijk privacybeleid, zich door een bewaarplicht minder kunnen differentiëren dan voorheen.

7. *Wat zijn de verwachte kosten van het verplicht bewaren van (bepaalde) soorten verkeersgegevens?*

De hoogte van de kosten hangt vooral af van de bewaartermijn, de gevraagde oplevertermijn, het aantal vorderingen, de complexiteit en structuur van de vragen, en de gevraagde betrouwbaarheid en beschikbaarheid. De kosten zullen per telecommunicatiedienst verschillen, gezien de grote verschillen in volume van de gegevens en het feit dat voor een aantal diensten nu al veel meer gegevens bewaard worden dan voor andere.

Tot slot

Indien besloten wordt om een bewaarplicht in te voeren zal er een functioneel geformuleerd kader opgesteld moeten worden, waarin de basisregels vastgelegd zijn. Vervolgens zullen deze regels per telecommunicatiedienst uitgewerkt moeten worden.

Binnen dit onderzoek is slechts een beperkt aantal telecommunicatiediensten onderzocht. De resultaten zijn dan ook niet zonder meer toepasbaar op andere diensten, zoals websurfen, “chat”, en file sharing.

Ten slotte is dit onderzoek primair gericht op de aanbieders. De belemmeringen die de opsporingsdiensten ondervinden door de afwezigheid van een bewaarplicht zullen, conform het eerder genoemde actiepunt, nog onderzocht moeten worden.

Stratix

Inhoudsopgave

1. Inleiding

De aanslagen in de Verenigde Staten op 11 september 2001 hebben voor veel overheden aanleiding gegeven de mogelijkheden om terrorisme actief te bestrijden, kritisch te bezien, en waar nodig uit te breiden. Ook in Nederland heeft de regering in dit kader een aantal acties uitgezet, samengebracht in het Actieplan Terrorismebestrijding en Veiligheid[3].

Actie 17 in het genoemde actieplan betreft de beschikbaarheid van historische verkeersgegevens bij de telecommunicatieaanbieders:

> **Actie 17:** onderzoek verrichten naar de categorieën gegevens die telecomaanbieders bewaren en de belemmeringen die de opsporings- en I&V diensten ondervinden door de afwezigheid van bewaarplichten voor historische verkeersgegevens. Versterken van mogelijkheden van analyse van internationaal telefoonverkeer (afgestemd met Europese lidstaten).

Dit rapport presenteert in dit kader de conclusies uit een onderzoek naar de categorieën van verkeersgegevens die door de aanbieders bewaard worden.

Aanbieders van telecommunicatienetwerken en -diensten verzamelen in hun dagelijkse operatie een schat van gegevens die voor de opsporing[4] van belang kunnen zijn. Zo registreert een telefoonnetwerk voor elk telefoongesprek onder andere de datum en tijd van het gesprek, de tijdsduur, en de nummers van betrokken abonnees. Mobiele netwerken registreren regelmatig de locatie van een ingeschakelde telefoon, ook zonder dat er een gesprek wordt gevoerd. Ook de infrastructuur van Internet Service Providers (ISP's) en andere aanbieders van elektronische diensten registreert in veel gevallen het gebruik van de aangeboden diensten.

Op 12 juli 2002 is door het Europees Parlement en de Raad van de Europese Unie richtlijn 2002/58/EG vastgesteld, betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie[5]. Deze richtlijn vervangt de bestaande richtlijn 97/66/EG, met dien verstande dat de werking is uitgebreid naar alle openbare elektronische communicatienetwerken en -diensten. De nieuwe richtlijn regelt onder andere, evenals de oude richtlijn, dat aanbieders van openbare elektronische communicatienetwerken en -diensten in principe alle verkeersgegevens dienen te wissen dan wel anoniem te maken wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie. Hierop bestaan enkele uitzonderingen; zo mogen de gegevens bewaard worden wanneer deze nodig zijn om de diensten in rekening te brengen. In dit laatste geval moeten de gegevens worden vernietigd zodra de periode verstreken is waarbinnen de klant tegen de rekening bezwaar kan maken of de betaling kan worden afgedwongen.

Door dit principe onverkort toe te passen zouden de mogelijkheden voor de opsporing om historische verkeersgegevens te verkrijgen dus beperkt worden tot hetgeen de aanbieders voor

---

[3] Brief aan de Tweede Kamer "Terroristische aanslagen in de Verenigde Staten", Kamerstukken II 27 925, Nr. 10

[4] Tenzij anders vermeld wordt onder "opsporing" steeds zowel de opsporingsdiensten als de Algemene Inlichtingen en Veiligheidsdienst (AIVD) verstaan

[5] Richtlijn betreffende privacy en elektronisch communicatie, PbEG L 101, blz. 37 e.v.

het in rekening brengen van de door hen aangeboden diensten nodig hebben. De richtlijn – zowel de huidige als de nieuwe– staat echter toe dat lidstaten (onder andere) wetgeving introduceren waardoor aanbieders alsnog verplicht kunnen worden verkeersgegevens ten behoeve van de opsporing voor een beperkte tijd te bewaren. Een dergelijke maatregel moet dan wel in overeenstemming dienen te zijn met onder andere de eisen die bijvoorbeeld uit de toepasselijke bepalingen (in het bijzonder artikel 8) van het EVRM[6] voortvloeien. Niet alleen zal aangetoond dienen te worden dat de maatregel noodzakelijk is in een democratische samenleving, maar ook zal een dergelijke maatregel dienen te voldoen aan eisen van subsidiariteit en proportionaliteit.

In opdracht van het Wetenschappelijk Onderzoek en Documentatie Centrum (WODC) van het Ministerie van Justitie heeft Stratix Consulting Group B.V. onderzoek verricht naar de situatie op de Nederlandse telecommunicatiemarkt.

Dit rapport presenteert de resultaten van het onderzoek naar de beschikbaarheid van verkeersgegevens bij aanbieders, in het bijzonder voor de diensten:

- Vaste telefonie;
- Mobiele telefonie;
- Internettoegang;
- E-mail;
- Toegang tot internet via internetcafés

Daarbij wordt ook de impact geschetst van een eventuele bewaarplicht op de betreffende aanbieders.

Het rapport is als volgt opgebouwd. De kernvraag, het kader en de gebruikte onderzoeksmethode worden in hoofdstuk twee uiteengezet. Vervolgens wordt in hoofdstuk drie de context belicht waarbinnen de kernvraag wordt gesteld. De behoefte van de opsporingsdiensten aan verkeersgegevens wordt beschreven in hoofdstuk vier. Dit vormt tezamen met de context en de vraagstelling de basis voor het veldonderzoek.

Hoofdstuk vijf geeft een algemeen overzicht van de beweegredenen van de aanbieders om gegevens te bewaren, en de redenen waarom die gegevens niet altijd beschikbaar zijn. In hoofdstuk zes zijn de bevindingen van de interviews aangaande de beschikbaarheid van verkeersgegevens voor de specifieke diensten verwerkt.

Hoofdstuk zeven beschrijft de mogelijke beleidsopties ten aanzien van een registratie en bewaarplicht, en de mogelijke consequenties hiervan. Afsluitende conclusies worden gegeven in hoofdstuk acht.

[6] EVRM: Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, waarvan artikel 8 onder andere het recht op respect voor een ieders correspondentie regelt

2. Vraagstelling

Het onderzoek, genoemd in actie 17 van het Actieplan Terrorismebestrijding en Veiligheid, omvat onderzoek naar de categorieën verkeersgegevens die telecommunicatiebedrijven bewaren.

De opsporing- en veiligheidsdiensten[7] worden in toenemende mate geconfronteerd met het feit dat verdachten gebruik maken van moderne telecommunicatiediensten. Daarmee ontstaat de noodzaak van 'digitaal rechercheren' oftewel het zoeken naar sporen die verdachten achterlaten bij het gebruikmaken van bijvoorbeeld internet- of telefoniediensten. Deze digitale sporen worden net als meer traditionele sporen in de opsporing gebruikt om specifieke omstandigheden aan te tonen, die als bewijs of als identificatie kunnen dienen.

Telecommunicatieaanbieders[8] leveren een reeks aan telefonie- en internetdiensten waar miljoenen mensen gebruik van maken. De voor deze diensten benodigde infrastructuur produceert gegevens, die een aanbieder nodig heeft voor de eigen bedrijfsvoering. De gegevens worden met name gebruikt voor het verhelpen van technische storingen, het opsporen van misbruik van de eigen diensten, het opstellen van facturen, en het afhandelen van klachten. Ook zeggen de gegevens iets over de gebruikers van de diensten, wat nuttig kan zijn voor de marketing.

Er bestaat echter onduidelijkheid over welke gegevens de telecommunicatieaanbieders precies bewaren, hoelang ze deze bewaren, en hoe goed de gegevens toegankelijk zijn. Verder is het niet duidelijk wat de invloed van een eventuele bewaarplicht op de bedrijfsvoering van de aanbieders zou zijn. Deze informatie is mede relevant om te kunnen beoordelen of het ontbreken van bewaarplichten een probleem is voor de opsporing, en om te kunnen beoordelen welke consequenties een eventuele bewaarplicht voor de aanbieders met zich mee zou brengen.

2.1 Kernvraag

Welke verkeersgegevens die voor de opsporing van belang zijn worden door de telecommunicatieaanbieders bewaard, en gedurende welke termijn; wat zouden de consequenties van een eventuele bewaarplicht zijn voor deze aanbieders?

Om inzicht te krijgen in deze materie worden de volgende specifieke vragen gesteld.

1. *Welke soorten verkeersgegevens worden door de aanbieders bewaard?*
2. *Met welk doel worden deze gegevens bewaard? Gelden daarbij (wettelijke) bewaarplichten?*

[7] Voor zover niet expliciet ander vermeld refereert het begrip "opsporing" in dit rapport aan zowel de opsporingsdiensten als de inlichtingen en veiligheidsdiensten.

[8] Voor zover niet expliciet anders vermeld refereert het begrip "telecommunicatieaanbieders" in dit rapport aan zowel netwerkaanbieders als dienstaanbieders in de zin van de Telecommunicatiewet.

3. *Op welke wijze worden deze gegevens bewaard (opslagmethode)?*
4. *Welke soorten verkeersgegevens worden het meest gevraagd door opsporingsdiensten?*
5. *Kan in alle gevallen aan die vraag worden voldaan, zo nee, in welke gevallen niet en wat is daarvan de reden?*
6. *Indien bewaarplichten voor bepaalde soorten verkeersgegevens zouden worden uitgebreid of ingevoerd, wat zijn de gevolgen voor de systemen / bedrijfsvoering?*
7. *Wat zijn de verwachte kosten van het verplicht bewaren van (bepaalde) soorten verkeersgegevens?*

Op deze vragen wordt in dit rapport een kwalitatief antwoord gegeven; gedetailleerde informatie is opgenomen in de bijlagen.

2.2 Kader en afbakening

Het onderzoek richt zich op de beschikbaarheid van historische verkeersgegevens bij vaste en mobiele telefonie, en bij drie specifieke internetdiensten: internettoegang via Internet Service Providers (ISP's), e-mail, en internettoegang via internetcafés. Gezien de grote verschillen tussen de verschillende telecommunicatiediensten in termen van volume, gebruik, en beschikbare gegevens is een dergelijke afbakening noodzakelijk. De keuze voor deze specifieke diensten is gebaseerd op de uitkomsten van een focussessie met vertegenwoordigers vanuit de opsporingsdiensten, gehouden op 26 maart 2002[9]. Daaruit bleek dat de behoefte vanuit de opsporing aan meer inzicht in verkeersgegevens bij deze telecommunicatiediensten het meest urgent is.

Het onderzoek betreft alleen verkeersgegevens. Verkeersgegevens vormen één categorie van gegevens naast gebruikersgegevens en inhoudelijke gegevens. Gegevens uit deze laatste twee categorieën vallen, evenals het op verzoek van de opsporingsdienst bewerken van gegevens, buiten dit onderzoek.

Het onderzoek beperkt zich tot een representatieve steekproef onder de aanbieders. Daarbij is de nadruk gelegd op de kwalitatieve aspecten van de onderzoeksvragen.

2.3 Onderzoeksmethode

Op 26 maart 2002 werd het onderzoek gestart met een focussessie. Hierin werden door de deelnemers, afkomstig uit PIDS, AIVD (voorheen de BVD), Politie, Openbaar Ministerie en Justitie, de hier behandelde diensten geïdentificeerd. De deelnemers gaven aan dat voor deze diensten het verkrijgen van inzicht in de beschikbaarheid van de verkeersgegevens belangrijk en urgent is in het kader van de opsporing.

Het feitelijke onderzoek is verricht aan de hand van een combinatie van literatuuronderzoek en interviewsessies. De gebruikte literatuur is te vinden in de bijlage 'Literatuurlijst'. Tevens hebben de opsporingsdiensten schriftelijke informatie aangeleverd met beschrijvingen van enkele relevante opsporingsonderzoeken uit de praktijk.

[9] Vertegenwoordigd waren naast het Ministerie van Justitie: de AIVD (Algemene Inlichtingen- en Veiligheidsdienst), KLPD (Korps Landelijke Politiediensten), en PIDS (Platform voor Interceptie Decryptie en Signaalanalyse)

Aan de hand van de literatuurstudie is een twaalftal “structured interviews” gehouden met aanbieders die verschillende vormen van de onderzochte diensten leveren. Tijdens deze interviews is met een combinatie van gesloten en open vragen gewerkt om een zo goed mogelijk beeld te krijgen; zo vroegen de onderzoekers steeds eerst in het algemeen naar beschikbare gegevens, om vervolgens specifiek te vragen naar de nog niet genoemde elementen die voor de opsporing van belang zijn.

Geïnterviewd werd steeds de persoon verantwoordelijk voor het contact met de opsporing, in de meeste gevallen vanuit de security afdeling. Waar deze persoon niet de technische kennis had werd tevens een technisch verantwoordelijke bij het interview betrokken.

2.3.1. Onderzochte aanbieders

De onderzochte aanbieders zijn gekozen op hun diversiteit als gevolg van verschillen in grootte, soorten klanten, en aangeboden diensten.

Onder de geïnterviewde partijen zijn drie mobiele telefonieaanbieders, waarvan twee grote en één kleinere, en één aanbieder van vaste telefonie. Samen vertegenwoordigen de onderzochte aanbieders meer dan 70% van de mobiele aansluitingen en vrijwel alle vaste aansluitingen.

Onderstaande tabel geeft een overzicht van de onderzochte telefonieaanbieders:

Aantal klanten	Voornaamste type klanten	Dienst	Aanduiding
+/- 7 000 000	Consument en zakelijk	Vaste telefonie	OP1
> 1 000 000	Consument en zakelijk	Mobiele telefonie	OP2
> 3 000 000	Consument en zakelijk	Mobiele telefonie	OP3
> 3 000 000	Consument en zakelijk	Mobiele telefonie	OP4

Voor wat betreft de internettoegang werden zes openbare ISP’s onderzocht, verdeeld over kleine, middelgrote, en grote bedrijven, en één niet-openbare aanbieder van internettoegang. De kleine ISP’s bedienen uitsluitend zakelijke klanten; de rest heeft zowel zakelijke als particuliere klanten. Ook wat betreft de toegangsvorm dekt het onderzoek de bestaande diversiteit af: in het onderzoek zijn ISP’s met toegang via inbelfaciliteiten, ADSL[10], kabel, en huurlijnen betrokken. Samen vertegenwoordigen deze ISP’s ongeveer 20% van de internet klanten. Daarmee geeft deze groep ISP’s een goed beeld van de industrie als geheel, zij het dat een steekproef van zeven partijen uit een populatie van iets meer dan honderd aanbieders in kwantitatief opzicht niet representatief kan zijn.

Onderstaande tabel geeft een overzicht van de onderzochte ISP’s.

Aantal klanten	Voornaamste type klanten	Type toegangsdienst				Aanduiding
		Inbel	ADSL	Kabel	Huurlijn	

[10] ADSL: Asymmetric Digital Subscriber Line, breedbandige toegang via de telefoonlijn

<10 000	Zakelijk	(✓)			✓	ISP1
<10 000	Zakelijk	✓	✓		✓	ISP3
10 000 - 100 000	Consument en zakelijk	✓	✓			ISP5
10 000 - 100 000	Consument	(✓)	(✓)	✓		ISP6
>100 000	Consument	✓	✓			ISP2
>100 000	Consument en zakelijk	✓	✓		(✓)	ISP4
>100 000 *	Instellingen	✓	(✓)		✓	ISP7

* ongeveer 150 instellingen met in totaal 450 000 gebruikers

✓ Aangeboden toegangsmethode
(✓) In mindere mate of alleen als reserve aangeboden

Naast de ISP's werden twee internetcafés onderzocht, op een populatie van enkele tientallen internetcafés:

Aantal werkplekken	**Dienst**	**Aanduiding**
300	Alleen webtoegang	IC1
30	Webtoegang, printen, floppy disk	IC2

2.3.2. Respons van de aanbieders

Van de veertien geselecteerde bedrijven weigerde één bedrijf mee te werken. Voorts bleek een aantal bedrijven, waaronder drie van de vier telefonieaanbieders, zeer terughoudend in het geven van informatie over hun netwerken en systemen. Het onderwerp van de studie wordt als controversieel ervaren, en veel van deze gegevens worden beschouwd als bedrijfsgeheim. Desondanks is voldoende respons verzameld om goed inzicht te krijgen in de beschikbare verkeersgegevens en de omgang met verkeersgegevens, waardoor de vragen 1 tot en met 6 uit de in 2.1 genoemde specifieke vragen goed beantwoord kunnen worden. Deze resultaten mogen dan ook representatief geacht worden voor de branche als geheel.

Voor wat betreft de informatie die nodig is om de consequenties van een eventuele bewaar- en/of registratieplicht (vraag 7 uit de genoemde lijst) in te schatten, reageerden de telefonieaanbieders aanzienlijk terughoudender dan de ISP's. De meeste ondervraagde ISP's gaven voldoende informatie over hun bestaande systemen om een redelijke indruk te krijgen van de architectuur van de bestaande systemen; terwijl de telefonieaanbieders hier vrijwel geen informatie over wilden geven. De voor vraag 7 gemaakte schattingen voor wat betreft de benodigde opslag voor verkeersgegevens binnen de telefonie zijn dan ook gebaseerd op de ervaring van de onderzoekers[11] en op openbaar bekende informatie. Deze schattingen zijn daardoor minder betrouwbaar dan de schattingen betreffende de ISP's.

[11] De onderzoekers zijn in het verleden bij diverse implementatieprojecten van verwerkingssystemen voor verkeersgegevens bij telefonieaanbieders betrokken geweest, waardoor zij een op ervaring gebaseerde schatting konden maken.

3. Context

Voor een adequate beantwoording van de onderzoeksvraag is het noodzakelijk de achtergrond te schetsen. Deze schets start met een korte uiteenzetting over het begrip verkeersgegeven, gevolgd door een korte beschrijving van de specifieke onderzochte telecommunicatiediensten en van de aanbieders van deze diensten.

3.1 Scope: wat is een verkeersgegeven

De discussie rond historische verkeersgegevens is niet nieuw. Aspecten ervan kwamen naar voren in het rapport "Opsporing Locaties Verzocht"[12] en het rapport van de commissie Mevis[13]. In 2001 werd het wetsvoorstel "Vorderen Gegevens Telecommunicatie"[14] aan de Tweede Kamer aangeboden; dit voorstel beoogt het juridisch kader te verduidelijken en uit te breiden. Het wetsvoorstel is in mei 2003, in gewijzigde vorm, door de Tweede Kamer aangenomen.

Dit rapport beperkt zich tot *verkeersgegevens*, waarmee in dit verband gegevens betreffende het gebruik van netwerken en diensten bedoeld worden. Verkeersgegevens worden daarmee onderscheiden van *gebruikersgegevens*, dat wil zeggen gegevens omtrent de gebruiker van de dienst (zoals naam, adres, woonplaats, nummer, en geabonneerde dienst), en van de *inhoud* van de communicatie.

In het wetsvoorstel Vorderen Gegevens Telecommunicatie wordt de term verkeersgegevens anders gebruikt. In dat voorstel worden verkeersgegevens omschreven als "gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker". Dat wil zeggen, de uiterlijke kenmerken van telecommunicatie en niet de inhoud. Zij kunnen volgens dit voorstel worden opgevraagd door een officier van justitie[15], of door één van de hoofden van de Inlichtingen en Veiligheidsdiensten[16]. Deze definitie van het begrip verkeersgegevens in het voorstel omvat, naast de in dit rapport gehanteerde betekenis van verkeersgegevens, ook de hierboven genoemde *gebruikersgegevens*. Het wetsvoorstel bevat overigens ook artikelen aan de hand waarvan een opsporingsambtenaar alleen *gebruikersgegevens* op kan vragen[17]. Het wetsvoorstel schrijft verder voor dat bij Algemene Maatregel van Bestuur de (verkeers)gegevens aangewezen worden die bij de aanbieders gevorderd kunnen worden.

In de eerder genoemde Europese Richtlijn 2002/58/EG worden verkeersgegevens gedefinieerd als "gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan". Verder geeft overweging 15 van de richtlijn enkele voorbeelden van verkeersgegevens: *"Verkeersgegevens kunnen o.a. gegevens zijn met betrekking tot de routering, de duur, het tijdstip of het volume van een*

[12] "Opsporing Locaties Verzocht", Research voor Beleid, Leiden, 2001

[13] "Gegevensvergaring in strafvordering", Rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, Mei 2001

[14] Wetsvoorstel "Vorderen Gegevens Telecommunicatie", Kamerstukken II 28 059, Nr. 1

[15] Wijziging van artikelen 126n en 126u Wetboek van Strafvordering

[16] Wijziging van artikel 27 Wet op de Inlichtingen- en Veiligheidsdiensten 2002

[17] Nieuwe artikelen 126na en 126ua Wetboek van Strafvordering

communicatie, het gebruikte protocol, de locatie van de eindapparatuur van de verzender of de ontvanger, het netwerk waarop de communicatie begint of eindigt, het begin, het einde of de duur van de verbinding; ze kunnen ook bestaan in het formaat waarin een communicatie door het netwerk wordt overgebracht."

Duidelijk is dat per telecommunicatiedienst verschillende verkeersgegevens van toepassing kunnen zijn. Zo is het begrip "gespreksduur" niet relevant voor SMS[18] of e-mail, en is het begrip "locatie" slechts een verkeersgegeven waar het mobiele diensten betreft, aangezien de locatie bij vaste diensten een gebruikersgegeven is.

3.2 Achtergrond onderzochte diensten

3.2.1. Vaste telefonie

Onder vaste telefonie wordt verstaan de telefoniediensten die gebruik maken van een vast netwerk tot aan de aansluiting van de gebruiker. Belangrijkste voorbeeld is het fijnmazige kopernetwerk dat geëxploiteerd wordt door KPN Telecom, maar ook telefoniediensten via glasvezelaansluitingen en via het kabelnetwerk vallen hieronder.

Binnen de vaste telefonie worden zowel analoge aansluitingen (PSTN, Public Switched Telephone Network) als digitale (ISDN, Integrated Services Digital Network) geleverd. In tegenstelling tot wat deze benamingen suggereren gaat het hierbij niet om gescheiden netwerken, maar om verschillende typen aansluitingen en de bijbehorende dienstverlening.

Op PSTN aansluitingen kan de gebruiker naast telefoons ook fax apparaten, modems, en andere apparatuur aansluiten. Voor de aanbieder is zonder de aansluiting af te tappen niet vast te stellen voor welk type apparatuur de aansluiting gebruikt wordt. Bij ISDN aansluitingen is dat anders: afhankelijk van het type apparatuur en de gebruikte dienst kan de telefooncentrale een indicatie geven dat bijvoorbeeld een dataverbinding of een spraakverbinding opgezet wordt.

Verkeersgegevens in de vaste telefonie worden voornamelijk gegenereerd door de telefooncentrale waarop de gebruiker is aangesloten. Daarnaast worden verkeersgegevens gegenereerd door telefooncentrales waarmee het netwerk gekoppeld is aan andere aanbieders, en door systemen voor toegevoegde waarde diensten zoals voice-mail.

3.2.2. Mobiele telefonie

Mobiele telefonie wordt in Nederland aangeboden op basis van de internationale GSM[19] standaard. Naast de zogenaamde circuitgeschakelde diensten, waaronder spraak, bieden de GSM netwerken ook andere diensten zoals SMS en sinds kort ook GPRS[20]. Met GPRS zijn datatoepassingen zoals mobiel internet (waaronder i-mode en WAP), chatten, en het versturen van multimedia berichten (MMS[21]) beter mogelijk dan voorheen.

---

18 SMS: Short Message Service, de berichtendienst binnen GSM

19 GSM: Global System for Mobile telecommunication

20 GPRS: General Packet Radio System, een pakketgeschakelde dienst binnen de GSM standaard

21 MMS: Multimedia Messaging Service, een op GPRS gebaseerde berichtendienst voor tekst, plaatjes, en geluid.

In de toekomst voorzien de aanbieders nog meer ontwikkeling richting datadiensten. Met name UMTS en Pre-Paid GPRS zullen op termijn bij alle aanbieders in het dienstenpakket aanwezig zijn.

Verkeersgegevens in de mobiele telefonie worden door een groot aantal elementen in het netwerk gegenereerd. De telefooncentrales leveren gegevens over circuitgeschakelde diensten, mobiliteit, en een deel van de gegevens over SMS; andere elementen leveren gegevens over GPRS, en aanvullende gegevens over SMS en over het gebruik van toegevoegde waarde diensten.

Een belangrijk onderscheid in de manier waarop mobiele telefonie wordt aangeboden is de wijze van betaling: pre-paid of post-paid. Bij pre-paid betaald de eindgebruiker vooruit voor de te gebruiken diensten, terwijl bij post-paid deze betaling achteraf plaats vindt. Juist deze verschillende manieren van afrekenen bepalen voor een groot deel welke gegevens beschikbaar zijn en hoe deze geregistreerd en bewaard worden. In het geval van pre-paid heeft de aanbieder voor wat de afrekening betreft geen belang bij het bewaren van verkeersgegevens. De dienst is immers reeds betaald. Bij post-paid betaalt de klant achteraf, en moet de operator dus verkeersgegevens verzamelen en in rekening brengen. Ook gebruikersgegevens zijn alleen bij post-paid nodig voor de bedrijfsvoering.

3.2.3. Internettoegang

De meest bekende vorm van dienstverlening door ISP's is de internettoegang. De toegang wordt tegenwoordig via een groot aantal technologieën geleverd: via huurlijnen, door inbellen vanuit PSTN, ISDN of GSM, via kabelmodems, ADSL[22], W-LAN's[23], en GPRS.

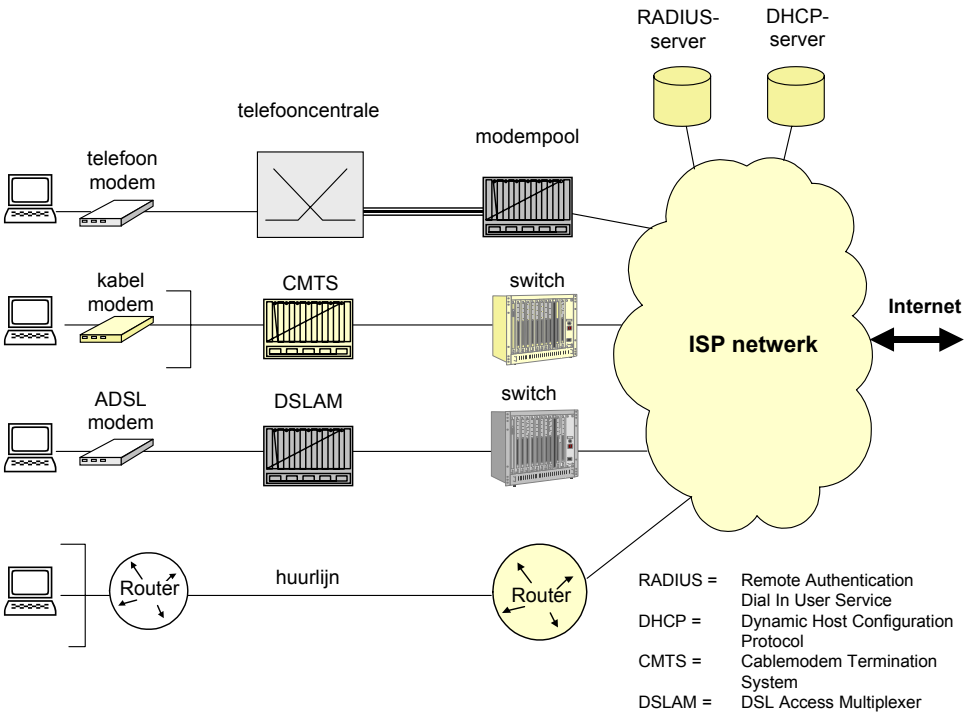
Op dit moment, eind 2002, wordt in Nederland vanaf ongeveer 3 miljoen telefoonaansluitingen tenminste één keer per maand verbinding gezocht met internet. Daarnaast zijn er iets meer dan een miljoen aansluitingen die toegang tot internet geven via kabelmodem en ADSL, en enkele tienduizenden bedrijven die via huurlijnen direct aangesloten op internet zijn aangesloten.

De klassieke internet-aansluiting, zoals in de zakelijke markt gebruikt, is een directe verbinding met een vast IP adres via een huurlijn naar een ISP. Tegenwoordig gebruiken veel kleine bedrijven ADSL; ook hier wordt in het algemeen een vast IP adres verstrekt. In de consumentenmarkt bieden de ISP's hun klanten meestal geen vast IP adres, maar krijgt de klant per toegangssessie een adres toegewezen. Na afloop van de sessie is dit adres weer voor andere klanten beschikbaar.

Figuur 1 geeft schematisch de meest gangbare wijzen van toegang tot internet via een ISP weer.

[22] ADSL: Asymmetric Digital Subscriber Line, een techniek voor snelle dataverbindingen via de telefoonlijn

[23] W-LAN: Wireless Local Area Network, ook als WiFi of 802.11 aangeduid: een techniek om op korte afstanden snelle draadloze datanetwerken op te zetten.



Figuur 1 Architectuur van populaire vormen van internettoegang

Bij toegang via de modempool (PSTN, ISDN, of GSM), dient een gebruiker in te loggen en worden user-ID en password door een RADIUS[24] server gecontroleerd. Deze server genereert sessiegegevens die gelogd kunnen worden. Op kabelnetten en bij ADSL-toegang wordt soms ook RADIUS ter authenticatie gebruikt; in andere gevallen geeft de DHCP[25] server automatisch een IP adres af, zonder authenticatie van de gebruiker. In dit geval is er geen sprake van een user-ID of password; wel kan de DHCP server andere gegevens over de toegangssessie registreren. Bij toegang via huurlijnen is er geen sprake van een toegangssessie, aangezien de toegang permanent beschikbaar is.

In principe is het mogelijk het IP verkeer over de toegangsdienst te registreren in de vorm van *IP Accounting*. Dit houdt in dat over bepaalde tijdsintervallen (bijvoorbeeld elke 5 minuten) een lijst gemaakt wordt van alle combinaties van IP bron- en bestemmingsadressen, samen met het aantal getransporteerde bytes. Zo is na te gaan welke computer binnen dat tijdsinterval met welke andere computer contact heeft gehad.

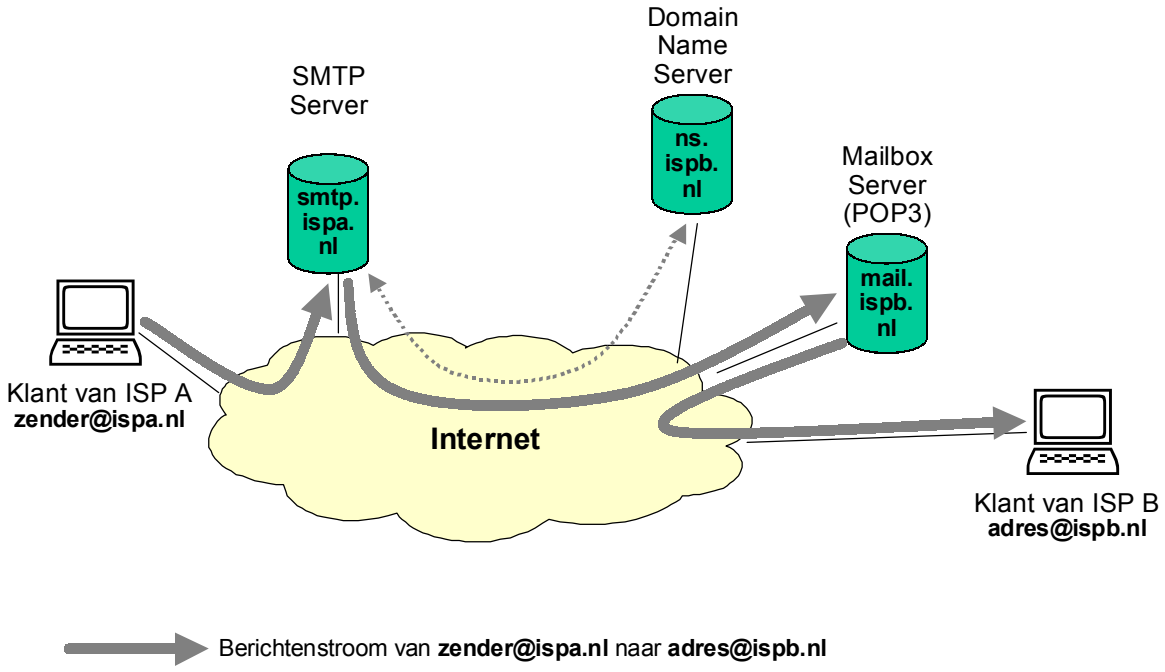
3.2.4. E-mail dienstverlening

De andere vorm van internet dienstverlening die naast de toegang is onderzocht is e-mail. Via e-mail kunnen gebruikers tekstberichten en andere gegevens uitwisselen met iedere andere gebruiker met een postbus die via het internet bereikbaar is.

[24] RADIUS: Remote Access Dial In User Service, een standaard voor authenticatie en autorisatie bij externe toegang tot een datanetwerk

[25] DHCP: Dynamic Host Configuration Protocol, een protocol voor het toewijzen van toegangsparameters binnen een netwerk

Figuur 2 geeft een voorbeeld van de eenvoudigste opzet weer, waarbij een klant van ISP A een e-mail stuurt aan een klant van ISP B, met het e-mail adres "adres@ispb.nl". Een uitgaande mail wordt verstuurd naar de SMTP[26] server van ISP A, met de domeinnaam **smtp.ispa.nl**. Via het domeinnaam systeem (DNS) wordt door deze server de naam van de Mailbox Server en het bijbehorende IP adres van **ispb.nl** opgevraagd. Daarna wordt het bericht direct doorgestuurd naar die server (hier **mail.ispb.nl**), die het ontvangt en in de mailbox *adres* plaatst, waarvandaan de ontvanger het bericht via het Post Office Protocol (POP3) op kan vragen.



Figuur 2 E-mail berichtenstroom

Overigens hoeven –in dit voorbeeld– de aanbieders ISP A en ISP B geen van beide bij de *toegangsdienst* betrokken te zijn. De zender en de ontvanger van het bericht kunnen via geheel andere aanbieders toegang tot het internet krijgen, en via die toegang verbinding maken met respectievelijk de SMTP Server en de Mailbox Server. De verkeersgegevens betreffende de toegang bevinden zich dan bij andere aanbieders dan de verkeersgegevens betreffende e-mail.

E-mail dienstverlening wordt door ISP's in veel variëteiten aangeboden: van een eenvoudige dienst zoals hierboven geschetst, tot complexe opstellingen voor virusfiltering en het blokkeren van ongewenste (commerciële) e-mail (ook bekend als spam) en web-based mailtoegang. In dat geval staat er vaak ook een groot aantal systemen opgesteld, die bovendien elkaars functie bij storingen kunnen overnemen. Bij het onderzoeken van de beschikbaarheid van verkeersgegevens uit e-mail systemen zijn partijen geïnterviewd met zowel een eenvoudige als een zeer uitgebreide e-mail dienstverlening.

[26] SMTP: Simple Mail Transfer Protocol, het meest gebruikelijke protocol om e-mail berichten door te geven

3.2.5. Toegang via internetcafés

Internetcafés bieden tegen betaling een werkplek, doorgaans een PC, met als belangrijkste dienst toegang tot het internet. Hierbij wordt gebruik gemaakt van de bovengenoemde toegangstechnieken.

Het aspect dat het internetcafé tot een apart onderwerp maakt is echter de manier waarop de dienst aan de klanten wordt aangeboden. Het café is vrij toegankelijk en er wordt doorgaans niet gecontroleerd op identiteit, waardoor de klant anoniem is. De klant huurt een werkplek voor een bepaalde tijd, van waaruit hij het publieke internet op kan. Hiertoe krijgt de klant een tijdelijk user-ID en logt daarmee in op een willekeurige PC. Nadat de klant de sessie heeft afgerond is de werkplek beschikbaar voor een volgende klant.

Onder de klanten van internetcafés vindt men toeristen maar ook buurtbewoners die het gezellig vinden om enige tijd in een internetcafé door te brengen, of die behoefte hebben aan een snelle verbinding. Soms kan er nog gebruik gemaakt worden van additionele diensten zoals printen, of data naar CD's schrijven. Internetcafés variëren in grootte van enkele tot honderden werkplekken.

De anonieme toegang zoals hier beschreven vindt men niet alleen bij internetcafés maar ook op andere publiek toegankelijke plaatsen waar toegang tot internet wordt aangeboden. Voorbeelden hiervan zijn openbare bibliotheken, scholen en universiteiten.

3.3 Achtergrond aanbieders

3.3.1. Marktstructuur

Tot aan het begin van de jaren negentig was de markt voor telefoniediensten een monopolistische. Het voormalige staatsbedrijf PTT Telecom, inmiddels KPN geheten, had het alleenrecht op het leveren van telefonie.

Met de opkomst van GSM is de markt voor mobiele diensten vrijgegeven. De overheid verstrekte aanvankelijk licenties aan één mobiele operator naast het bestaande KPN, en later nog aan drie anderen. Daarnaast zijn er in Nederland nog enkele Service Providers dan wel Mobile Virtual Network Operators (MVNO's), die gebruik maken van het netwerk van één van deze vijf aanbieders.

Sindsdien is ook de markt voor vaste telefoniediensten vrijgegeven. Aanbieders kunnen telefoniediensten leveren door zelf klanten aan te sluiten, bijvoorbeeld via glasvezels of via de kabel, maar zij kunnen ook het kopernetwerk van KPN gebruiken om diensten te leveren. Evenals in de mobiele telefonie zijn er aanbieders zonder eigen netwerk, die de diensten van een ander netwerk verkopen.

Op de markt voor internetdiensten is er sprake van vrije concurrentie. Er zijn dan ook meer dan honderd bedrijven in Nederland die toegang tot internet leveren, de zogenaamde Internet Service Providers (ISP's). De meeste ISP's leveren naast toegang ook aanvullende diensten, zoals e-mail, domeinnaamregistratie, webhosting etc. Verder zijn er bedrijven die zich alleen richten deze aanvullende diensten.

3.3.2. Omgang met verkeersgegevens

De telefonieaanbieders hanteren strakke regels waar het gaat om de beveiliging van gegevens en de toegang tot die gegevens. Zij hebben een ver doorgevoerde functiescheiding binnen het bedrijf, en beperken de toegang tot gegevens zoveel mogelijk tot die personen die de gegevens voor hun functie nodig hebben (*need-to-know*). Dit geldt in het bijzonder voor gevoelige gegevens, waaronder verkeersgegevens.

ISP's geven in het algemeen de voorkeur aan het principe van *need-to-withhold*[27]. Deze voorkeur wordt in belangrijke mate gevoed door de snelle ontwikkeling van de internet techniek, en door de relatief beperkte omvang van deze bedrijven en daardoor sterke interne sociale controle. Onder de motorkap kunnen kijken is bij deze stand van zaken van technologie en markt een must. Men kiest er bij ISP's bewust voor intern open met informatie om te gaan. Onder het motto "twee weten meer dan één" en de noodzaak tot flexibele interne vervanging hebben veel medewerkers toegang tot de verschillende systemen. Verkeersgegevens zijn dan ook voor veel medewerkers toegankelijk.

3.3.3. De keten van faciliteiten

Aanbieders maken veelvuldig gebruik van de faciliteiten van andere aanbieders. Een internet gebruiker belt bijvoorbeeld vanaf zijn vaste aansluiting van KPN, via verkeerscentrales van Worldcom, naar een nummer op een modempool bij UUnet. Die routeert het verkeer naar het netwerk en de e-mail servers van een ISP. Deze apparatuur kan echter ook weer volledig ingehuurd zijn bij verschillende derden. In dit voorbeeld heeft de gebruiker alleen een contractuele relatie met KPN en met de ISP, terwijl alle andere partijen een directe of indirecte relatie met de ISP hebben. Zo ontstaat er een "keten van faciliteiten" die bijvoorbeeld de ISP, de houder van de modembanken, en de telecomaanbieder van deze partij omvat.

Vooral in het 'gratis internet' segment zijn er Virtuele ISP's; bedrijven die zich volledig op de verkoop van hun diensten concentreren en geheel geen eigen infrastructuur hebben. Zij ontvangen veelal een zeer beperkte verzameling verkeersgegevens van de bezitters van de netwerkapparatuur en servers. Als uiteindelijke aanbieder van de dienst zijn zij echter wel degenen aan wie de opsporingsdiensten zich wenden om verkeersgegevens op te vragen.

De mobiele telefonieaanbieders hebben in Nederland ieder een eigen netwerk aangelegd. *Roaming* tussen Nederlandse partijen onderling komt dan ook niet meer voor; wel hebben de aanbieders afspraken met buitenlandse partijen om elkaars klanten te bedienen wanneer deze in een ander land zijn. Die partijen sturen in dat geval de bijbehorende verkeersgegevens aan de oorspronkelijke aanbieder.

Als gevolg van de financiële druk die de mobiele telefonieaanbieders op dit moment ervaren is het gezamenlijk aanleggen van de nieuwe UMTS netwerken wel actueel. Hierdoor kan een situatie ontstaan waarbij ook binnen Nederland de netwerkaanbieders voor hun verkeersgegevens van elkaar afhankelijk worden.

---

[27] Need to withhold: alleen als er goede reden is om aan iemand informatie te onthouden wordt deze voor hem afgeschermd

3.3.4. De keten van diensten

Naast deze “keten van faciliteiten”, waarbij er altijd één partij aanspreekbaar is aangezien deze de uiteindelijke dienst aanbiedt, is er sprake van een door de klant zelf opgezette “keten van diensten”: de gebruiker neemt een telefoniedienst af van bijvoorbeeld KPN, een toegangsdienst van een ISP, een e-maildienst van weer een andere ISP, om vervolgens via die e-maildienst weer andere diensten bij andere partijen te bestellen. In dit geval heeft de gebruiker een relatie met ieder van de aanbieders in de keten, en kunnen de opsporingsdiensten elk van die aanbieders aanspreken voor verkeersgegevens omtrent de door die aanbieder geleverde dienst. Bij zogenaamde Peer-to-Peer diensten, zoals de file sharing dienst KaZaA, wordt de dienst bovendien niet door een aanbieder maar door een eindgebruiker “geleverd”.

Ook de zogenaamde *content* diensten binnen de telefonie, zoals de 0900 diensten en de betaalde SMS diensten, worden grotendeels door andere spelers geleverd. Daarnaast kan de gebruiker van een vast telefonienetwerk er voor kiezen een deel van de telefoniedienst bij een andere partij af te nemen via de Carrier Select dan wel Carrier Pre-Select dienst. Ook hier ontstaat dus een “keten van diensten”.

4. Behoefte van de opsporing

4.1 Algemeen

In de gesprekken met vertegenwoordigers van de opsporingsdiensten werd duidelijk dat het opvragen van verkeersgegevens een onmisbaar element binnen de moderne opsporing is. In een groot deel van de onderzoeken naar misdrijven worden dergelijke gegevens opgevraagd en gebruikt. Ook voor het inlichtingen- en veiligheidswerk zijn dergelijke gegevens relevant.

Deze praktijk is in de laatste jaren zeer snel gegroeid. Hierbij gaat het in de meeste gevallen om traditionele misdaad, ook wel 'old crimes' genoemd. Onder 'new crimes' verstaat men die misdrijven die zijn ontstaan en plaatsvinden in het domein van de nieuwe technologie. Enkele voorbeelden, genoemd door opsporingsdiensten, zijn:

- Voorbeelden van *'Old Crimes'*: belastingfraude, handel met voorkennis, BTW – carrousel, douanefraude, bedreiging, moord, kinderpornografie, oplichting, drugszaken, wapenhandel;
- Voorbeelden van *'New Crimes'*: digitale heling, hacking, virusverspreiding.

De behoefte van opsporingdiensten aan verkeersgegevens komt voort uit de algemene behoefte aan gegevens die voor elk justitieel onderzoek van toepassing is. In algemene termen stellen de opsporingsdiensten vragen bij aanbieders van telefoniediensten en internetdiensten die beginnen met: wie, wat, hoe, waar, en wanneer. Enkele voorbeelden van verkeersgegevens, gerelateerd aan de eerder genoemde telecommunicatiediensten, zijn:

- Welke personen heeft de verdachte in de afgelopen week gebeld?
- Wat is het nummer van de verdachte die op tijdstip X vanaf locatie Y naar persoon Z belde?
- Wie stuurde aan de verdachte op die datum een e-mail? Wanneer heeft hij voor het laatst zijn e-mail benaderd?
- Wie had er op die datum toegang tot internet vanaf die aansluiting, en wat deed die persoon op dat moment via die toegang?

De antwoorden die gegeven worden dankzij verkeersgegevens leveren daarmee sporen op die informatie bieden over de omstandigheden en de verdachte(n) inzake een gepleegd misdrijf of dreiging van een misdrijf . Hierbij moet men ook denken aan het opstellen van daderprofielen en het identificeren van een *modus operandi*. Dergelijk recherche werk kan als bewijsmateriaal fungeren, maar het kan ook leiden tot nieuwe acties in een onderzoek zoals het aftappen van e-mail of telefonie.

Elke telecommunicatiedienst heeft een eigen verzameling attributen, die als verkeersgegeven geregistreerd kunnen worden, en waarmee deze vragen mogelijk beantwoord kunnen worden. In het algemeen gaat het daarbij ten minste om een identiteit ten behoeve van de dienst (bijvoorbeeld een telefoonnummer of een user-ID), een aansluiting op een onderliggende dienst (bijvoorbeeld een IP adres), de bestemming, de datum en tijd, de locatie van de gebruiker (voor GSM/GPRS) op basis van de betrokken antennesector, en de gebruikte dienst.

Gegevens betreffende de gebruiker zelf (naam, adres en woonplaats gegevens) zijn eveneens van belang voor de opsporingsdiensten, maar behoren tot de *gebruikersgegevens* en niet tot de *verkeersgegevens*; deze gegevens vallen daarom buiten het kader van dit onderzoek.

4.2 Benodigde bewaartermijn en snelheid van levering

De termijn waarbinnen de opsporingsdiensten historische verkeersgegevens nodig kunnen hebben hangt af van de aard van het onderzoek. De opsporingsdiensten geven aan dat om effectief gebruik te kunnen maken van dergelijke gegevens, de bewaartermijn minimaal een jaar moet bedragen[28]. In een deel van de zaken zou drie maanden al voldoende kunnen zijn, maar vaak is een langere termijn nodig, in sommige gevallen zelfs van meerdere jaren.

De benodigde termijn wordt vooral veroorzaakt door de tijd die vaak tussen misdrijf en onderzoek ligt. Daar komt bij dat de opsporing met name bij internet diensten vaak een spoor langs verschillende aanbieders terug moet volgen; om een bepaalde handeling terug te kunnen herleiden tot een gebruiker zijn vaak gegevens van een aantal partijen in de keten van diensten nodig, waarbij de gegevens van iedere partij weer naar een volgende stap in de keten verwijzen. Als ieder van deze partijen een aantal werkdagen nodig heeft om te reageren, kan het enige tijd duren voordat de laatste partij in de keten gevonden is.

De opsporingsdiensten geven aan dat de snelheid waarmee verkeersgegevens beschikbaar te maken moeten zijn varieert met de mate van urgentie in een opsporingszaak. Vertegenwoordigers vanuit de opsporing gaven aan in spoedeisende gevallen zoals gijzelingszaken de gegevens binnen 24 uur te willen hebben, terwijl voor een regulier onderzoek 72 uur nog acceptabel is[29]. In beide gevallen wil men de gegevens in een elektronisch formaat.

De voor de opsporing relevante verkeersgegevens voor de onderzochte telecommunicatie-diensten worden hieronder omschreven; in Bijlage B zijn deze gegevens in detail opgenomen, en in Bijlage D uitgezet tegen de beschikbare gegevens.

4.3 Benodigde gegevens

4.3.1. Vaste telefonie

Met betrekking tot de vaste telefonie zijn de volgende verkeersgegevens relevant voor de opsporing:

- Identiteit van de aansluiting: dit is het telefoonnummer (ook wel A-nummer of CLI[30]);
- Identiteit van de bestemming: het telefoonnummer van degene die men belt (ook wel het B-nummer);
- Het type dienst: zoals spraak, fax, of data (niet mogelijk bij PSTN[31]);

[28] Resultaat van de focussessie met vertegenwoordigers vanuit de opsporingsdiensten, gehouden op 26 maart 2002
[29] Resultaat van de focussessie met vertegenwoordigers vanuit de opsporingsdiensten, gehouden op 26 maart 2002
[30] CLI: Calling Line Identity, het telefoonnummer van de beller

- Datum / tijd / duur van de verbinding: Gegevens omtrent de start en eindtijd van een gesprek;
- Status van de verbinding: is het gesprek beantwoord, is deze normaal beëindigd en door wie is deze beëindigd.

Deze gegevens zijn relevant voor gesprekken van en naar de gebruiker, en voor zowel beantwoorde als onbeantwoorde oproepen.

4.3.2. Mobiele telefonie

Verkeersgegevens met betrekking tot GSM zijn sterk verschillend afhankelijk van de gebruikte dienst. In het volgende worden de relevante verkeersgegevens aangegeven voor mobiele telefonie (spraak en circuitgeschakelde data), voor GPRS, en voor SMS.

GSM algemeen

Met betrekking tot mobiele telefonie op basis van GSM zijn de volgende verkeersgegevens relevant voor de opsporing:

- De identiteit van de aansluiting: het telefoonnummer, ook wel MSISDN[32], en de daaraan gekoppelde unieke identiteit IMSI[33] op de SIM[34]-kaart
- De identiteit van het gebruikte toestel, IMEI[35]
- De datum / tijd / duur: begin en eindtijd van een communicatiesessie
- De locatie van de oproeper tijdens een sessie.
- Status van de sessie: Beantwoord of niet beantwoord, reden tot afbreken van de sessie (ook wel *cause for release*)
- De bestemming van de oproep:
  - Telefoonnummer van de bestemming (B-nummer),
  - In het geval van een oproep naar een mobiel toestel: de IMSI, IMEI, en locatie van de bestemming
- Type dienst: Spraak, fax, SMS, MMS, GPRS, etc (Teleservice/bearer service)

Deze gegevens zijn relevant voor gesprekken van en naar de gebruiker, en voor zowel beantwoorde als onbeantwoorde oproepen.

GPRS

Voor datadiensten via GPRS zijn de volgende verkeersgegevens relevant voor wat betreft de toegangssessie:

- De identiteit van de aansluiting: het telefoonnummer, ook wel MSISDN, en de daaraan gekoppelde unieke identiteit IMSI op de SIM-kaart

---

[31] Bij PSTN, oftewel de “gewone” analoge telefoniedienst, is voor de aanbieder niet na te gaan of de verbinding voor spraak, data, of fax gebruikt werd. Bij een verbinding tussen twee ISDN aansluitingen kan dit in principe wel, maar het hangt af van manier waarop de dienst gebruikt werd.

[32] MSISDN: Mobile Station International Subscriber Directory Number, oftewel het gebruikte telefoonnummer van de mobiele aansluiting

[33] IMSI: International Mobile Subscriber Identity, identiteit op de SIM kaart. Identificeert een mobiele aansluiting.

[34] SIM: Subscriber Identity Module

[35] IMEI: International Mobile Equipment Identity

- De identiteit van het gebruikte toestel, IMEI
- Sessie: toegekend IP adres;
- Het APN[36]. Aangezien verschillende APN's gebruikt kunnen worden voor bijvoorbeeld een koppeling met het openbare internet, de WAP gateway of een directe verbinding met het bedrijfsnetwerk, geeft het APN enige informatie over het type dienst tijdens een GPRS sessie;
- Datum / tijd / duur / locatie: begintijd, eindtijd van de datasessie; en de locatie op deze tijdstippen;
- Volume: hoeveelheid ingaande en uitgaande data.

Voor wat betreft de eigenlijke *communicatie* tijdens de toegangssessie hebben de diensten behoefte aan de volgende gegevens:

- Identiteit van de bron: het IP adres of de naam van de computer waarvandaan de gegevens kwamen;
- Identiteit van de bestemming: het IP adres of de naam van de computer waar de gegevens naar toe gingen;
- Type dienst: de dienst die via de verkregen toegang afgenomen werd;
- Datum / tijd en tijdsduur van het gebruik van de afgenomen dienst.

SMS

Verkeersgegevens die voor SMS relevant zijn:

- De identiteit van de aansluiting: het telefoonnummer, ook wel MSISDN, en de daaraan gekoppelde unieke identiteit IMSI op de SIM-kaart
- De identiteit van het gebruikte toestel, IMEI
- Bestemming: gebruikte SMSC[37], B-nummer, IMSI, IMEI;
- Volume: aantal tekens in SMS;
- Tijdstip van verzending;
- Tijdstip van ontvangst;
- Locatie bij verzending / ontvangst.

Ook deze gegevens zijn relevant voor berichten van en naar de gebruiker.

4.3.3. Internettoegang

Verkeersgegevens met betrekking tot de toegangsdienst zijn onder te verdelen in gegevens die iets zeggen over de *toegangssessie* en gegevens die iets zeggen over de eigenlijke *communicatie*.

De opsporingsdiensten geven aan dat zij voor wat betreft de *toegangssessie* de volgende verkeersgegevens nodig hebben:

- De identiteit van de aansluiting: dit kan een telefoonnummer zijn, een poortnummer, een IMSI, of een ander gegeven waarmee de aansluiting van de gebruiker geïdentificeerd kan worden;

[36] APN: Access Point Name, identificeert de bestemming voor alle data vanaf een mobiel apparaat, waar vandaan de koppeling wordt gemaakt met de eindbestemming

[37] SMS Service Centre, de server die SMS berichten doorstuurt naar de bestemming

- De identiteit van de gebruiker: een aantal toegangsdiensten gaat uit van een user-ID, die aan bijbehorende gebruikersgegevens gekoppeld kan worden;
- Het IP adres: dit is in de meeste gevallen een tijdelijk adres voor de duur van een sessie. Dit adres, in combinatie met datum en tijd, maakt het mogelijk de sessiegegevens te koppelen aan dienstgegevens, ook als de dienst door een andere aanbieder wordt geleverd;
- Datum / tijd en tijdsduur van de sessie;
- Volume: het totale aantal bytes en/of packets dat gedurende de sessie van en naar de gebruiker getransporteerd werd.

Voor wat betreft de eigenlijke *communicatie* tijdens de toegangssessie hebben de diensten behoefte aan de volgende gegevens:

- Identiteit van de bron: het IP adres of de naam van de computer waarvandaan de gegevens kwamen;
- Identiteit van de bestemming: het IP adres of de naam van de computer waar de gegevens naar toe gingen;
- Type dienst: de dienst die via de verkregen toegang afgenomen werd;
- Datum / tijd en tijdsduur van het gebruik van de afgenomen dienst.

4.3.4. E-mail

Met betrekking tot de e-mail dienst heeft de opsporing behoefte aan de volgende gegevens:

- E-mail adres zender en ontvanger(s): hiermee is in sommige gevallen de identiteit van de gebruikers te achterhalen;
- IP adres zender: hiermee is de afzender aan de gebruikte toegangsdienst te koppelen;
- IP adres ontvanger: hiermee is de ontvanger aan de gebruikte toegangsdienst te koppelen;
- Identiteit van het bericht: Message-ID, een uniek gegeven waarmee een bericht in de keten van aanbieders te traceren is;
- Datum / tijd van verzending en van doorgifte;
- Grootte van het bericht;
- Onderwerp[38].

Naast deze gegevens *per bericht* heeft de opsporing behoefte aan gegevens betreffende het *opvragen* van een mailbox; deze gegevens zijn ook van toepassing als er geen berichten blijken te zijn:

- E-mail adres gebruiker;
- IP adres gebruiker: hiermee is de e-mail dienst aan de toegangsdienst te koppelen;
- Datum / tijd dat de mailbox werd opgevraagd.

4.3.5. Internettoegang via een internetcafé

Verkeersgegevens met betrekking tot de toegangsdienst die geboden wordt door internetcafé zijn grotendeels vergelijkbaar met de zoals gepresenteerd in paragraaf 4.3.3, voor internettoegang in het algemeen. Het bijzondere karakter ligt vooral in de anonieme toegang tot de werkplek. Het betreft:

[38] Hoewel het onderwerp van een e-mail bij de benodigde verkeersgegevens genoemd werd, wordt dit in het algemeen niet als een verkeersgegeven maar als een inhoudsgegeven beschouwd.

- De identiteit van de aansluiting: een gegeven waarmee de specifieke werkplek geïdentificeerd kan worden. Dit kan een MAC adres of een IP adres zijn.
- De identiteit van de gebruiker: een user-ID, creditcard nummer, of ander gegeven dat de sessiegegevens koppelt aan een identiteit; ook als de gebruiker anoniem is kan een user-ID in sommige gevallen een koppeling leveren tussen verschillende sessies door dezelfde gebruiker.
- Het IP adres: dit kan een tijdelijk adres voor de duur van een sessie zijn, of een adres dat vast aan een werkplek gekoppeld is. Dit adres, in combinatie met datum en tijd voor zover het een tijdelijk adres is, maakt het mogelijk de sessiegegevens te koppelen aan dienstgegevens, ook als de dienst door een andere aanbieder wordt geleverd;
- Datum / tijd en tijdsduur: periode waarin een klant gebruik heeft gemaakt van een werkplek;
- Volume: het totale aantal bytes en/of packets dat gedurende de sessie van en naar de gebruiker getransporteerd werd.

Voor wat betreft de eigenlijke *communicatie* tijdens de toegangssessie hebben de opsporingsdiensten, net als bij andere toegangsvormen, behoefte aan de volgende gegevens:
- Identiteit van de bron: het IP adres of de naam van de computer waarvandaan de gegevens kwamen;
- Identiteit van de bestemming: het IP adres of de naam van de computer waar de gegevens naar toe gingen;
- Type dienst: de dienst die via de verkregen toegang afgenomen werd;
- Datum / tijd en tijdsduur van het gebruik van de afgenomen dienst.

4.4 Voorbeelden vanuit de opsporing

Het KLPD gaf ten behoeve van het onderzoek een tiental voorbeelden van zaken waarbij internet verkeersgegevens een rol hadden gespeeld. Alhoewel deze selectie niet als een representatieve steekproef mag worden gezien, geven deze zaken wel een goed beeld van het soort situaties waarbinnen deze verkeersgegevens gebruikt worden.

De helft van de voorbeelden betrof zaken waarbij een strafbaar feit met behulp van internet gepleegd was: het betrof gevallen van hacking, bedreiging per e-mail, en verspreiding van kinderporno. In de andere helft van de gevallen werd het feit niet met behulp van internet gepleegd, maar speelden internet verkeersgegevens wel een rol bij het oplossen van het misdrijf. Het betrof een moord, enkele diefstallen, en een geval van drugshandel.

Gegevens omtrent toegangssessies opgevraagd
In één zaak werd een user-ID gezocht van een verdachte waarvan het telefoonnummer bekend was. In alle andere zaken werden NAW gegevens gezocht bij een dynamisch uitgegeven IP adres, dat in een voorafgaande fase van het onderzoek gevonden was.

In al deze gevallen waren verkeersgegevens van de toegangssessies nodig om de vraag te beantwoorden.

In de meeste van deze zaken werd de gevraagde informatie ook gevonden; in de zaken waar dit niet lukte kwam dat in één geval omdat de aanbieder in het geheel geen toegangssessies registreerde, in één geval omdat de aansluiting zonder nummeridentificatie niet uniek geïdentificeerd kon worden, en in twee gevallen omdat de aanbieder weigerde mee te werken.

Gegevens omtrent e-mail opgevraagd
In vier van de genoemde zaken werd het gebruik van e-mail onderzocht. Eén daarvan betrof een situatie waar het slachtoffer een e-mail had ontvangen waarin het IP adres van de afzender stond; hierdoor waren er verder geen verkeersgegevens omtrent e-mail nodig. In de andere gevallen werden de e-mail gegevens bij de aanbieder opgevraagd en verkregen. Hierdoor kreeg men de IP adressen en tijdstippen dat bepaalde berichten waren verstuurd; met deze gegevens kon vervolgens de gebruiker bij een andere aanbieder geïdentificeerd worden.

Gegevens omtrent toegang via internetcafés opgevraagd
Een voorbeeld van een succesvol opsporingsonderzoek betrof een bommelding gemaakt vanuit een openbare schoolbibliotheek. Een dergelijke openbare gelegenheid is in dit opzicht vergelijkbaar met een internetcafé. Hoewel het onderzoek in eerste instantie strandde op het feit dat de dader anoniem gebruik had gemaakt van de toegangsdienst, kon dankzij de verkeersgegevens in onder andere de proxyservers van de bibliotheek de dader alsnog achterhaald worden. Hierbij was cruciaal dat uit deze digitale sporen afgeleid kon worden wat de verdachte tijdens dezelfde sessie als de bommelding nog meer gedaan had, hetgeen een e-mail adres opleverde; via de verkeersgegevens van de e-mail aanbieder konden andere inlogsessies van de verdachte gevonden worden, die uiteindelijk leidden tot een identificeerbare verdachte.

5. Registreren en bewaren van verkeersgegevens bij aanbieders van telecommunicatiediensten

5.1 Algemeen

Dit hoofdstuk geeft in algemene termen de redenen die de aanbieders hanteren om verkeersgegevens te registreren, te bewaren, dan wel te verwijderen. In het volgende hoofdstuk wordt ingegaan op de specifieke onderzochte diensten.

De aanbieders geven aan dat de registratie en opslag van verkeersgegevens primair in dienst staat van de eigen bedrijfsvoering. De aanbieder maakt een afweging tussen de kosten en de baten van het registreren en bewaren van een verkeersgegeven. De voornaamste bedrijfsprocessen waarbij verkeersgegevens een rol spelen zijn:

- Technische operatie
- Bestrijding fraude en misbruik
- Facturering
- Marketing

Wanneer de aanbieder besluit dat bepaalde verkeersgegevens van belang zijn voor het bedrijfsproces, is de bewaartermijn in de meeste gevallen ook afhankelijk van het doel van het verkeersgegeven. Deze termijn blijkt te variëren van enkele dagen tot enkele jaren. Bij drie aanbieders (twee ISP's en één mobiele aanbieder) bleek dat men bepaalde verkeersgegevens onbeperkt lang op CD bewaarde. De beslissing tot het onbeperkt bewaren van de gegevens wordt bij deze aanbieders genomen door de persoon die het technische beheer voert over de gegevenshuishouding. Argumenten als 'het neemt zo weinig plek in beslag, waarom zou ik het weggooien' of 'we hebben altijd alles al bewaard' worden hierbij gebruikt.

De telefonieaanbieders noemen naast de eigen bedrijfsvoering ook andere redenen om verkeersgegevens op te slaan. Deze worden gevonden in de behoefte van de opsporingsdiensten en de wettelijke verplichting hiervoor. De enige wettelijke verplichting om verkeersgegevens op te slaan, anders dan als deel van een factuur, komt voort uit het Besluit Bijzondere Vergaring Nummergegevens Telecommunicatie[39]. In dit besluit wordt vastgelegd dat, voor zover van gebruikers geen NAW gegevens beschikbaar zijn, de aanbieders specifiek omschreven verkeersgegevens voor ten minste drie maanden moeten bewaren om een gebruiker te kunnen identificeren. Het besluit is primair gericht op de Pre-Paid mobiele eindgebruiker, waarvan in de meeste gevallen geen NAW gegevens bekend zijn. Alle onderzochte aanbieders van mobiele telefoniediensten slaan de verkeersgegevens van Pre-Paid klanten voor ten minste zes maanden op.

Ten slotte geven de onderzochte aanbieders aan dat men zich zeer bewust is van een eigen maatschappelijke verantwoordelijkheid. Dit betekent dat, wanneer men zelf overtuigd is van de noodzaak, de aanbieders altijd bereid zijn tot medewerking. Zo gaf één aanbieder als voorbeeld aan dat deze tijdens een gijzeling niet alleen verkeersgegevens aan de politie geleverd had,

[39] Gepubliceerd in Stb. 2002, 31

maar ook gegevens betreffende het opladen van pre-paid tegoeden.

5.2 Redenen vanuit de bedrijfsvoering om verkeersgegevens te bewaren

Hieronder worden de redenen opgesomd waarom een aanbieder van telecommunicatiediensten in de praktijk besluit een verkeersgegeven uit bedrijfsmatige overwegingen te registreren en voor een bepaalde termijn te bewaren:

Technische operatie

- *Het verhelpen van een storing*
  Verkeersgegevens worden veel toegepast in het opsporen en verhelpen van storingen. Hiervoor zijn in het algemeen alleen zeer recente gegevens relevant. Wanneer er behoefte is aan meer gegevens voor het verhelpen van de storing dan gewoonlijk worden geregistreerd bestaat er vaak de mogelijkheid tijdelijk nog gedetailleerdere gegevens te registreren.
- *Optimalisatie van de operatie*
  Verkeersgegevens geven inzicht in het prestatie niveau van diensten. De kwaliteit van de dienst kan dankzij dit inzicht verbeterd worden door bijvoorbeeld een aanpassing in de architectuur. Voor dit doel worden echter de detailgegevens niet bewaard, aangezien geaggregeerde overzichten voldoende inzicht geven.

Bestrijding fraude en misbruik

- *Detectie van misbruik van diensten*
  Misbruik van de diensten schaadt de operatie en het is in het belang van de dienstaanbieder dit te bestrijden.
  Telefonieaanbieders krijgen veelvuldig te maken met gebruikers die de dienst gebruiken zonder daarvoor te willen betalen. Daarnaast vallen ook “plaaggevallen” (ongewenste telefoontjes) onder misbruik.
  Hoewel een ISP soms ook wel te maken heeft met misbruik van diensten binnen de eigen klantenkring, zijn het vaak ook de eigen klanten die getroffen worden door misbruik van buitenaf. Voorbeelden hiervan zijn hacking (inbraak op systemen) en spam (ongewenste massale e-mail). Verkeersgegevens bieden de ISP de mogelijkheid daders te traceren of om beveiligingsgaten te vinden en te dichten.

Facturering

- *Afrekening*
  Voor de telefonieaanbieders is het op kunnen stellen van de rekening dé grote drijfveer om verkeersgegevens te registreren. Gegevens zoals de identiteit van de aansluiting, de begin- en eindtijd van een verbinding en de bestemming van de verbinding zijn parameters voor de hoogte van de kosten voor de eindgebruiker.
  Ook bij ISP’s worden verkeersgegevens in het geval van gebruiksafhankelijke afrekening (vooral bij ADSL en kabeltoegang) ingezet om het gebruik vast te stellen. Zodra de facturen zijn geproduceerd, zijn de verkeersgegevens voor dit doeleinde niet langer van toepassing en kunnen zij in principe worden verwijderd. De facturen zelf worden wel

enkele jaren bewaard, maar deze bevatten in de meeste gevallen geaggregeerde gegevens (totaalverbruik naar type dienst) en geen specifieke verkeersgegevens.

- *Ophelderen afrekening*
  Verkeersgegevens worden ook wel ten behoeve van het ophelderen van disputen omtrent facturen bewaard. Daarmee kunnen mogelijke onduidelijkheden opgehelderd worden. De detailgegevens worden dan bijvoorbeeld bewaard tot de eerstvolgende factuurdatum, in de praktijk één of twee maanden.

Marketing

- *Analyse gebruikersgedrag*
  Verkeersgegevens worden regelmatig ingezet voor het analyseren van gebruikersgedrag. De gegevens worden gebruikt voor zeer gerichte marketingactiviteiten. Soms worden hiervoor (tijdelijk) extra verkeersgegevens opgeslagen. Veel van deze gegevens worden echter geaggregeerd bewaard zonder dat deze nog terug te voeren zijn op de individuele gebruiker. In de toekomst zullen gegevens voor marketingdoeleinden moeten voldoen aan het “opt-in” systeem of anders anoniem gemaakt moeten worden.

  Een voorbeeld van analyse van gebruikersgedrag is een ISP die per gebruiker de meest recente POP3 sessie logde. Een campagne rond e-mail werd vervolgens aan die klanten gericht die geen gebruik van e-mail (meer) maakten.

  Een bijzonder voorbeeld van analyse van gebruikersgedrag is het beschikbaar maken van de verkeersgegevens op internet waardoor de klant de mogelijkheid krijgt zijn of haar eigen belgedrag te analyseren.

5.3 Belemmeringen bij het opvragen van gegevens

In een aantal situaties blijken de door de opsporing gevraagde verkeersgegevens niet beschikbaar te zijn. De belangrijkste door de aanbieders genoemde oorzaken zijn de volgende:

Verkeersgegeven is niet beschikbaar of niet van toepassing door de aard van de dienst
Afhankelijk van de aard van de dienst of de manier waarop deze geïmplementeerd is, zijn bepaalde gegevens niet beschikbaar of niet van toepassing. Hier kunnen verschillende redenen voor zijn:

- *Het gegeven is niet van toepassing gezien de aard van de dienst:*
  De gegevens die de opsporingsdiensten nodig hebben zijn in het hoofdstuk 3.3 in zijn algemeenheid beschreven. Een aantal van deze gegevens heeft echter, afhankelijk van de aard van de dienst, in sommige gevallen geen zinvolle betekenis en is daarmee niet van toepassing voor deze dienst.

  Een voorbeeld is de begin- en eindtijd van een toegangssessie, in het geval de toegangsdienst als vaste dienst over een huurlijn aangeboden wordt. De sessie is dan immers permanent aanwezig, ongeacht of deze gebruikt wordt of niet. Begin- en eindtijden

hebben dan geen betekenis.

- *Het is technisch niet mogelijk het gegeven te krijgen*
  In sommige gevallen is het gevraagde gegeven wel zinvol te definiëren, maar om technische redenen op geen enkele manier uit de bestaande infrastructuur te krijgen. Een voorbeeld hiervan zijn de kabelnetwerken, die berusten op een businfrastructuur. Bij dergelijke infrastructuren is niet na te gaan via welke fysieke aansluiting een eindgebruiker gekoppeld is aan het netwerk. Het signaal komt immers binnen over een kabel waarmee een aantal huishoudens direct gekoppeld is. Dat houdt in dat de geografische locatie van die fysieke aansluiting niet exact achterhaald kan worden; het is alleen bekend op welk kabelsegment de gebruiker aangesloten was. (Wel kan via de abonneegegevens nagegaan worden op welk adres deze geregistreerd is, maar dit biedt geen zekerheid dat de gebruiker zich ook daadwerkelijk op dat adres bevond.)

Verkeersgegevens worden niet geregistreerd
De apparatuur waarmee de diensten worden geleverd zijn in de meeste gevallen in staat verkeersgegevens te genereren. Wanneer de aanbieder deze gegevens echter niet nodig heeft voor de bedrijfsvoering, of wanneer het verwerken van de gegevens teveel middelen in beslag neemt in verhouding tot het nut voor de bedrijfsvoering, zal men vaak besluiten de “logging” uit te schakelen.

De meeste ISP’s registreren om die reden geen detailgegevens omtrent het IP verkeer (IP accounting). Eén van de ondervraagde ISP’s (de kleinste van de ondervraagde aanbieders) doet dit wel.

De telefonieaanbieders registreren eveneens lang niet alles wat de apparatuur mogelijk maakt; zo registreren de meeste aanbieders geen *call attempts*, oftewel onbeantwoorde oproepen. Alleen beantwoorde gesprekken worden in rekening gebracht, en dus worden alleen die gesprekken op de centrale geregistreerd.

De internetcafés blijken uitermate weinig te registreren. Van de twee bedrijven die geïnterviewd zijn bleek één café vrijwel niets te loggen. Dit is zeer wel te verklaren aangezien de meeste loggegevens in het algemeen weinig waarde hebben voor de bedrijfsvoering. Het enige gegeven dat van primaire waarde is, is de tijdregistratie, aangezien de kosten van de dienstverlening afhankelijk zijn van de tijdsduur dat de klant er gebruik van maakt. Genoemd café logde zelfs die informatie alleen op papier en bewaarde deze slechts tot het moment van afrekenen.

Gegevens zijn verloren gegaan.
In een aantal gevallen kunnen gegevens verloren gaan die normaal wel gelogd worden. Dit komt met name bij de ISP’s voor; geen van de ondervraagde telefonieaanbieders noemt deze situatie. De opzet van systemen bij de aanbieders van telefoniediensten is vrijwel altijd zeer robuust uitgevoerd waardoor het verlies van gegevens nauwelijks voorkomt.

De volgende oorzaken werden door de ondervraagde ISP’s genoemd:

- *Het ontbreken van back-up systemen*
  Een aantal ISP's blijkt voor de gelogde verkeersgegevens geen back-up faciliteiten geïnstalleerd te hebben. Dit is vaak een ingecalculeerd risico, gezien de geringe betekenis van de gegevens voor de bedrijfsvoering en de kosten van back-up faciliteiten.
  Bij problemen, bijvoorbeeld als gevolg van een harddiskcrash, kunnen de gegevens dan verloren gaan.
- *Het vervangen van oude apparatuur*
  Het vervangen van oude apparatuur kan leiden tot verlies aan verkeersgegevens. De verkeersgegevens die op de oude apparatuur bewaard zijn hebben vaak niet veel waarde meer voor de ISP wanneer deze overgaat op een nieuw systeem. Dit kan zijn omdat de verkeersgegevens te oud zijn om nog van nut te zijn maar ook omdat het vervangende systeem op een ander gegevensstructuur gebaseerd is en derhalve de oude gegevens niet kan verwerken.
- *Herinrichting van het netwerk en/of nummerplannen*
  Meerdere ISP's gaven aan dat de gebruiksdynamiek en verkeersgroei met enige regelmaat leidt tot aanpassing van de architectuur en/of het omnummeren in het eigen netwerk. De oude opzet wordt na de verbouwing vaak niet bewaard. Daardoor kan het bijvoorbeeld gebeuren dat een IP adres na enige tijd niet meer tot een gebruiker te herleiden valt, omdat niet meer kan worden nagegaan, hoe dat IP adres op dat moment toegepast werd. Eén ISP gaf als voorbeeld aan dat de architectuur van de e-mail dienst gemiddeld elke maand een wijziging ondergaat.
- *Gegeven gaat tijdens de overdracht verloren*
  Drie ISP's noemden de inherente onbetrouwbaarheid van het UDP protocol, dat gebruikt wordt bij het versturen van RADIUS accounting records die de verkeersgegevens bevatten. Bij sommige ISP's blijkt in de praktijk zelfs tot 10% van de RADIUS sessiegegevens verloren te gaan als gevolg van het ontbreken van een overdrachtscontrole in dit protocol. In het geval van gebruiksafhankelijke afrekening wordt bij de prijsstelling rekening gehouden met een dergelijk gegevensverlies.
- *Gegeven gaat verloren tijdens herinstallatie*
  Dit aspect speelt bij internetcafés. Het is bij internetcafés gebruikelijk dat alle werkstations na elke sessie of tijdens het periodiek onderhoud worden voorzien van een nieuw 'image'. Dit brengt de werkplek terug in de originele staat en wist tevens alle lokaal op de werkplek opgeslagen verkeersgegevens. Dit heeft voor een internetcafé een groot voordeel voor wat betreft de beheersbaarheid van alle werkplekken.

Gegevens wel aanwezig maar moeilijk te leveren

De gegevens waarover de aanbieders beschikken bevat naast de verkeersgegevens waar de opsporingsdienst naar op zoek is, natuurlijk nog veel meer andere gegevens. Om in deze hooiberg aan gegevens de juiste te vinden, is in veel gevallen een verwerkingsslag noodzakelijk.

Een aantal factoren kan de verwerkingslag bemoeilijken:

- *Verkeersgegeven zijn verdeeld over meerdere partijen in de keten van faciliteiten*
  Bij ISP's geldt dat voor het leveren van de verkeersgegevens van één dienst vaak een andere partij benaderd moet worden, omdat deze een aandeel heeft in het leveren van die

dienst. In de praktijk kan dit meerdere werkdagen kosten. Alle ISP's geven aan in meer of mindere mate afhankelijk van logging door derde partijen te zijn doordat ze een deel van hun dienst uitbesteed hebben.
Telefonieaanbieders zijn voornamelijk verticaal georganiseerd en kennen daardoor dit probleem veel minder. De verkeersgegevens zijn centraal aanwezig bij één en dezelfde operator.

- *De gegevens bevinden op verschillende fysieke servers en (soorten) media*
  Verkeersgegevens worden bij de meeste ISP's op iedere server apart gelogd. Daarmee is er meestal meer dan één logfile die doorzocht moet worden om een bepaald gegeven te vinden. Wanneer de opslag van gegevens ook nog eens op CD of tape wordt gedaan, voegt dit een extra complicatie toe: voor het opsporen van de juiste tape of CD is meestal handwerk nodig. ISP2 geeft aan dat het zoeken naar een juiste CD met verkeersgegevens, en het vervolgens uitvoeren van een zoekopdracht op niet geïndexeerde zoekcriteria, ongeveer een werkweek in beslag neemt. Ook OP3 slaat de gegevens specifiek voor de security-operatie (waaronder het voldoen aan vorderingen vanuit de opsporing valt) op CD's op; het bedrijf kent hierdoor dezelfde problematiek.
  Alle onderzochte telefonieaanbieders maken, in tegenstelling tot de ISP's, specifiek voor de security-operatie een kopie van de meest gevraagde verkeersgegevens aan de ingang van het factureringssysteem. Daarmee worden de verkeersgegevens, voor zover op dat punt in de keten aanwezig, bij deze aanbieders uniform opgeslagen.
- *De logfile(s) met verschillende opbouw*
  Logfiles hebben vaak niet dezelfde opbouw, bijvoorbeeld omdat men verschillende software gebruikt. Bij ISP's speelt dit gebrek aan uniformiteit, vaak al binnen één bedrijf, hetgeen het zoeken in de gegevens lastig maakt. Bij telefonieaanbieders speelt deze kwestie niet voor zover de gegevens in het factureringssysteem worden geregistreerd. Het feit dat alle gegevens al terecht zijn gekomen in één systeem geeft aan dat er reeds een bewerkingsslag (de zogenaamde 'mediation') overheen is gegaan om de data uniform te krijgen. Wel hebben gegevens voor binnenkomende gesprekken –als ze überhaupt opgeslagen worden– vaak een andere herkomst en een ander formaat. Dit geldt eveneens voor verkeersgegevens van de eigen klanten die in het buitenland *roamen*.
- *De logfile(s) zeer omvangrijk qua volume*
  De zoektijd is afhankelijk van de hoeveelheid data en van de grootte van de systemen. Door de snelle groei van het gebruik in de laatste jaren hebben de ISP's vaak meer data dan zij bij het ontwerp van de systemen aangenomen hadden, waardoor het zoeken bemoeilijkt wordt.
  Telefonieaanbieders kennen eveneens een groei in het volume van verkeersgegevens. Zij zijn echter veel beter voorbereid op deze groei en zien pas grote problemen bij het doorzoeken van de gegevens wanneer zij meer soorten verkeersgegevens zouden moeten bewaren dan zij nu doen.
- *De logfile(s) zonder de juiste indexering*
  De indexering van logfiles zorgt voor een snelle verwerking van zoekopdrachten. Aanbieders optimaliseren deze indexering naar de eigen zoekbehoefte. Zoekopdrachten gebaseerd op andere zoeksleutel kosten dan meer tijd. Een voorbeeld: een ISP zoekt de gegevens altijd op user-ID en datum/tijd, en heeft daarop zijn index gebaseerd. Om nu vanuit een gegeven IP adres in een gegeven tijdvak de bijbehorende gegevens te vinden

moeten de gegevens sequentieel doorzocht worden. De index heeft in een dergelijk geval geen nut, waardoor het zoeken aanzienlijk langer zal duren. Ook de telefonieaanbieders blijken in sommige gevallen systemen te gebruiken waarbij het zoeken op bepaalde parameters geoptimaliseerd wordt, waardoor bijvoorbeeld het zoeken op B-nummer veel langer duurt dan het zoeken op A-nummer.

- *Geen menskracht om de zoekopdracht uit te voeren*
  De inspanning die een zoekopdracht vergt omvat ook de inzet van deskundig personeel dat niet altijd direct beschikbaar is. Eén ISP geeft bijvoorbeeld aan dat slechts één persoon binnen het bedrijf belast is met security. Bij afwezigheid van deze werknemer, door bijvoorbeeld ziekte of verlof, is daarmee ook de expertise afwezig. Antwoord op een verzoek vanuit de opsporing kan dan enkele dagen op zich laten wachten. De telefonieaanbieders hebben soortgelijke problemen, hoewel de schaalgrootte er meestal voor zorgt dat deskundig personeel niet snel de bottleneck zal zijn.

Gegevens zijn aanwezig maar de dienstaanbieder overhandigt ze niet vrijwillig
Sommige ISP's blijken in de praktijk veel moeite te hebben met het overhandigen van gegevens aan de opsporingsdiensten. Meer dan eens is aangegeven dat verzoeken om vrijwillige verstrekking geweigerd zijn. Op basis van een vordering worden de gegevens wel overhandigd, tenzij er twijfel bestaat over de legitimiteit van de vordering.

Bescherming van de verkeersgegevens vanuit het oogpunt van privacy is een belangrijk aspect van het imago dat sommige ISP's nastreven. Het feit dat de ISP wereld van oudsher sterke wortels heeft in de geest dat het internet een terrein is zonder fysieke en juridische grenzen, speelt daarbij een rol. Deze filosofie heeft nog altijd zijn plaats in de hedendaagse bedrijfsvoering en openbaart zich bijvoorbeeld in het weigeren informatie over klanten te overhandigen aan officiële instanties.

Telefonieaanbieders blijken een andere houding te hebben. Zij hebben het proces van informatieverstrekking –mede door de veel frequentere vraag– beter geregeld, en zij zijn zich ook veel beter bewust van de regels.

5.4 Ervaring met verzoeken en vorderingen vanuit de opsporing

Telefonieaanbieders hebben in het algemeen een zeer rijk verleden waar het gaat om het meewerken aan verzoeken en vorderingen vanuit de opsporing.

Het soort vragen dat de telefonieaanbieders krijgen is gevarieerd van aard. In een aantal gevallen worden complexere analyses gevraagd dan alleen het opzoeken van gegevens op basis van identiteit en datum/tijd. Het feit dat criminelen vaak op de hoogte zijn van de mogelijkheden en beperkingen voor de opsporing, en zich daar deels ook op richten, kan de vraag verder compliceren. Een voorbeeld hiervan, genoemd door één van de mobiele operators, was een verdachte die uiteindelijk gebruik bleek te maken van vele mobiele identiteiten in de vorm van ruim 100 verschillende SIM-kaarten, gecombineerd met verscheidene mobiele telefoons.

De ISP's blijken tot op heden slechts in zeer beperkte mate verzoeken te krijgen vanuit de opsporingsdiensten. De twee grootste geïnterviewde ISP's, die veel consumenten als klant hebben, geven aan dat zij van justitie enkele tientallen verzoeken om verkeersgegevens per jaar ontvangen; een derde iets kleinere ISP heeft in de laatste jaren een handvol verzoeken gekregen. De kleinste ISP's, die voornamelijk de zakelijke markt bedienen, hebben in de afgelopen jaren in het geheel geen of zeer weinig verzoeken gekregen. Daarbij moet worden aangetekend dat de opsporingsdiensten in het verleden zeer terughoudend zijn geweest met dergelijke verzoeken; de verwachting is dan ook dat het aantal in de komende tijd zal stijgen. Bovendien hadden veel ISP's in het verleden nauwelijks (betrouwbare) NAW gegevens van hun klanten, waardoor de waarde van verkeersgegevens ook beperkt bleef. Doordat er steeds minder "gratis" toegangsdiensten aan worden geboden, hebben de ISP's in toenemende mate NAW gegevens nodig voor de facturering, waardoor deze gegevens betrouwbaarder worden.

Opgevraagde verkeersgegevens betreffen vaak het zoeken naar een user-ID bij een gegeven combinatie van IP adres en datum / tijd. Door de manier waarop de sessiegegevens worden gegenereerd en opgeslagen zijn voor dit type vragen meestal meerdere zoekslagen nodig.

ISP1 registreert en bewaart als enige IP accounting logs (in principe de meest informatierijke logmethode) en geeft aan dat de opsporing nog nooit om deze informatie gevraagd heeft.

De twee geïnterviewde internetcafés blijken nauwelijks ervaring te hebben met opsporingsdiensten. IC1 is in zijn vijfjarig bestaan één keer door rechercheurs om een logfile gevraagd; bij IC2 zijn nog nooit gegevens opgevraagd.

6. Beschikbare verkeersgegevens per aangeboden dienst

In dit hoofdstuk wordt uiteengezet welke gegevens beschikbaar zijn bij de telefonieaanbieders, ISP's, en internetcafés met betrekking tot de onderzochte telecommunicatiediensten. Met *beschikbaar* wordt hier bedoeld: gegevens die vanuit de infrastructuur worden gegenereerd en die daadwerkelijk worden geregistreerd, en dus niet gegevens die de infrastructuur kan produceren maar die momenteel niet verwerkt worden.

De hier beschreven informatie is in de vorm van tabellen opgenomen in de bijlage 'Beschikbaarheid Verkeersgegevens'. Een overzicht van de behoefte van de opsporingsdiensten vergeleken met de beschikbare informatie is opgenomen in de bijlage 'Behoefte van de opsporing versus beschikbaarheid'.

6.1 Vaste telefonie (zie tabel 6 en tabel 7 in Bijlage C)

Bewaard worden het A-nummer (het nummer van de oproeper), het B-nummer (het nummer van de opgeroepene) en de datum, het tijdstip en de duur van de geslaagde gesprekken. Wanneer het A-nummer of B-nummer, dat in feite direct gekoppeld is aan de fysieke aansluiting, een klant betreft van de aanbieder zelf dan is de geografische locatie van de aansluiting daarmee eveneens direct bekend; zo niet dan is in elk geval bekend welke andere aanbieder deze informatie kan leveren.

Deze gegevens zijn bekend voor alle vanuit het eigen netwerk ontspringend verkeer. Dit geldt ook voor het verkeer dat de aanbieder van het vaste netwerk afhandelt bij carrier (pre)select diensten en 0800 nummers. De gegevens worden gedurende vijf tot zes maanden bewaard.

Wanneer het inkomend verkeer betreft, afkomstig van andere operators, dan worden hiervoor eveneens gegevens voor opgeslagen. De volledigheid ervan is afhankelijk van de informatie die de andere, mogelijk buitenlandse, operator doorstuurt. Met name het A-nummer wordt niet altijd doorgegeven. De gegevens van inkomend verkeer vanuit andere netwerken zijn niet direct opvraagbaar, aangezien ze in andere systemen worden geregistreerd dan de systemen waar het ontspringende verkeer wordt geregistreerd. Dit is direct het gevolg van de manier waarop de verkeersgegevens worden gebruikt voor de afrekening van het gebruik van de diensten. Het ontspringende verkeer wordt met de klant zelf afgerekend, terwijl het inkomende verkeer wordt afgerekend met de andere operators.

Vergeleken met de eerder beschreven behoefte van de opsporing ontbreken vooral de niet geslaagde gesprekken ("call attempts"), en een deel van de gegevens over het inkomende verkeer. De bewaartermijn is met zes maanden aanzienlijk korter dan de gewenste termijn van een jaar.

6.2 Mobiele telefonie (zie tabel 8 en tabel 9 in Bijlage C)

Algemeen

Elke aanbieder van mobiele telefoniediensten kan voor de geleverde diensten een basisset aan gegevens leveren. Hieronder vallen de identiteit van de klant (MSISDN en/of IMSI), het B-nummer, de begin- en eindtijd van elke sessie en, mits het toestel daadwerkelijk bij de sessie

betrokken was, het IMEI nummer van het toestel en de begin en eindlocatie van elke sessie. Welke gegevens daarnaast bewaard worden is afhankelijk van het type dienst, zoals gesprekken (en andere "circuit switched" verbindingen, zoals de oudere uitvoering van WAP), SMS, of GPRS. De bewaartermijnen variëren tussen zes maanden en een jaar, en zijn daarmee in een deel van de gevallen korter dan door de opsporing gewenst.

Gesprekken en andere "circuit switched" verbindingen
Alle drie operators laten weten dat zij alleen gegevens voor beantwoorde gesprekken bewaren. De niet beantwoorde oproepen (*call attempts*) kunnen door de centrale wel geregistreerd worden, maar dit wordt bij twee van de drie aanbieders niet gedaan, terwijl de derde de gegevens in een vroeg stadium verwijdert. Ook locatiegegevens zijn in principe beschikbaar, maar zolang de abonnee geen gesprek voert worden deze locatie *updates* niet verwerkt of bewaard.

Het aantal gegevens dat bij inkomende internationale gesprekken wordt meegestuurd is afhankelijk van hetgeen de buitenlandse partij heeft geïmplementeerd. In veel gevallen worden er bij oproepen vanuit het buitenland minder gegevens meegestuurd. Ook van gesprekken die de klant zelf in het buitenland pleegt, komen "roaming records" binnen die meestal minder informatie bevatten; met name is hier de Cell Id meestal niet bekend.

Twee van de drie onderzochte aanbieders registreren zowel ingaande als uitgaande gesprekken; de derde heeft alleen de gegevens van uitgaande gesprekken beschikbaar, en bewaart geen gegevens over inkomende gesprekken. De locatie van de gebruiker is bij sommige typen doorgeschakelde gesprekken nooit bekend[40].

Een operator geeft aan dat één gesprek vanuit de centrale meerdere records kan opleveren. Dit heeft tot gevolg dat bij eventuele bestandsanalyse de gegevens niet uit één record komen maar door een samenstelling van records.

In dichtbevolkte gebieden worden locaties soms afgedekt door meer dan drie zendmasten. Dit maakt het zoeken naar verkeersgegevens op basis van locatiegegevens een bewerkelijke operatie, aangezien de gegevens voor alle mogelijk bij een locatie behorende masten doorzocht moeten worden.

Van de door de opsporing gewenste gegevens ontbreken vooral de "call attempts", en een deel van de informatie in het geval van roaming en van inkomende gesprekken uit het buitenland. Bij één aanbieder ontbreekt zelfs alle informatie over inkomende gesprekken.

SMS diensten
Voor SMS berichten (originating en terminating) worden verkeersgegevens geregistreerd. Wanneer het een SMS betreft afkomstige vanuit een ander netwerk, of waar gebruik gemaakt is van een ander service center dan het eigen, levert dit echter relatief weinig informatie. De

[40] Dit geldt voor directe doorschakeling (Call Forward Unconditional) en voor doorschakeling wegens niet bereikbaar (Call Forward on Not Reachable). Bij doorschakeling wegens in gesprek (Call Forward on Busy) of niet beantwoord (Call Forward on No reply) is de locatie van het gebelde toestel wel bekend.

beschikbare verkeersgegevens voor een verzonden SMS zijn IMSI, MSISDN, IMEI, Cell Id, gebruikte SMSC, B-nummer (bestemming), datum en tijd. Alle operators kunnen deze gegevens in principe leveren. In het geval dat een andere dan het eigen service center gebruikt is kan de aanbieder veelal alleen het service center nummer leveren en niet het B-nummer. Voor een ontvangen SMS worden IMSI, MSISDN, IMEI, en Cell Id van de ontvanger, het gebruikte SMSC, het A-nummer (bron), datum en tijd geregistreerd. Bij gebruik van anonieme toegangspunten voor het versturen van SMS berichten zoals webinterfaces en bedrijfsnetwerken is het A-nummer meestal onbekend.

Volumegegevens (aantal bytes) worden voor SMS niet door de aanbieders geregistreerd.

Van de door de opsporing gewenste gegevens blijkt bij uitgaande berichten via het SMSC van de eigen aanbieder alleen het volume te ontbreken, terwijl bij inkomende berichten en bij berichten via een andere SMSC een groter deel van de informatie ontbreekt.

GPRS
Bij het gebruik van GPRS zijn de standaard verkeersgegevens van GSM van toepassing: MSISDN, IMSI, IMEI, de datum en het tijdstip, de duur van de sessie en de locatie waar de sessie werd opgezet en afgebroken. Alle operators kunnen deze gegevens leveren. Specifiek voor GPRS is er sprake van sessie gegevens zoals het IP adres, de naam van de netwerktoegang (Access Point Name), het soort dienst en het volume dat tijdens de sessie wordt verwerkt nog bij. Van deze gegevens kunnen de operators allemaal het volume en de Access Point Name leveren, maar verdere verkeersgegevens over het verkeer dat de klant via de verbinding transporteert kunnen de aanbieders niet geven.

Doordat de aanbieders geen IP adres registreren, is de GPRS sessie niet eenvoudig te koppelen aan de door de achterliggende ISP verleende diensten.

6.3 Toegangsdiensten (zie tabel 10 tot en met tabel 17 in Bijlage C)

Voor de verschillende vormen van internet toegang wordt in het algemeen met servers gewerkt die met één van twee gebruikelijke standaarden werken: RADIUS en DHCP. Daarbij levert het RADIUS protocol aanzienlijk meer informatie dan het DHCP protocol. Voor beide protocollen geldt dat het begin en het einde van een sessie in aparte records worden geregistreerd, waardoor het zoeken in de records complexer is dan bij de call records uit de telefonie.

De bewaartermijnen bij de verschillende aanbieders van inbelfaciliteiten variëren sterk, van zeven dagen tot onbeperkte opslag. Voor de opslag van de gegevens gebruiken de meeste ISP's in eerste instantie de vaste schijf in een server, en voor langere termijnen (meer dan een maand) een niet direct toegankelijk medium zoals CD of tape. Bij de opslag wordt vaak gebruik gemaakt van compressie waardoor zonder informatieverlies het datavolume sterk afneemt.

Van de door de opsporing gevraagde informatie is in het algemeen bij gebruik van RADIUS een groot deel aanwezig; informatie over de gebruikte diensten en over de servers waarmee de

gebruiker contact heeft gehad ontbreekt echter altijd, en bij inbellen ontbreekt soms het A-nummer. Bij gebruik van DHCP is er verder geen user-id aanwezig.

Toegang via inbellen
Zes ISP's gebruiken de RADIUS standaard voor authenticatie bij inbellen, wat een enigszins uniform beeld geeft wat betreft de beschikbaarheid van de specifieke verkeersgegevens. Wel produceren sommige RADIUS servers meer informatie dan andere, maar er is een aantal basiselementen dat door elke RADIUS server geleverd wordt.

De identiteit van de aansluiting, de nummeridentificatie (ook wel bekend als A-nummer of CLI), wordt bij alle ISP's vastgelegd, mits niet door de gebruiker onderdrukt. Eén ISP laat het gebruik van de toegangsdienst niet toe zonder nummeridentificatie. De overigen hebben in dat geval geen informatie over de aansluiting. Overigens beschikt de telefonieaanbieder wel over dit gegeven, en is het in veel gevallen mogelijk door koppeling van gegevens bij de opsporingsdienst de informatie alsnog te krijgen.

Bij alle ondervraagde ISP's worden het toegekende IP adres en de gebruikte user-ID via de RADIUS log geregistreerd[41], evenals het begin en eindtijdstip van de aansluitsessie en het volume aan uitgewisselde data binnen de sessie. Door de uitbesteding van de inbeldienst voor een deel van de klanten heeft ISP5 voor deze klanten zelf geen volume-informatie.

Toegang via ADSL
Zes ISP's bieden ADSL diensten aan. Vier ISP's gebruiken RADIUS servers, de andere twee gebruiken DHCP. De RADIUS systemen delen IP adressen uit op basis van het een user-ID, de DHCP systemen op basis van het MAC adres van het modem. Bij DHCP is er dan ook geen sprake van een user-ID.

Zowel de RADIUS als de DHCP servers genereren logs. In alle gevallen zijn begin- en eindtijd van de sessie bekend. Gezien de potentieel lange sessieduur bij ADSL verbindingen (vaak meerdere maanden) gebruikt één ISP "intermediate accounting" waardoor elk uur een update plaatsvindt van de loggegevens. Alle andere ISP's doen dit niet. De begin en eindtijd van de aansluitsessie bieden vanwege de lange sessieduur in dat geval weinig informatie over het feitelijk gebruik.

Bij de ISP's die gebruik maken van DHCP is de identiteit van de aansluiting niet bekend; het MAC adres identificeert echter wel het modem, en daarmee indirect de abonnee. Eén ISP overweegt over te stappen op DHCP met option 82, waarbij dit gegeven wel beschikbaar kan komen.

[41] De nieuwe DirecInternet dienst van KPN is niet bij het onderzoek betrokken; bij deze dienst is er geen unieke "user-id" maar dient de nummeridentificatie als enige identificatie. De toegang wordt zonder nummeridentificatie dan ook geweigerd.

Toegang via de kabel
Slechts één ISP binnen de interviewgroep levert toegangsdiensten via de kabel. Deze gebruikt voor een deel van zijn kabelnetwerken DHCP, en voor een deel RADIUS. De ISP hanteert een bewaartermijn van drie maanden voor de DHCP en RADIUS logs.

De identiteit van de gebruiker is bij de DHCP logs alleen indirect vast te stellen aan de hand van het MAC adres van het modem dat de klant in bruikleen heeft. De infrastructuur weigert de toegang als een MAC adres niet overeenkomt met het netwerksegment waar dat modem zich zou moeten bevinden. Overigens is het technisch mogelijk dit MAC adres te vervalsen. Bij gebruik van RADIUS is een user-ID bekend.

Het totale volume wordt per toegekend IP adres opgeteld en is zodoende per klant bekend.

Toegang via een huurlijn
Toegang via huurlijnen worden door vier van de zeven ISP's als dienst geleverd. Bij één ISP wordt voor deze dienst in het geheel niets gelogd; één ISP meet de volumes per IP adres, één ISP meet het volume per lijn, en één ISP doet aan volledige IP accounting. Bij deze vaste verbindingen zijn de identiteit van de aansluiting en de identiteit van de transportdienst statisch. De gebruiker is daarmee altijd bekend, en omdat de verbinding praktisch gezien altijd open staat is er geen sprake van een begin of eindtijd van de sessie. Aanvullende informatie kan alleen verkregen worden door de IP stroom te analyseren.

Doordat ISP1 "IP accounting" toepast, kunnen bij benadering de begin en eindtijd van een dienstsessie, de identiteit van de benaderde server, en het volume achterhaald worden. ISP1 is van plan de IP accounting binnen enige tijd af te schaffen in verband met de volumes; ISP3 heeft om diezelfde reden IP accounting al afgeschaft.

Andere toegangsvormen
Wireless Local Area Network (W-LAN) diensten worden nog niet, of op zeer kleine experimentele schaal geleverd. Plannen om W-LAN op grotere schaal toe te passen bestaan er wel. Dit geeft potentieel een nieuwe problemen met authenticatie aangezien de momenteel gebruikte standaarden nog onvoldoende beveiliging bieden.

Ook toegang vanuit GPRS wordt nog nauwelijks gebruikt; slechts één van de ondervraagde ISP's biedt deze dienst momenteel aan.

Additionele opmerkingen toegangsdiensten
De meeste ISP's gebruiken geen webproxy meer, of hebben deze optioneel gemaakt. Twee ISP's hebben nog wel een geforceerde webproxy voor de klanten van de gratis toegangsdienst, maar niet voor de betaalde dienst. Daardoor wordt surfgedrag in steeds minder gevallen gelogd.

6.4 E-mail (zie tabel 18 en tabel 19 in Bijlage C)

E-mail diensten worden door zes van de zeven partijen aangeboden. In de meeste gevallen wordt informatie over elk bericht (SMTP) en elke ophaalsessie (POP3) geregistreerd; deze logs bevatten een deel van de door de opsporing gevraagde informatie.

De POP3 en SMTP logs worden wisselend lang bewaard, van enkele dagen tot drie maanden. ISP6 zet de gegevens na een maand op CD, en vernietigt de CD als de gegevens ongeveer drie maanden oud zijn. Alle anderen bewaren de gegevens op hard disk, in de meeste gevallen slechts enkele dagen. De termijn is bij deze aanbieders niet altijd gelijk, maar hangt af van de ruimte op de server. Aangezien de e-mail dienst in de meeste gevallen gratis wordt aangeboden, is het belang van deze informatie voor de aanbieder beperkt; er wordt dan ook weinig moeite gedaan om de informatie veilig te stellen (geen back-ups).

ISP7, die zelf geen e-maildiensten aanbiedt, transporteert uiteraard wel e-mail verkeer van de aangesloten klanten. De klanten hebben echter hun eigen e-mail servers; de ISP heeft dan ook geen gegevens over deze dienst.

Gegevens per bericht

De beschikbaarheid van verkeersgegevens geeft een wisselend beeld. Vijf van de zes ISP's loggen SMTP verkeer, waarin ieder bericht gelogd wordt. ISP2 besteedt de dienst uit en krijgt geen SMTP gegevens. De beschikbaarheid van die SMTP gegevens is daarmee afhankelijk van hetgeen deze dienstverlener logt.

De vijf ISP's die SMTP verkeer loggen, beschikken daarmee in de meeste gevallen over de volgende gegevens:

- Voor elk binnenkomend bericht: zendend e-mail adres (dit kan vals zijn), ontvangende e-mail adressen, datum en tijd, status, naam van de laatste server waar het bericht vandaan komt (dit kan vals zijn), IP adres van de laatste server, status, en message-ID (waarmee het bericht in logs van andere aanbieders te traceren is)

- Voor elk uitgaand bericht: zendend e-mail adres (dit kan vals zijn) en IP adres (is niet te vervalsen zonder de medewerking van de ISP), ontvangende e-mail adressen, datum en tijd, status, volgende server waar het bericht naar toe is gestuurd, en message-ID (waarmee het bericht in logs van andere aanbieders te traceren is)

De grotere ISP's gebruiken meerdere platforms met verschillende software, waardoor er verschillende logfiles ontstaan. Met name het IP adres van de laatste server (bij binnenkomende berichten) en het IP adres van de zender (bij uitgaande berichten) worden bij deze ISP's niet voor alle berichten gelogd.

Het IP adres van de zender is niet altijd daadwerkelijk dat van de gebruiker; het kan ook het adres zijn van een dienst zoals www.twigger.nl waarbij men via webmail bij een e-mail account komt.

Het onderwerp van een bericht wordt door geen van de aanbieders gelogd.

Gegevens per ophaalsessie
Alle zes ISP's hebben POP3 logs, waarin iedere ophaalsessie gelogd wordt.

ISP2 verwijdert deze gegevens onmiddellijk na verwerking en bewaart alleen het tijdstip van de laatste POP sessie, dus wanneer een eindgebruiker voor het laatst zijn e-mail postbus heeft benaderd.

De overige vijf ISP's beschikken voor elke ophaalsessie over datum en tijd, IP adres waarvandaan de mail werd opgevraagd, e-mail adres van de gebruiker, aantal berichten dat op de server stond en het aantal dat opgehaald werd, en de totale grootte van de berichten op de server en van de opgehaalde berichten.

Overige opmerkingen
Eén ISP zal in de nabije toekomst spam assessment (beveiliging tegen ongewenste e-mail) aanbieden als toevoeging aan de e-mail dienst. Deze spam assessment werkt op basis van white listing en levert een white list, in versleutelde (binaire) vorm, van die klant op van vroegere e-mail contacten. Dit geeft potentieel een blik in de e-mail geschiedenis van deze eindgebruiker: het is niet mogelijk de adressen uit de white list te halen, maar het is wel mogelijk om te toetsen of de gebruiker met een bepaald adres contact heeft gehad.

6.5 Internetcafés (zie tabel 20 en tabel 21 in Bijlage C)

Eén partij registreert bij de verkoop van toegangskaarten de user-ID op de kaart, de datum en tijd, en de prijs. Tijdens het gebruik wordt het werkstation, de user-ID, begin- en eindtijd, het aantal bytes (in/uit) gelogd, en voor urenkaarten het resterende tegoed gelogd. De tweede partij heeft geen server opstelling en schrijft alleen de tijd van binnenkomst op een briefje, dat na het vertrek weggegooid wordt. Verkeersgegevens gerelateerd aan het gebruik van de dienst worden in geen van beide internetcafés geregistreerd.

Doordat de PC's periodiek van een "clean image" voorzien worden is er geen history of lokale cache beschikbaar, of zijn deze slechts tot het volgende onderhoud beschikbaar. Deze lokaal opgeslagen gegevens kunnen ook door de gebruiker gewist worden.

7. Consequenties van een bewaarplicht en/of registratieplicht

7.1 Inleiding

Uit het voorgaande blijkt dat aanbieders niet altijd aan de wensen van de opsporingsdiensten kunnen voldoen voor wat betreft historische verkeersgegevens. Een groot aantal gegevens wordt wel verzameld, maar in veel gevallen minder lang bewaard dan voor de opsporing gewenst is. Daarbij zijn er met name in de ISP wereld grote verschillen in de bewaarde gegevens en bewaartermijnen per aanbieder.

Een mogelijkheid om deze discrepantie te verkleinen is dat aanbieders een bewaarplicht voor een bepaalde termijn krijgen voor bepaalde gegevens, mits ze deze gegevens al verwerken. Dit zal blijven leiden tot heterogeniteit, omdat niet alle aanbieders dezelfde gegevens registreren en verwerken.

Een verdergaande stap is het opleggen van een registratieplicht van bepaalde gegevens die de overheid nodig acht, ook al heeft een aanbieder ze zelf niet nodig voor zijn eigen bedrijfsvoering. Hierdoor wordt de genoemde heterogeniteit vermeden.

In het onderstaande worden de consequenties voor de aanbieders besproken van een eventuele bewaarplicht voor bepaalde gegevens, en van een eventuele registratieplicht voor diezelfde gegevens. Die consequenties hangen niet alleen af van de specifieke gegevens die de aanbieders moeten bewaren en van de duur van de bewaarplicht, maar ook van de gevraagde toegankelijkheid van de gegevens.

De voornaamste consequentie van een bewaar- c.q. registratieplicht is de benodigde investering. Daarnaast brengt elke investering ook operationele kosten met zich mee (technisch onderhoud, dagelijkse operatie, kosten van back-up media, gebruik van ruimte etc.), en wordt de invoering van nieuwe diensten complexer door de additionele verplichting waar rekening mee gehouden moet worden. “Zachtere”, en dus moeilijker aan te tonen effecten kunnen ontstaan doordat aanbieders die zich tot nu toe profileren met een duidelijk privacybeleid, zich minder kunnen differentiëren dan voorheen. Zo maakt één ISP expliciet reclame met het feit dat deze, in tegenstelling tot veel andere ISP’s, verkeersgegevens binnen enkele dagen verwijdert. Een dergelijke positionering zou bij een bewaarplicht voor bijvoorbeeld een jaar niet meer mogelijk zijn.

7.2 Benodigde systeemuitbreidingen

De benodigde investeringen hangen voor een groot deel af van het volume aan gegevens, en zullen daarom per dienst verschillend zijn. De in de volgende paragrafen geschatte volumes gaan uit van een bewaartermijn van twaalf maanden, hetgeen overeenkomt met de termijn die door de opsporing als noodzakelijk genoemd werd.

Bedragen worden hier niet genoemd; deze zullen mede afhangen van de door de regelgever te stellen eisen. Met name hangen de investeringen af van:

- de gevraagde bewaartermijn,
- de specifieke gegevens die bewaard moeten worden,

- de snelheid waarmee de aanbieders de gegevens moeten kunnen leveren (binnen enkele minuten, uren, of dagen),
- het aantal te verwachten vorderingen,
- de soorten vragen die de aanbieders moeten kunnen beantwoorden (met name de "zoeksleutels", zoals IP adres, B-nummer, locatie, etc.),
- de gevraagde beschikbaarheid en betrouwbaarheid van de gegevens (veel ISP's maken op dit moment geen back-ups van de gelogde gegevens, en accepteren dat de logs af en toe verloren gaan).

De benodigde investeringen bestaan niet uitsluitend uit apparatuur: naast de benodigde hardware zoals servers, schijfruimte, RAID controllers, en back-up systemen, zullen er in veel gevallen software licenties gekocht moeten worden, en zal de bestaande software aangepast moeten worden. Daarnaast brengen de installatie en de eventuele aanpassingen in de operationele omgeving kosten met zich mee. Een vuistregel is daarbij dat de totale investering ongeveer het dubbele bedraagt van de directe kosten aan hardware en software.

Voor de totale kosten maakt het verder een groot verschil of iedere aanbieder zelfstandig een oplossing realiseert, of dat een aantal aanbieders gebruik maakt van de schaalvoordelen die kunnen ontstaan door gezamenlijk een oplossing op te (laten) zetten. Ook kan het voordelen opleveren als de benodigde uitbreiding om aan een eventuele verplichting te voldoen gecombineerd kan worden met andere noodzakelijke veranderingen.

7.2.1. Vaste telefonie

De ondervraagde telefonieaanbieder bewaart de benodigde gegevens over de uitgaande, beantwoorde gesprekken van zijn klanten. Dit geldt zelfs voor gratis gesprekken (0800) en voor gesprekken die via een andere operator lopen (Carrier Select en Carrier Pre-Select), ondanks het feit dat deze gesprekken niet bij de klant in rekening worden gebracht. Inkomende gesprekken vanuit andere netwerken worden in andere centrales geregistreerd, en in andere systemen verwerkt, dan de uitgaande gesprekken; hierdoor zijn deze gegevens wel aanwezig maar niet direct beschikbaar voor de security afdeling.

Bestaande gegevens twaalf maanden bewaren

Een bewaartermijn van twaalf maanden voor gegevens over uitgaande gesprekken zou extra investeringen vergen, aangezien de gegevens nu voor vijf maanden bewaard worden. Het gaat dan om het implementeren van extra opslagcapaciteit voor het systeem van de security afdeling.

Om naar schatting 35 miljoen records per dag zeven maanden langer te bewaren is ongeveer 900 Gigabyte[42] extra schijfruimte nodig.

In plaats van het opslaan op vaste schijven is het ook mogelijk de verkeersgegevens op DVD op te slaan. In dat geval zijn de gegevens minder snel te benaderen. Bij een beperkt aantallen

[42] Uitgaande van 35 miljoen records per dag (schatting gebaseerd op kwartaalcijfers KPN), waarvan 110 bytes per record 212 dagen (zeven maanden) langer bewaard moet worden; 35 miljoen * 110 byte * 212 = 816.200 Megabyte; met enige overhead voor indices e.d. komt dit op 900 Gigabyte

vorderingen (tot enkele tientallen per dag) zal dit in de praktijk slechts enkele minuten verschil maken in de responstijd. Voorwaarde is dan wel dat de vorderingen steeds betrekking hebben op een periode van hoogstens enkele dagen, en zo geformuleerd zijn dat de bestaande index gebruikt kan worden. Bij het ontwerp van het systeem zal er daarom duidelijkheid moeten zijn over de soorten te stellen vragen. Zoekopdrachten die niet aan deze voorwaarden voldoen zullen bij gebruik van DVD's veel langer duren: het ten behoeve van één zoekopdracht sequentieel doorzoeken van alle 900 Gigabyte op DVD's kost bijvoorbeeld ongeveer een week, terwijl diezelfde opdracht op een snelle server, met de data op harde schijven, minder dan een dag kost.

Om ook gegevens over de binnenkomende gesprekken vanuit andere netwerken beschikbaar te maken is eveneens een investering nodig. Aangezien deze gegevens niet direct toegankelijk zijn, gaat het niet alleen om additionele opslagcapaciteit maar ook om interfaces vanaf diverse systemen naar het security systeem.

Niet beantwoorde gesprekken registreren en bewaren
Call attempts, oftewel niet beantwoorde oproepen (bijvoorbeeld wegens in gesprek, niet beantwoord, of congestie), worden door de aanbieder geheel niet geregistreerd.

Een registratieplicht voor call attempts zou niet alleen consequenties hebben voor het opslagsysteem, voor de mediation[43] systemen, en voor de interne datacommunicatienetwerken, maar ook voor de hardware van de telefooncentrales zelf. In de centrales moeten met name de lokale opslag en de datacommunicatiefaciliteiten uitgebreid worden[44].

7.2.2. Mobiele telefonie

Alle ondervraagde telefonieaanbieders bewaren in elk geval de door de opsporing gevraagde gegevens over de uitgaande, beantwoorde gesprekken van hun klanten. Dit geldt zelfs voor gratis gesprekken (0800). Twee van de drie ondervraagde aanbieders bewaren ook inkomende gesprekken vanuit andere netwerken. Call attempts (niet beantwoorde oproepen) worden door geen van de aanbieders bewaard.

Voor pre-paid gesprekken werden de verkeersgegevens tot voor kort niet door alle mobiele aanbieders bewaard, maar als gevolg van het Besluit Bijzondere Vergaring Nummergegevens Telecommunicatie gebeurt dit nu wel.

De gegevens worden ten minste vijf maanden bewaard, en bij één aanbieder onbeperkt lang.

Bestaande gegevens twaalf maanden bewaren
Een bewaartermijn van twaalf maanden zou van twee van de ondervraagde operators extra investeringen vergen; deze bewaren de gegevens nu voor vijf respectievelijk zes maanden. Het

[43] Mediation: het systeem dat de in de telefooncentrale geregistreerde gegevens ophaalt, formatteert, en doorgeeft aan de overige systemen

[44] In het ergste geval kan het zelfs nodig zijn additionele centrales te plaatsen als de bestaande centrales niet ver genoeg uitbreidbaar meer zijn.

gaat dan om het implementeren van extra capaciteit voor het opslagsysteem van de security afdeling.

Voor een grote mobiele operator (30-40% van de markt) is voor een uitbreiding van zes naar twaalf maanden, voor inkomende en uitgaande gesprekken, ongeveer 900 Gigabyte[45] extra schijfruimte nodig. Een kleinere mobiele operator (15% van de markt) heeft voor een uitbreiding van zes naar twaalf maanden ongeveer 400 Gigabyte nodig.

In plaats van het opslaan op vaste schijven is het ook mogelijk de verkeersgegevens op DVD op te slaan. In dat geval zijn de gegevens minder snel te benaderen. Bij een beperkt aantallen vorderingen (tot enkele tientallen per dag) zal dit in de praktijk slechts enkele minuten verschil maken in de responstijd. Net als bij vaste telefonie is de voorwaarde dan wel dat de vorderingen steeds betrekking hebben op een periode van hoogstens enkele dagen, en zo geformuleerd zijn dat de bestaande index gebruikt kan worden.

Niet beantwoorde gesprekken registreren en bewaren
Call attempts, oftewel niet beantwoorde oproepen (bijvoorbeeld in gesprek, niet beantwoord, of congestie), worden door twee van de aanbieders geheel niet geregistreerd, en bij de derde vroeg in het proces door de mediation verwijderd.

Een registratieplicht voor call attempts zou niet alleen consequenties hebben voor de opslag, de mediation systemen, en de interne datacommunicatienetwerken, maar ook voor de hardware van de telefooncentrales zelf. Met name de lokale opslag en de datacommunicatiefaciliteiten van de centrales moeten uitgebreid worden.

Voor een grote mobiele operator (30-40% van de markt) gaat het bij de niet beantwoorde gesprekken om ongeveer 18 miljoen records per dag, hetgeen neerkomt op ongeveer 750 Gigabyte[46] voor twaalf maanden opslag. Ook hier geldt dat het op DVD bewaren een alternatief kan zijn; de eerder genoemde brander met jukebox zal in dat geval groter moeten zijn.

7.2.3. Internettoegang

Alle ondervraagde ISP's registreren en bewaren gegevens over internet toegangssessies; de bewaartermijn varieert van enkele dagen tot enkele maanden of zelfs onbeperkt (op CD dan wel op tape). De kleinste van de ondervraagde ISP's logt als enige ook *IP accounting* gegevens, die informatie geven over de bron en bestemming van de verstuurde IP pakketten.

Bestaande gegevens twaalf maanden bewaren
Uitgaande van 6 miljard internet inbelminuten in het derde kwartaal van 2002[47] worden er in Nederland ongeveer 150 miljoen toegangsessies per maand gelogd, hetgeen 300 miljoen

[45] Uitgaande van 36 miljoen records per dag, waarvan 130 bytes per record 183 dagen (zes maanden) langer bewaard moet worden; 36 miljoen * 130 byte * 183 = 856.440 Megabyte; met enige overhead komt dit op 900 Gigabyte

[46] Uitgaande van 18 miljoen records per dag, waarvan 110 bytes per record 365 dagen (12 maanden) bewaard moet worden; 18 miljoen * 110 byte * 365 = 722.700 Megabyte; met enige overhead komt dit op 750 Gigabyte

[47] KPN Kwartaalbericht 15 november 2002.

records per maand oplevert[48]. Hier komen nog eens ongeveer 60 miljoen records per maand voor kabel en ADSL toegang bij. Het opslaan van inlogsessies van een RADIUS of DHCP log blijkt in de praktijk ongeveer 600 byte per record te kosten, waarmee het totale volume voor alle aanbieders op ongeveer 220 Gigabyte per maand komt. Dit komt voor de grootste ISP's, met 10% van de markt, neer op ongeveer 20 Gigabyte per maand, en voor een middelgrote ISP op 1 à 2 Gigabyte per maand.

Een aantal ISP's bewaart de verkeersgegevens initieel op de harde schijf, maar schuift de gegevens na enkele weken door naar tape of CD. Om de verkeersgegevens voor alle toegangssessies 11 maanden langer op harde schijf te bewaren, is voor een grote ISP ongeveer 220 Gigabyte nodig. Voor een middelgrote ISP komt dit op ongeveer 20 Gigabyte.

De gegevens op CD of DVD branden leidt tot veel lagere kosten: een middelgrote ISP heeft slechts een CD-brander nodig. In dit geval levert elke vordering dan wel enkele mandagen werk. Als de ISP's in staat zouden moeten zijn, zoals door de behoeftestellers is gevraagd, om binnen enkele uren de gevraagde gegevens op te leveren zouden zij de loggegevens op een aparte server met een CD-jukebox of DVD-jukebox moeten aanschaffen.

Voor de meeste ISP's zou er verder nog een personeelsuitbreiding nodig zijn, met name indien er ook buiten kantooruren gegevens opgeleverd moeten kunnen worden.

Overigens moet opgemerkt worden dat een deel van de verkeersgegevens als gevolg van het gebruikte UDP protocol verloren gaat (in sommige gevallen tot 10%), en dat het bijzonder moeilijk voor de ISP's zou zijn om hier fundamenteel verbetering in aan te brengen.

IP accounting gegevens registreren en bewaren

Loggen op bron en bestemmingsbasis van verkeersgegevens van IP-pakketten (IP accounting) is van een totaal andere orde dan de eerder beschreven toegangsgegevens. De enige geïnterviewde ISP die dit doet gaf aan dat, op een datastroom van 2 Mbit/s, er 8 Megabyte per uur aan accounting data werden gegenereerd. Een tweede ISP die ooit IP accounting ingeschakeld had, is daarvan afgestapt omdat het systeem te zwaar belast werd. Men kijkt nu alleen naar het totale volume van en naar een aan de klant toegekend IP adres.

Met naar schatting 25 Gbit/s relevant internet verkeer in Nederland[49] komt loggen van IP stromen (bron, bestemming, volume, en datum/tijd) in intervallen van vijf minuten neer op ca. 60 Terabyte aan verkeersgegevens per maand. Voor een grote ISP zou dit neerkomen op 6 Terabyte per maand, ofwel 72 Terabyte voor een jaar opslag; daarbij moet het systeem een volume van 5 Megabyte per seconde[50] kunnen verwerken en opslaan. Als er weinig eisen aan de zoeksnelheid gesteld worden dan kan in plaats daarvan een groot aantal DVD jukeboxes gecombineerd worden[51].

---

48 Er worden een record geproduceerd voor het inloggen, en een record voor het uitloggen.

49 Geëxtrapoleerd uit gegevens van de AMS-IX.

50 6 Terabyte per maand komt neer op 200 Gigabyte per dag, ofwel 2,3 Megabyte per seconde; het systeem moet echter tenminste het dubbele daarvan aankunnen om ook tijdens piektijden de gegevens te kunnen verwerken.

51 Gebruikelijke DVD jukeboxes kunnen ongeveer 2 Terabyte opslaan; voor 72 Terabyte zijn dus 36 jukeboxes nodig.

Daarnaast zullen de meeste ISP's gedwongen zijn van hun centrale routers een beduidend krachtiger versie aan te schaffen en tegelijk met het groeiende verkeer hun registratiesystemen uit te breiden.

Door langere intervallen te nemen kunnen de kosten verlaagd worden, maar de gegevens verliezen daarmee ook aan betekenis: de kans dat hetzelfde IP adres, binnen het gelogde interval, aan verschillende gebruikers toegekend is geweest neemt dan sterk toe, waardoor niet meer te herleiden is bij welke gebruiker de gegevens horen. Een IP adres wordt immers vaak binnen enkele seconden na het einde van een toegangssessie aan een andere gebruiker toegekend.

7.2.4. E-mail verkeersgegevens

De meeste ISP's registreren zowel POP3 als SMTP, voor zover zij deze diensten aanbieden. Uit de POP3 logs is zichtbaar wanneer een gebruiker de mailbox raadpleegde[52], hoeveel berichten er opgehaald werden, hoeveel er nog overbleven op de server, en hoe groot die berichten in totaal waren. Uit de SMTP logs is in elk geval voor elk e-mailbericht de afzender, bestemming, en datum zichtbaar; vaak bevat deze log nog andere gegevens.

Eén ISP beschikt niet over een SMTP log, en bewaart ook geen POP3 gegevens. Wel verwerkt deze ISP de miljoenen POP3 sessies per dag in zijn systeem tot alleen een registratie van het laatste tijdstip dat een gebruiker zijn mailbox raadpleegde.

Het volume aan verkeersgegevens voor het opvragen van e-mail ligt substantieel boven het volume voor toegangssessies. Een praktische schatting van enkele ISP's is 5 à 10 keer zoveel POP3 mailbox-loggegevens als toegangssessies per gebruiker. Gebruikers met vaste aansluitingen (kabelmodems, ADSL etc.) hebben de neiging frequenter de mailbox uit te vragen. Dat resulteert in zo'n 2,5 miljard records per maand voor alle ISP's samen.

Bestaande gegevens twaalf maanden bewaren

Naast mailbox logs kunnen gegevens over de individuele berichten worden gelogd (SMTP-logs). In de praktijk blijken deze verkeersgegevens door veel ISP's te worden gelogd, maar na een week te worden overschreven. Een ruwe schatting leert dat het Nederlandse e-mailverkeer ca. 60 miljoen records per dag, ofwel 1,8 miljard per maand oplevert[53].

De e-mail verkeersgegevens in zijn volledigheid opslaan levert dus een grotere belasting op dan alleen de toegangssessies registreren. Uitgaande van voorgaande schattingen leveren deze logs een volume van ongeveer 2,2 Terabyte per maand[54] voor alle ISP's samen, ofwel 26 Terabyte per jaar.

---

[52] In feite zegt de POP3 log alleen wanneer de e-mail client op de PC van de gebruiker de mailbox raadpleegde; de gebruiker hoeft daarbij niet aanwezig te zijn. Sommige gebruikers laten dit proces dag en nacht doorlopen.

[53] 11 miljoenen gebruikers die een paar e-mailberichten per dag ontvangen, die ieder meerdere servers doorlopen

[54] Per maand 2,5 miljard POP3 records van ieder 400 byte, en 1,8 miljard SMTP records van ieder 600 byte, levert 2080 Gigabyte, waar nog enige overhead bij komt

Een grote ISP, met 10% van de markt, heeft in dit geval ongeveer 2,6 Terabyte nodig. Voor een middelgrote ISP komt dit op ongeveer 260 Gigabyte.

De gegevens op CD of DVD branden leidt wederom tot veel lagere kosten: een grote ISP heeft dan twee DVD-jukeboxes voor in totaal 2,6 Terabyte nodig; bij een middelgrote ISP betreft het een kleinere DVD-jukebox met 260 Gigabyte.

POP3 en SMTP registreren en bewaren
Aangezien de meeste ISP's de POP3 en SMTP gegevens nu reeds registreren en voor enige tijd bewaren, zal een registratieplicht voor deze ISP's geen directe consequenties hebben. Eén van de ondervraagde ISP's beschikt niet over SMTP gegevens; voor deze aanbieder zou een registratieplicht inhouden dat deze afspraken moet maken met het bedrijf dat de e-mail dienst voor de ISP verzorgt zodat deze de gegevens bewaart, of aan de ISP overhandigt zodat deze ze kan bewaren.

7.2.5. Internetcafés

Zoals eerder gesteld registreren de internetcafés relatief weinig informatie; een bewaarplicht voor wat betreft de toegangsessies zou dan ook relatief weinig effect hebben. Anders ligt het voor de lokaal op de PC's opgeslagen informatie, zoals de "browser history" (lijst van bezochte websites), die momenteel zonder meer door de aanbieders overschreven wordt.

Bestaande gegevens twaalf maanden bewaren
IC1 bewaart een beperkte hoeveelheid gegevens voor wat betreft de toegangssessies. Door het lage volume is het zonder meer mogelijk deze gegevens twaalf maanden te bewaren.

Een bewaarplicht voor lokaal op de PC's opgeslagen informatie zou wel grote consequenties voor de aanbieders hebben, aangezien zij momenteel geen proces hebben om die informatie te bewaren. IC2 heeft zelfs geen centrale server en geen processen om informatie te registeren; deze partij zou zowel het netwerk als de bedrijfsvoering anders in moeten vullen om verkeersgegevens te kunnen registreren. IC1 heeft wel een centrale server; deze zou de software door de leverancier aan moeten laten passen en de centrale server uit moeten breiden. Het voert echter voor dit onderzoek te ver om de kosten van een dergelijk verandering in te schatten.

Toegangssessies registreren en bewaren
Kleinere internetcafés zoals IC2 hebben momenteel geen noodzaak om gegevens voor wat betreft toegangssessies te registreren. IC1 doet dit wel, met name omdat deze informatie door de veel grotere schaal van IC1 zinvol is voor marketingdoeleinden.

Om de toegangssessies te kunnen loggen zal een aanbieder een centrale DHCP server nodig hebben, die in staat is de gegevens te loggen. IC2 gebruikt de DHCP functie die in de ADSL router ingebouwd is, waardoor loggen in het geheel niet mogelijk is. Voor een dergelijk kleine aanbieder volstaat een vrij eenvoudige server; het beheer en de dagelijkse operatie wordt daarbij wel veel complexer, waardoor de aanbieder extra deskundigheid aan zal moeten trekken.

8. Conclusies en aanbevelingen

8.1 Algemeen

Uit het voorgaande blijkt dat de aanbieder van telecommunicatiediensten een groot deel van de informatie waar de opsporingsdiensten behoefte aan hebben, binnen de reguliere bedrijfsvoering registreren en verwerken. Zij doen dit om verschillende redenen, waarbij facturering de belangrijkste is.

De bewaartermijnen bij de aanbieders worden gedreven door de bedrijfsvoering en variëren van enkele dagen tot enkele maanden, of in sommige gevallen onbeperkt. In veel gevallen is de bewaartermijn korter dan de behoefte van de opsporingsdiensten; dezen geven aan dat, afhankelijk van het soort delict, een bewaartermijn van een jaar nodig kan zijn.

8.2 Beschikbaarheid van de benodigde verkeersgegevens per dienst

8.2.1. Vaste telefonie

Van de voor de opsporing benodigde gegevens bewaart de onderzochte aanbieder een groot deel; alleen de niet geslaagde gesprekken (call attempts) ontbreken. Bovendien zijn inkomende gesprekken vanuit andere netwerken moeilijk toegankelijk.

De aanbieder bewaart de gegevens momenteel voor vijf tot zes maanden.

8.2.2. Mobiele telefonie

De onderzochte aanbieders bewaren een groot deel van de voor de opsporing benodigde gegevens in het geval van geslaagde, uitgaande gesprekken. Bij GPRS ontbreekt echter het IP adres, en bij SMS ontbreekt in bepaalde gevallen informatie over zender of ontvanger, wanneer deze een ander netwerk heeft gebruikt.

Niet geslaagde gesprekken (call attempts) worden niet geregistreerd, of binnen enkele uren gewist. Verder registreert één van de aanbieders geen inkomende gesprekken vanuit andere netwerken.

Eén van de aanbieders bewaart de gegevens voor een jaar; de andere twee voor zes maanden.

8.2.3. Internettoegang

De meeste ISP's bewaren voor wat betreft de toegangsdienst de voor de opsporing benodigde sessiegegevens. Daarmee valt te herleiden welke gebruiker (user-ID) op welke tijden toegang had tot het internet, en met welk IP adres.

Gegevens over de computers waarmee een gebruiker contact heeft gehad (IP accounting) worden in de meeste gevallen niet geregistreerd in verband met de grote hoeveelheden informatie. Dit betekent ook dat diensten die geheel door gebruikers worden verzorgd (zogenaamde Peer-to-Peer diensten) in het geheel geen verkeersgegevens bij de ISP's genereren.

De ISP's kennen vaak geen vaste bewaartermijn; men gooit de gegevens weg zodra de betreffende computer te vol raakt, of men zet de gegevens op CD. De termijn kan daardoor variëren tussen enkele dagen en enkele maanden, of onbeperkt lang in het geval van CD's.

8.2.4. E-mail

De meeste onderzochte aanbieders bewaren een deel van de benodigde gegevens betreffende hun e-mail dienst; de situatie is echter nogal verschillend. Eén aanbieder bewaart niets, behalve het tijdstip van de laatste ophaalsessie per gebruiker; de anderen bewaren per bericht in elk geval zender, ontvanger, en tijdstip van verzending. Van de gevraagde informatie ontbreken in alle gevallen gegevens over het pad dat een bericht langs eerdere servers gevolgd heeft; alleen de laatste server is bekend.

Ook voor e-mail kennen de ISP's vaak geen vaste bewaartermijn. De termijn kan variëren tussen enkele dagen en enkele maanden, of onbeperkt lang in het geval van CD's.

8.2.5. Internetcafés

Van de onderzochte internetcafés bewaart één aanbieder in het geheel geen gegevens; de ander bewaart sessiegegevens per werkplek. Internetcafés zijn anoniem, waardoor er geen gegevens over de gebruiker beschikbaar zijn.

8.3 Ervaring met de opsporing

In de telefoniewereld worden historische verkeersgegevens regelmatig opgevraagd. Deze praktijk heeft een lange historie en de aanbieders zijn op de vraag vanuit de opsporing ingespeeld. Voor zover gegevens beschikbaar zijn, en voor zover er geen complexe analyse nodig is om de gevraagde gegevens te leveren, zijn zij goed in staat aan de vorderingen te voldoen.

Naast de wettelijke verplichting om gegevens aan te leveren, zien veel aanbieders ook een eigen maatschappelijke verantwoordelijkheid. Indien zij zelf het belang van een onderzoek inzien zijn zij eerder bereid vrijwillig uitvoeriger mee te werken.

Hoewel de opsporingsdiensten aangeven dat ook historische verkeersgegevens van ISP's bijzonder belangrijk voor ze zijn, blijkt het feitelijke aantal vorderingen nog zeer beperkt; het gaat tot nu toe om enkele tientallen per jaar voor een grote ISP, ofwel enkele honderden per jaar in totaal. Daarbij moet echter aangetekend worden dat de opsporingsdiensten nu nog zeer terughoudend zijn bij het opvragen van deze gegevens bij ISP's, omdat deze praktijk nog vrij recent is en de processen bij de aanbieders nog niet volledig zijn uitgewerkt. Het valt dan ook te verwachten dat de vraag naar historische verkeersgegevens bij ISP's in de toekomst fors zal toenemen. Ook het toenemende gebruik van het internet en het verdwijnen van "gratis" toegangsdiensten, waarbij NAW gegevens vaak niet bekend of niet betrouwbaar zijn, zullen bijdragen aan een toenemend gebruik van historische verkeersgegevens omtrent internet in de opsporing.

8.4 Consequenties van een eventuele bewaarplicht

Een bewaarplicht voor historische verkeersgegevens zou, voor zover deze verder gaat dan de huidige praktijk, voor de aanbieders vooral financiële consequenties hebben. Daarnaast kan een consequentie zijn dat aanbieders die zich tot nu toe profileren met een duidelijk privacybeleid, zich door een bewaarplicht minder goed kunnen differentiëren dan voorheen.

De additionele investeringen en operationele kosten hangen niet alleen af van de bewaartermijn, maar vooral van de gevraagde levertijd, het aantal vorderingen, en de complexiteit en structuur van de te stellen vragen. Daarnaast hangen de kosten sterk af van de gestelde eisen aan de betrouwbaarheid en de beschikbaarheid van gegevens. Verder kunnen er schaalvoordelen ontstaan indien aanbieders samen een oplossing laten implementeren, of indien zij de implementatie met andere veranderingen kunnen combineren.

Een bewaarplicht voor gegevens die nu al door de aanbieders geregistreerd worden zou, als er geen verdere eisen gesteld zouden worden, voornamelijk operationele kosten met zich meebrengen. De enige investering zou bij sommige aanbieders een extra CD of DVD brander zijn; anderen zouden hun servers enigszins moeten uitbreiden. In een dergelijke situatie zouden de aanbieders echter slechts een klein aantal vorderingen kunnen verwerken, en zou de levertijd van de gegevens meerdere werkdagen bedragen.

De kosten van het bewaren hangen dan ook sterk af van de te verwachten aantallen vorderingen en de gevraagde levertijd van verkeersgegevens. Deze factoren bepalen het medium en de architectuur van de opslag, en hebben daarmee grote consequenties voor de benodigde investeringen. Bij een levertijd van meerdere dagen kan men, bij kleine aantallen vorderingen, nog handmatig CD's opzoeken; om binnen uren te kunnen leveren is, zeker bij grotere aantallen vorderingen, een tape-robot, CD- of DVD-jukebox nodig, en om de tijd tot minuten terug te brengen of om nog grotere aantallen vorderingen aan te kunnen moeten de gegevens op een harddisk-systeem staan.

Verder is het voor een snelle levering noodzakelijk van te voren te weten op basis van welke gegevens gezocht zal moeten worden. Hiermee wordt namelijk de zoekstructuur van de gegevens gedefinieerd. Een goed voorbeeld is het Besluit Bijzondere Vergaring Nummergegevens Telecommunicatie[55], waarin specifiek wordt vastgelegd welke gegevens de in de vordering vermeld moeten zijn om de benodigde informatie te kunnen krijgen. De aanbieders kan de indicering (zoeksleutels) hier op aanpassen[56].

8.5 Aanbevelingen

Indien besloten wordt om een bewaarplicht in te voeren zal er een functioneel geformuleerd kader opgesteld moeten worden, waarin de basisregels vastgelegd zijn. Vervolgens zullen deze regels per telecommunicatiedienst uitgewerkt moeten worden; met name moet per dienst bepaald worden welke gegevens bewaard moeten worden en voor hoe lang, en op basis van welke gegevens een vordering opgesteld kan worden.

[55] Gepubliceerd in Stb. 2002, 31

[56] In het genoemde besluit gaat het om locatie en tijdstip; een aanbieder zal in dat geval een index opzetten bestaande uit zendmast en tijdstip, naast de meer gebruikelijke index bestaande uit IMSI en tijdstip

Binnen dit onderzoek is slechts een beperkt aantal telecommunicatiediensten onderzocht. De resultaten zijn niet zonder meer toepasbaar op andere telecommunicatiediensten, zoals websurfen, website hosting, Peer-to-Peer file sharing, Voice over IP (VoIP), en chat (Internet Relay Chat, IRC). Om regels voor deze diensten op te kunnen stellen zal dan ook verder onderzoek nodig zijn. De regels zullen bovendien regelmatig aangevuld moeten worden vanuit de nieuwste stand van de techniek en van de markt.

Het onderzoek was gericht op de aanbieders, en heeft daarmee slechts een deel van Actiepunt 17 uitgevoerd. Naast dit deel geldt het actiepunt nog onderzoek naar de belemmeringen die de opsporing ondervindt door de afwezigheid van bewaarplichten voor historische verkeersgegevens, en het versterken van de mogelijkheden van analyse van internationaal telefoonverkeer.

Bijlage A: Gebruikte afkortingen

ADSL	Asymmetric Digital Subscriber Line
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMS-IX	Amsterdam Internet Exchange
APN	Access Point Name
CD	Compact Disk
CDR	Call Detail Record
CLI	Calling Line Identifier
CMTS	Cable Modem Termination System
DGTP	Directoraat Generaal Telecommunicatie en Post
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSLAM	Digital Subscriber Line Access Multiplexer
DVD	Digital Versatile Disk
FTP	File Transfer Protocol
GB	Gigabyte
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HD	Hard Disk
HTTP	Hyper Text Transfer Protocol
I&V	Inlichtingen en Veiligheid
IMAP	Internet Mail Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
KLPD	Korps Landelijke Politiediensten
LAN	Local Area Network
MAC	Media Access Control
MB	Megabyte
MMS	Multimedia Message Service
Modem	Modulator – Demodulator
MVNO	Mobile Virtual Network Operator
NAT	Network Address Translation
NAW	Naam, Adres en Woonplaats
PC	Personal Computer
PDP	Packet Data Protocol
PIDS	Platform voor Interceptie Decryptie en Signaalanalyse
POP3	Post Office Protocol version 3
PSTN	Public Switched Telephone Network
RADIUS	Remote Access Dial In User Service
RAID	Redundant Array of Independent Disks

SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Centre
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transaction Control Protocol / Internet Protocol
TKGP	Trunk Group
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VoIP	Voice over IP
WAP	Wireless Application Protocol
WBP	Wet Bescherming Persoonsgegevens
WiFi	Wireless Fidelity
W-LAN	Wireless Local Area Network
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Bijlage B: Behoefte van de opsporing

Tabel 1: Relevante verkeersgegevens bij mobiele telefoniediensten

Verkeersgegeven	Uitleg
GSM algemeen	
MSISDN	Mobile Station ISDN. Het nummer waarmee een mobiel station bereikbaar is. Het bestaat uit de internationale prefix, landcode, eventuele regiocode, en abonneenummer. Het is door de aanbieder direct gekoppeld aan de IMSI code. Dit nummer kan gekoppeld worden aan de NAW gegevens van de houder in het geval van Post-paid. Bij Pre-paid klanten is deze koppeling vaak niet te maken aangezien de NAW gegevens niet bekend zijn.
IMSI	International Mobile Subscriber Identity. De unieke identificatiecode van een abonnee in het GSM/GPRS netwerk. Het nummer bestaat uit de landcode, netwerkcode en MSIN[57]. Deze identiteit kan gekoppeld worden aan de NAW gegevens van de houder in het geval van Post-paid. Bij Pre-paid klanten is deze koppeling vaak niet te maken aangezien de NAW gegevens niet bekend zijn. De IMSI is opgeslagen op de SIM[58]-kaart.
IMEI	International Mobile Equipment Identity. Hardware code van het gebruikte mobiele apparaat.
Datum / tijd	De begintijd van een dienst of gesprek.
Locatie	Locatie van de mobiele eindgebruiker. De locatie bij de start en bij het eind van een sessie kan gegeven worden.
Type dienst	Welk type GSM dienst wordt gebruikt. Voorbeelden hiervan zijn: fax, data, spraak, SMS.
Status	Status geeft de omstandigheden aan betreffende een specifieke sessie. De parameter "'Succesful/Unsuccesful" geeft aan of een poging tot het opzetten van een sessie is gelukt en "Cause for Release" geeft de reden van het afbreken van een sessie aan, hetgeen inzicht biedt in de omstandigheden waaronder een sessie is beëindigd.
GSM (circuitgeschakeld) specifiek	
Identiteit bestemming	Het gebelde nummer (B-nummer) dan wel het daadwerkelijk bereikte nummer. Deze identiteit kan gekoppeld worden aan een geografische locatie van de aansluiting of aan de NAW gegevens van de houder.
IMSI (gebelde)	In het geval er een mobiel nummer gebeld werd: de IMSI van de gebelde
IMEI (gebelde)	In het geval er een mobiel nummer gebeld werd: de IMEI van het toestel van de gebelde
Locatie (gebelde)	In het geval er een mobiel nummer gebeld werd: de locatie (cell ID) van de gebelde
Duur	Tijdsduur tussen beantwoording en gesprekseinde
GPRS specifiek	
APN (GPRS)	Het APN is de benaming van de bestemming voor alle data

[57] MSIN: Mobile Subscriber Identity Number

[58] SIM: Subscriber Identity Module; Identiteitskaart die in het mobiele apparaat.

	vanaf een mobiel apparaat, waar vandaan de data verder wordt doorgegeven naar de eindbestemming. Aangezien verschillende APN's gebruikt kunnen worden voor bijvoorbeeld een koppeling met het openbare internet, de WAP gateway of een directe verbinding met het bedrijfsnetwerk, geeft het APN informatie over het type dienst tijdens een GPRS sessie;
PDP identiteit (GPRS)	De tijdelijke identiteit toegekend voor een sessie aan een GPRS gebruiker. Dit is in het algemeen een IP-adres.
Volume data (GPRS)	Het ingaande en uitgaande volume aan data dat een gebruiker gedurende een sessie heeft verstuurd en ontvangen.
SMS specifiek	
MSISDN (ontvanger)	Het nummer van de ontvanger
IMSI (ontvanger)	De IMSI van de ontvanger
IMEI (ontvanger)	Het IMEI van het toestel waarop het bericht werd ontvangen
SMSC	Het knooppunt vanwaar SMS berichten worden verstuurd en afgeleverd.
Datum / tijd aflevering	Het tijdstip dat het bericht daadwerkelijk wordt afgeleverd
Volume	Het aantal tekens in een bericht
Locatie (ontvanger)	De locatie (cell ID) van de ontvanger op het moment dat het bericht wordt afgeleverd

Tabel 2: Relevante verkeersgegevens bij vaste telefoniediensten

Verkeersgegeven	Uitleg
Identiteit aansluiting	A-nummer: De unieke identiteit van de fysieke aansluiting. Deze identiteit kan gekoppeld worden aan een geografische locatie van de aansluiting of aan de NAW gegevens van de houder.
Identiteit aansluiting van bestemming	B-nummer: De unieke identiteit van de fysieke aansluiting van de bestemming. Deze identiteit kan gekoppeld worden aan een geografische locatie van de aansluiting of aan de NAW gegevens van de houder.
Type dienst	Spraak, fax of data. Alleen relevant voor ISDN en niet voor PSTN.
Datum / tijd / duur	Tijdstip van sessie.
Status	Status geeft de omstandigheden aan betreffende een specifieke sessie. De parameter "'Succesful/Unsuccesful" geeft aan of een poging tot het opzetten van een sessie is gelukt en "Cause for Release" geeft de reden van het afbreken van een sessie aan, hetgeen inzicht biedt in de omstandigheden waaronder een sessie is beëindigd.

Tabel 3: Relevante verkeersgegevens bij toegangsdiensten

Verkeersgegeven	Uitleg
• Identiteit aansluiting	De fysieke aansluiting gebruikt voor toegang tot het netwerk krijgt een unieke identiteit. Deze identiteit kan gekoppeld worden aan een geografische locatie van de

Verkeersgegeven	Uitleg
	aansluiting of aan de NAW gegevens van de houder. Voorbeelden hiervan zijn: Nummeridentificatie (CLI)[59] bij dial-up diensten, IMSI[60] bij GSM/GPRS, MAC adres bij Ethernet / W-LAN
• Identiteit gebruiker	User-ID: een gegeven waarmee de bijbehorende gebruikersgegevens gevonden kunnen worden.
• Identiteit transportlaag	De eindgebruiker van de toegangsdienst krijgt een unieke identiteit ten behoeve van de transportdienst. Alle overige sessiegegevens kunnen op die manier gekoppeld worden aan een eindgebruiker. Voorbeelden hiervan zijn: tijdelijk of permanent IP adres.
• Begin en eind aansluitsessie	De start- en stoptijdstip van de sessie waarin een eindgebruiker of systeem gebruik maakt van de toegangsdienst.
• Begin en eind dienstsessie	De start- en stoptijd van de tijd dat een eindgebruiker gebruik maakt van een bepaalde dienst over het netwerk. De relevantie van het gegeven is niet begrensd tot die diensten die door de eigen ISP wordt geleverd.
• Target host	Het IP adres en hostname van de computer waarmee verbinding werd gezocht.
• Source host	Het IP adres en hostname van de computer waarvandaan gecommuniceerd werd.
• Type dienst	Welk type dienst is aangeroepen tijdens het gebruik van de toegangsdienst. Voorbeelden hiervan zijn: e-mail, HTTP (websurfen), chat, VoIP en FTP.
• Routing transportlaag	Gegevens die worden uitgewisseld tussen de eindgebruiker en alle voor hem bereikbare netwerken volgen een bepaalde route. Van deze route kan de eerstvolgende host in keten geregistreerd worden.
• Routing dienst	Ongeacht de routering op de transportlaag kan een op dienstniveau een herroutering plaatsvinden. Het gevraagde gegeven is de computer die de dienst routeert. Voorbeelden zijn: anonymous re-mailers, mirror servers, VoIP gateways
• Volume	Eindgebruikers genereren een aantal bytes en packets tijdens een sessie (zowel uplink als downlink). Dit gegeven kan een inzicht bieden over de uitgewisselde informatie.

Tabel 4: Relevante verkeersgegevens bij e-mail

Verkeersgegeven	Uitleg

[59] CLI: Calling Line Id (ook wel Nummeridentificatie of A-nummer). Identificeert een telefoonaansluiting. Bij ISDN kunnen er meerdere CLI's per aansluiting zijn.

[60] IMSI: International Mobile Subscriber Identity, identiteit op de SIM kaart. Identificeert een mobiele aansluiting.

Verkeersgegeven	Uitleg
• E-mail adres zender	Legt de koppeling tussen e-mail bestand en de identiteit van de eigenaar van het e-mail adres dat door de zender is gebruikt. De identiteit van de eigenaar en de zender hoeven niet noodzakelijk één en dezelfde te zijn.
• IP adres zender	IP adres van de computer waarvandaan de e-mail verstuurd werd
• Datum / tijd verzending, doorgifte, etc	Datum en tijd dat de e-mail verstuurd werd; naast het algemene nut van deze informatie is dit gegeven noodzakelijk om een dynamisch IP adres aan een gebruiker te koppelen.
• Message-ID (RFC-822)	Unieke identiteit van het e-mail bericht, nodig om het bericht in de verdere keten te kunnen volgen.
• Onderwerp	Onderwerp van het e-mail bericht.
• Status	Status geeft weer of een e-mail succesvol bezorgd is.
• Grootte (bytes)	De grootte van het e-mail bericht. Geeft tevens een indicatie van het soort gegevens dat verstuurd is.
• Naam en IP adres van eventuele SMTP Relays	Gebruikte servers om het bericht door te routeren; dit kan relevant zijn om de uiteindelijke ontvanger te traceren.
• Mailbox server ontvanger	Geeft aan welke server gebruikt werd door de ontvanger en hoe de ontvanger de e-mail ontving (POP3, IMAP, webmail)
• E-mail adres ontvanger(s)	Het e-mail adres van de ontvanger kan de koppeling zijn met de identiteit van de ontvangende eindgebruiker.
• Datum / tijd opvragen e-mail	De datum / tijd waarop de gebruiker de inhoud van zijn mailbox opgevraagd heeft, ongeacht of er daadwerkelijk berichten waren.

Tabel 5: Relevante gegevens bij diensten van internetcafés

Gegeven	**Uitleg**
Identiteit gebruiker	Het gebruik en de betaling van de dienst staat in direct verband met de eindgebruiker van de dienst. In werkelijkheid is de gebruiker echter anoniem.
Datum / tijd /duur gebruik werkplek	Het begin- en eindtijdstip van het gebruik van de werkplek.
Betalingsgegevens	Voor het gebruik van de diensten van een internetcafé moet betaald worden. De manier waarop het gebruik betaald wordt kan wel (pin, creditcard) of geen (contant) gegevens opleveren omtrent de gebruiker (strikt genomen geen verkeersgegeven).
Identiteit transportlaag	Adres van de werkplek waarop wordt ingelogd. Dit gegeven koppelt de werkplek aan de eindgebruiker en alle overige sessiegegevens kunnen op die manier gekoppeld worden aan een eindgebruiker. De eindgebruiker is echter in het algemeen

Gegeven	Uitleg
	anoniem.
Begin en eind aansluitsessie	De start- en stoptijdstip van de sessie waarin een eindgebruiker of systeem gebruik maakt van de toegangsdienst. Wanneer internetcafé gebruik maakt van een permanente verbinding voor alle werkplekken, bijvoorbeeld van een ADSL verbinding of een huurlijn, dan heeft dit gegeven geen betekenis.
Begin en eind dienstsessie	De start- en stoptijd van de tijd dat een eindgebruiker gebruik maakt van een bepaalde dienst over het netwerk. De relevantie van het gegeven is niet begrensd tot die diensten die door de eigen ISP wordt geleverd.
Target host	Het IP adres en hostname van de computer waarmee verbinding werd gezocht.
Source host	Het IP adres en hostname van de computer waarvandaan gecommuniceerd werd.
Type dienst	Welk type dienst is aangeroepen tijdens het gebruik van de toegangsdienst. Voorbeelden hiervan zijn: e-mail, HTTP (websurfen), chat, VoIP en FTP.
Routing transportlaag	Gegevens die worden uitgewisseld tussen de eindgebruiker en alle voor hem bereikbare netwerken volgen een bepaalde route. Van deze route kan de eerstvolgende host in keten geregistreerd worden.
Routing dienst	Ongeacht de routering op de transportlaag kan een op dienstniveau een herroutering plaatsvinden. Het gevraagde gegeven is de computer die de dienst routeert. Voorbeelden zijn: anonymous re-mailers, mirror servers, VoIP gateways
Volume	Eindgebruikers genereren een aantal bytes en packets tijdens een sessie (zowel uplink als downlink). Dit gegeven kan een inzicht bieden over de uitgewisselde informatie.

Bijlage C: Beschikbaarheid verkeersgegevens

Vaste telefoniediensten

Tabel 6: Algemene bewaarinformatie, vaste telefonie

Operator	Bewaartermijn	Oslag medium	Opmerkingen
• OP1	5 maand tot 6 maanden	HD[61]	Bijbehorende facturen worden enkele jaren bewaard voor eventueel financieel onderzoek.

Tabel 7: Verkeersgegeven specifieke beschikbaarheidsinformatie, vaste telefonie

Verkeersgegeven	Opmerking
• Identiteit aansluiting	Het A-nummer is beschikbaar. Het toestelnummer vanuit een bedrijfsnetwerk is niet altijd beschikbaar.
• Identiteit aansluiting van bestemming	Het B-nummer is beschikbaar.
• Type dienst	Type dienst is beschikbaar bij ISDN. Niet van toepassing bij PSTN.
• Datum / tijd / duur	De timestamp van een sessie is beschikbaar.

Call attempts worden niet geregistreerd. Deze functionaliteit is in principe wel beschikbaar in de centrale maar wordt niet toegepast.

Verkeersgegevens voor inkomende gesprekken worden wel geregistreerd maar komen niet in de database waarover de security operatie direct de beschikking heeft. Dit betekent dat het een grotere inspanning vergt deze informatie te vergaren.

Mobiele telefoniediensten

Tabel 8: Algemene bewaarinformatie per aanbieder van mobiele telefonie

Operator	Bewaartermijn	Opslag medium	Opmerkingen
• OP2	6 maanden	HD / CD[62]	Ongeveer 260Gb aan data. De back-up op CD wordt onbeperkt bewaard.
• OP3	1 jaar	CD	De data wordt per 7 dagen op 4 CD's aangeleverd. Nadat de bewaartermijn is verstreken worden de CD's vernietigd.
• OP4	6 maanden	HD	Roterend bewaard (nieuwste maand vervangt oudste).

[61] HD: Hard Disk (vaste schijf)
[62] CD: Compact Disk

Tabel 9: Verkeersgegeven specifieke beschikbaarheidinformatie mobiele telefonie

Verkeersgegeven	Beschikbaarheid verkeersgegeven (uit 3 operators)	Opmerking
GSM		
Verkeersgegevens met betrekking tot de beller		
• MSISDN	OP2, OP3, OP4	
• IMSI[63]	OP2, OP3, OP4	Bij OP3 is de IMSI niet opgenomen in de security database.
• IMEI	OP2, OP3, OP4	
• Datum / tijd / duur	OP2, OP3, OP4	
• Locatie (tijdgebonden)	OP2, OP3, OP4	Locatie van het begin en einde gesprek o.b.v. Cell-ID; Niet beschikbaar bij roaming gesprekken en bij doorgeschakelde gesprekken.
• Type dienst	OP2, OP3, OP4	Bij OP2 is deze informatie in de securitydatabase aanwezig.
• Status	OP3	OP3 beschikt over de ‘cause for release’
Verkeersgegevens met betrekking tot de gebelde		
• MSISDN	OP2, OP3, OP4	
• IMSI	OP2, OP3, OP4	Alleen beschikbaar wanneer de gebelde een eigen klant is. Bij OP3 is dit gegeven niet opgenomen in de security database.
• IMEI	OP2, OP3, OP4	Alleen beschikbaar wanneer de gebelde een eigen klant is. Bij OP3 is dit gegeven niet opgenomen in de security database.
• Locatie (tijdgebonden)	OP2, OP3, OP4	Alleen beschikbaar wanneer de gebelde een eigen klant is. Bij OP3 is dit gegeven niet opgenomen in de security database.
GPRS		
• MSISDN	OP2, OP3, OP4	
• IMSI	OP2, OP3, OP4	Bij OP3 is dit gegeven niet opgenomen in de security database.
• IMEI	OP2, OP3, OP4	
• Datum / tijd / duur van aansluitsessie	OP2, OP3, OP4	
• Locatie (tijdegebonden)	OP2, OP3, OP4	O.b.v. Cell-ID.
• APN (GPRS)	OP2, OP3, OP4	
• Volume data (GPRS)	OP2, OP3, OP4	
• PDP identiteit (GPRS): IP-adres	-	Niet beschikbaar

[63] IMSI: International Mobile Subscriber Identity, identiteit op de SIM kaart. Identificeert een mobiele aansluiting.

Verkeersgegeven	Beschikbaarheid verkeersgegeven (uit 3 operators)	Opmerking
• Begin en eind dienstsessie	-	Niet beschikbaar.
• Target / source host	-	Niet beschikbaar.
• Type dienst	-	Niet beschikbaar.
• Routing transportdienst	-	Niet beschikbaar.
• Routing dienst	-	Niet beschikbaar.
SMS		
Verkeersgegevens met betrekking tot de zender		
• MSISDN	OP2, OP3, OP4	
• IMSI	OP2, OP3, OP4	Bij OP3 is dit gegeven niet opgenomen in de security database.
• IMEI	OP2, OP3, OP4	
• SMSC	OP2, OP4, OP3	
• Datum / tijd	OP2, OP3, OP4	
• Volume	-	Niet beschikbaar.
• Locatie (tijdgebonden)	OP2, OP3, OP4	O.b.v. Cell-ID; Niet beschikbaar wanneer beller in het buitenland is.
Verkeersgegevens met betrekking tot de ontvanger		
• MSISDN	OP2, OP3, OP4	Alleen beschikbaar bij eigen SMS-C
• IMSI	OP2, OP3, OP4	Alleen beschikbaar voor de ontvanger wanneer deze eveneens een eigen klant is.
• IMEI	OP2, OP3, OP4	Alleen beschikbaar voor de ontvanger wanneer deze eveneens een eigen klant is.
• SMSC	OP2, OP3, OP4	Alleen beschikbaar voor de ontvanger wanneer deze eveneens een eigen klant is.
• Locatie	OP2, OP3, OP4	Alleen beschikbaar voor de ontvanger wanneer deze eveneens een eigen klant is.

Toegangsdiensten

Voor de toegangsdiensten wordt de beschikbaarheid van de in hoofdstuk vier geïdentificeerde verkeersgegevens waaraan de opsporing behoefte heeft, per geïnterviewde ISP gepresenteerd in een tabel. Een opdeling per dienst is gemaakt op:

- algemene bewaarinformatie per ISP;
- de beschikbaarheid van specifieke verkeersgegevens.

Algemene bewaarinformatie betreft de bewaartermijn, het opslagmedium, het soort logging en additionele opmerkingen per dienst. De beschikbaarheid van een verkeersgegevens wordt gespecificeerd door het noemen van de ISP's die over een specifiek verkeersgegeven beschikken. Toegevoegd is hoeveel dit er in totaal zijn waarbij opgemerkt wordt dat niet alle ISP's een bepaalde dienst aanbieden.

Inbel verkeersgegevens

Tabel 10: Algemene bewaarinformatie per ISP: inbeldienst

ISP	Bewaartermijn	Opslag medium	RADIUS/DHCP/ IP accounting	Opmerkingen
• ISP1	6 maanden, afhankelijk van ruimte op server	HD	N/N/J	De IP accounting logs zijn nog nooit opgevraagd
• ISP2	Onbeperkt	CD	J/N/N	
• ISP3	7 dagen, roterend	HD	J/N/N	
• ISP4	Zeer beperkt, roterend	HD	J/N/N	Meestal slechts enkele dagen
• ISP5	1 maand, zal teruggaan naar 1 week	HD	J/N/N	
• ISP6	3 maanden	HD/CD	J/N/N	Eerst op HD dan op CD. CD wordt vernietigd wanneer 3 maanden om zijn
• ISP7	Onbeperkt	HD/Tape	J/N/N	

Tabel 11: Specifieke beschikbaarheidinformatie: verkeersgegevens m.b.t. inbeldienst

Verkeersgegeven	Beschikbaarheid verkeersgegeven uit 7 ISP's	Opmerking
• Identiteit aansluiting	7: ISP1-07	Nummeridentificatie (CLI) is bekend, indien niet onderdrukt. ISP7 weigert toegang bij onderdrukte nummeridentificatie
• Identiteit gebruiker (user-ID)	6: ISP2-ISP7	
• Identiteit transportdienst (IP adres)	7: ISP1-07	ISP1: IP adres uit IP accountinglog; overigen uit RADIUS
• Begin en eind aansluitsessie	6: ISP2-07	ISP1: deels te herleiden uit IP accountinglog
• Begin en eind dienstsessie	0	ISP1: deels te herleiden uit IP accountinglog
• Target / source host	1: ISP1	ISP1: uit IP accountinglog
• Type dienst	0	ISP1: valt soms uit target host te herleiden
• Routing transportdienst	1: ISP1	ISP1: uit IP accountinglog

Verkeersgegeven	Beschikbaarheid verkeersgegeven uit 7 ISP's	Opmerking
• Routing dienst	0	
• Volume	7: ISP1-07	ISP5: slechts voor een deel van de klanten direct toegang tot volume gegevens

ADSL

Tabel 12: Algemene bewaarinformatie per ISP: ADSL

ISP	Bewaartermijn	Opslag medium	RADIUS/DHCP/ IP accounting	Opmerkingen
• ISP1	n.v.t.	n.v.t.	n.v.t.	Geen ADSL
• ISP2	n.v.t.	n.v.t.	N/J/N	Geen sessie of volume gegevens van 3e partij; niet bekend of 3e gegevens opslaat
• ISP3	7 dagen	HD	J/N/N	Geen intermediate accounting[64]
• ISP4	Enkele dagen tot 3 maanden	HD	J/N/N	Intermediate accounting elk uur
• ISP5	7 dagen	HD	N/J/N	Geen intermediate accounting
• ISP6	3 maanden	HD/CD	J/N/N	Eerst op HD dan op CD. CD wordt vernietigd wanneer 3 maanden om zijn
• ISP7	-	HD	J/N/N	Nog in ontwikkeling

Tabel 13: Specifieke beschikbaarheidinformatie: verkeersgegevens m.b.t. ADSL

Verkeersgegeven	Beschikbaarheid verkeersgegeven uit 6 ISP's	Opmerking
• Identiteit aansluiting	ISP3, ISP4, ISP5, ISP6	MAC adres (is te vervalsen). ISP5: toekomstig ook circuit-id, waardoor fysieke aansluitlijn bekend is.
• Identiteit gebruiker (user-ID)	ISP3, ISP4, ISP6	ISP2, ISP5: Geen koppeling tussen MAC adres en eindgebruiker
• Identiteit transportdienst (IP adres)	ISP3, ISP4, ISP6	
• Begin en eind	ISP3, ISP4, ISP5,	

[64] *ADSL sessies kunnen soms maanden duren vanwege het always on karakter van de dienst. Om toch informatie in de log op te nemen voordat de sessie wordt afgebroken, wat na de factuurdatum kan zijn, wordt door sommige partijen intermediate (tussentijdse) billing toegepast.*

Verkeersgegeven	Beschikbaarheid verkeersgegeven uit 6 ISP's	Opmerking
aansluitsessie	ISP6	
• Begin en eind dienstsessie	-	
• Target / source host	-	
• Type dienst	-	
• Routing transportdienst	-	
• Routing dienst	-	
• Volume	ISP3, ISP4, ISP6	ISP3, ISP6: Per IP adres totaalvolume count

Kabel

Eén ISP binnen de interviewgroep levert kabeldiensten.

Tabel 14: Algemene bewaarinformatie per ISP: kabel

ISP	Bewaartermijn	Opslag medium	RADIUS/DHCP/ IP accounting	Opmerkingen
• ISP6	3 maanden	HD/CD	N/J/N	Eerst op HD dan op CD. CD wordt vernietigd wanneer 3 maanden om zijn

Tabel 15: Specifieke beschikbaarheidinformatie: verkeersgegevens m.b.t. kabel

Verkeersgegeven	Beschikbaarheid verkeersgegeven uit 1 ISP	Opmerking
• Identiteit aansluiting	1: ISP6	Op het MAC adres van de modem in bruikleen. Aansluiting niet exact te traceren a.g.v. busarchitectuur
• Identiteit transportdienst	1: ISP6 (IP adres)	Uit DHCP log
• Begin en eind aansluitsessie	1: ISP6	Uit DHCP log
• Begin en eind dienstsessie	-	
• Target / source host	-	
• Type dienst	-	
• Routing transportdienst	-	
• Routing dienst	-	
• Volume	1: ISP6	Per IP adres totaalvolume count

Huurlijn

Tabel 16: Algemene bewaarinformatie per ISP: huurlijn

ISP	Bewaartermijn	Opslag medium	RADIUS/DHCP/ IP accounting	Opmerkingen
• ISP1	6 maanden, afhankelijk van ruimte op server	HD	N/N/J	nu IP accounting per 5 minuten; van plan dit af te schaffen
• ISP3	n.v.t.	n.v.t.	N/N/N	Alleen totaal volume per tijdseenheid
• ISP4	n.v.t.	n.v.t.	N/N/N	Niets geregistreerd
• ISP7	n.v.t.	n.v.t.	N/N/N	Alleen totaal volume per tijdseenheid, uitgesplitst naar on-net, AMS-IX, en Internationaal

Tabel 17: Specifieke beschikbaarheidinformatie: verkeersgegevens m.b.t. toegang via huurlijn

Verkeersgegeven	Beschikbaarheid verkeersgegeven uit 4 ISP's	Opmerking
• Identiteit aansluiting	-	Altijd bekend bij Huurlijn verbindingen
• Identiteit transportdienst (IP adres)	Alle	Vast IP adres bij Huurlijn verbindingen
• Identiteit gebruiker (user-ID)	-	n.v.t.
• Begin en eind aansluitsessie	-	n.v.t.
• Begin en eind dienstsessie	-	ISP1: deels te herleiden uit IP accountinglog
• Target / source host	1: ISP1	ISP1: uit IP accountinglog
• Type dienst	-	ISP1: valt soms uit target host te herleiden
• Routing transportdienst	1: ISP1	ISP1: uit IP accountinglog ISP7: Totalen gesplitst naar On-Net, AMS-IX, Internationaal
• Routing dienst	-	
• Volume	3: ISP1, ISP3, ISP7	ISP1: uit IP accounting ISP3: Per IP adres totaalvolume

Verkeersgegeven	Beschikbaarheid verkeersgegeven uit 4 ISP's	Opmerking
		ISP7: verkeersstatistieken

E-mail

Tabel 18: Algemene bewaarinformatie per ISP: e-mail

ISP	Bewaartermijn	Opslag medium	Opmerkingen
• ISP1	1 maand, soms langer afhankelijk van ruimte op server	HD	Alleen voor klanten die gebruik maken van ISP1's batch SMTP dienst
• ISP2	POP3 wordt verwerkt, daarna weggegooid. SMTP log geheel niet beschikbaar.	HD	Na verwerking blijft alleen datum/tijd laatste keer POP3-access per account over
• ISP3	1 week	HD	Er zijn meerdere logs van functioneel dezelfde machines. Architectuur van mailsysteem verandert per maand
• ISP4	Enkele dagen	HD	Bewaartijd variabel i.v.m. storingen of technische problemen
• ISP5	1 week	HD	Maillogs staan verspreid over verschillende servers, er is geen back up faciliteit.
• ISP6	3 maanden	CD	
• ISP7	n.v.t.	n.v.t.	Biedt geen e-mail aan

Tabel 19: Specifieke beschikbaarheidinformatie: verkeersgegevens m.b.t. e-mail

Verkeersgegeven	Beschikbaarheid (uit 6 ISP's)	Opmerkingen
• E-mail adres afzender	5: ISP1, ISP3, ISP4, ISP5, ISP6	Kan vals zijn
• IP adres afzender	3: ISP1, ISP5, ISP6	Alleen voor e-mail verzonden door de eigen klanten
• Datum/tijd verzending, doorgifte, etc	5: ISP1, ISP3, ISP4, ISP5, ISP6	ISP2 heeft wel de timestamp van de laatste POP3-sessie
• Message-ID (RFC-822)	3: ISP1, ISP5, ISP6	ISP3 heeft dit voor een deel van de berichten
• Onderwerp	-	Wordt door de ISP's als inhoud beschouwd en niet als verkeersgegeven
• Status	3: ISP1, ISP5, ISP6	ISP3 heeft dit voor een deel van de berichten

Verkeersgegeven	Beschikbaarheid (uit 6 ISP's)	Opmerkingen
• Volume (bytes)	3: ISP1, ISP3, ISP6	
• Naam & IP adres van zendend SMTP systeem	5: ISP1, ISP3, ISP4, ISP5, ISP6	
• E-mail adres ontvanger(s)	5: ISP1, ISP3, ISP4, ISP5, ISP6	

Overig e-mail: één aanbieder is van plan spam-assessment voor zakelijke klanten te implementeren; dit levert een profiel van vroegere e-mail contacten in versleutelde (binaire) vorm in een "white list" van die klant. Deze informatie is niet terug te herleiden tot een lijst van contacten, wel kan men controleren of een gegeven e-mail adres in de "white list" voorkomt.

Internetcafés

Tabel 20: Algemene bewaarinformatie per internetcafé

IC	Bewaartermijn	Opslag medium	Opmerkingen
• IC01	meerdere maanden	HD	Bij de verkoop wordt de user-ID op de anonieme gebruikerskaart, de datum en tijd, en de prijs gelogd. Bij het gebruik wordt het werkstation, de user-ID, begin- en eindtijd, het aantal bytes (in/uit), en voor urenkaarten het tegoed gelogd. Voor toegang tot de volledige logs moet de beheersorganisatie worden ingeschakeld.
• IC02	n.v.t.	n.v.t.	Er wordt niets bewust gelogd; eventueel blijft informatie (history, cache) op de PC's staan tot de volgende keer dat de PC opgeschoond wordt (ongeveer eens per week).

Tabel 21: Specifieke beschikbaarheidinformatie: verkeersgegevens m.b.t. internetcafés

Verkeersgegeven	Beschikbaarheid (uit 2 internetcafés)	Opmerkingen
Identiteit gebruiker	-	Klanten zijn anoniem; betaling is altijd contant.
Datum / tijd /duur gebruik werkplek	IC1	Gebruik van werkplek wordt gelogd door de beheersapplicatie bij IC1. IC2 noteert de starttijd op papier en rekent af wanneer de klant de sessie heeft beëindigd, waarna het papier

Verkeersgegeven	Beschikbaarheid (uit 2 internetcafés)	Opmerkingen
		wordt.weggegooid.
Betalingsgegevens	-	Alleen contant. IC1 overweegt het toestaan van credit card betalingen maar het contant betalen blijft het voornaamst.
Identiteit transportlaag	IC1	IC1: werkstations hebben een vast IP-adres.
Begin en eind aansluitsessie	n.v.t.	IC1 en IC2 gebruiken respectievelijk een huurlijn en een ADSL verbinding. Beide internetcafés beëindigen de aansluitsessie in principe nooit.
Begin en eind dienstsessie	-	Geen logging vindt plaats van de activiteiten van gebruikers.
Target host	-	
Source host	-	
Type dienst	-	
Routing transportlaag	-	
Routing dienst	-	
Volume	IC1	De beheersorganisatie registreert het ingaande en uitgaande volume per werkstation.

Bijlage D: Behoefte van de opsporing versus beschikbaarheid

In de onderstaande tabellen wordt de eerder beschreven behoefte van de opsporingsdiensten (in de linkerkolom) uitgezet tegen de gegevens die de aanbieders registreren en bewaren.

Vaste Telefoniediensten

Tabel 22: Verkeersgegevens bij vaste telefoniediensten

Welke gegevens worden geregistreerd en bewaard:

Verkeersgegeven	Bewaard?	Opmerking
Identiteit aansluiting (A-nummer)	Ja	
Identiteit aansluiting van bestemming (B-nummer)	Ja	
Type dienst	Ja	
Datum / tijd / duur	Ja	
Status	Ja	Niet in security applicatie, daardoor moeilijker te verkrijgen

Voor welke types gesprekken worden bovenstaande gegevens geregistreerd en bewaard:

Type	Bewaard?	Opmerking
Beantwoord, uitgaand gesprek	Ja	
Onbeantwoord, uitgaand gesprek	Nee	Bij de meeste aanbieders niet geregistreerd; bij één aanbieder wel geregistreerd maar binnen enkele uren verwijderd
Beantwoord, inkomend gesprek	Meestal wel	In interconnectiesysteem, niet in security applicatie; daardoor moeilijker te verkrijgen. Eén aanbieder registreert deze gesprekken niet.
Onbeantwoord, inkomend gesprek	Nee	Bij de meeste aanbieders niet geregistreerd; bij één aanbieder wel geregistreerd maar binnen enkele uren verwijderd

Mobiele Telefoniediensten

Tabel 23: Verkeersgegevens bij mobiele telefoniediensten

Verkeersgegeven	Bewaard?	Opmerking
GSM algemeen		
MSISDN	In de meeste gevallen wel, bij sommige diensten niet	Is anders via IMSI te achterhalen
IMSI	Ja	
IMEI	Ja	Alleen bij diensten waarbij

Verkeersgegeven	Bewaard?	Opmerking
		het toestel gebruikt wordt (niet bij doorgeschakelde gesprekken)
Datum / tijd	Ja	
Locatie	Ja	Alleen bij diensten waarbij het toestel gebruikt wordt; bovendien vaak niet bij gebruik in het buitenland
Type dienst	Ja	
Status	Ja	Niet bij alle aanbieders in de security applicatie, wel in billing systeem
GSM (circuitgeschakeld) specifiek		
Identiteit bestemming (B-nummer)	Ja	
IMSI (gebelde)	Ja	Alleen indien gebelde hetzelfde netwerk gebruikt
IMEI (gebelde)	Ja	Alleen indien gebelde hetzelfde netwerk gebruikt en het gesprek op het mobiele toestel opneemt
Locatie (gebelde)	Ja	Alleen indien gebelde hetzelfde netwerk gebruikt en het gesprek op het mobiele toestel opneemt
Duur	Ja	
GPRS specifiek		
APN	Ja	
PDP identiteit (IP adres)	Nee	Afhankelijk van de gebruikte dienst kan dit via de ISP beschikbaar zijn
Volume data	Ja	Niet in de security applicatie beschikbaar, wel in billing systeem
SMS specifiek		
MSISDN (ontvanger)	Ja	Alleen als de eigen SMSC gebruikt wordt (bij één operator worden andere SMSC's geblokkeerd)
IMSI (ontvanger)	Ja	Alleen indien ontvanger hetzelfde netwerk gebruikt
IMEI (ontvanger)	Ja	Alleen indien ontvanger hetzelfde netwerk gebruikt
SMSC	Ja	
Datum / tijd aflevering	Ja	Alleen als de eigen SMSC gebruikt wordt
Volume (aantal tekens)	Nee	
Locatie (ontvanger)	Ja	Alleen indien ontvanger hetzelfde netwerk gebruikt

Voor welke types gesprekken worden bovenstaande gegevens gelogd:

Type	Bewaard?	Opmerking
Beantwoord, uitgaand gesprek	Ja	
Onbeantwoord, uitgaand gesprek	Nee	
Beantwoord, inkomend gesprek	Ja	Eén aanbieder registreert deze niet
Onbeantwoord, inkomend gesprek	Nee	

Internet toegangsdiensten

Tabel 24: Verkeersgegevens bij toegangsdiensten: inbellen

Verkeersgegeven	Bewaard?	Opmerking
• Identiteit aansluiting (CLI)	Ja	Indien niet door gebruiker geblokkeerd
• Identiteit gebruiker	Ja	
• Identiteit transportlaag (IP adres)	Ja	
• Begin en eind aansluitsessie	Ja	
• Begin en eind dienstsessie	Nee	
• Target/Source host	Nee	Alleen bij IP accounting (één aanbieder
• Type dienst	Nee	
• Routing transportlaag	Nee	Alleen bij IP accounting (één aanbieder)
• Routing dienst	Nee	
• Volume	Ja	

Tabel 25: Verkeersgegevens bij toegangsdiensten: ADSL

Verkeersgegeven	Bewaard?	Opmerking
• Identiteit gebruiker	Ja	Bij vier van de zes aanbieders; zo niet dan wel een MAC adres
• Identiteit aansluiting	Nee	
• Identiteit transportlaag (IP adres)	Ja	Afhankelijk van ISP
• Begin en eind aansluitsessie	Ja, geeft veelal weinig informatie gezien lange aansluitsessies	
• Begin en eind dienstsessie	Nee	
• Target host	Nee	
• Source host	Nee	
• Type dienst	Nee	
• Routing transportlaag	Nee	
• Routing dienst	Nee	
• Volume	Ja	

Tabel 26: Verkeersgegevens bij toegangsdiensten: kabel

Verkeersgegeven	Bewaard?	Opmerking
• Identiteit aansluiting	Ja	MAC adres (is te vervalsen)
• Identiteit transportlaag	Ja	
• Begin en eind aansluitsessie	Ja	
• Begin en eind dienstsessie	Nee	
• Target host	Nee	
• Source host	Nee	
• Type dienst	Nee	
• Routing transportlaag	Nee	
• Routing dienst	Nee	
• Volume	Ja	

Tabel 27: verkeersgegevens bij toegangsdiensten: huurlijn

Verkeersgegeven	Bewaard?	Opmerking
• Identiteit aansluiting	n.v.t.	Vaste aansluiting
• Identiteit transportlaag	n.v.t.	Vast IP adres
• Begin en eind aansluitsessie	n.v.t.	Altijd aangesloten
• Begin en eind dienstsessie	Nee	Deels te herleiden uit IP accounting (één aanbieder)
• Target host	Eén van zeven aanbieders (IP accounting)	
• Source host	Eén van zeven aanbieders (IP accounting)	
• Type dienst	Nee	Deels te herleiden uit IP accounting (één aanbieder)
• Routing transportlaag	Eén van zeven aanbieders (IP accounting)	
• Routing dienst	Nee	
• Volume	Drie van zeven aanbieders	

E-mail

Tabel 28: Verkeersgegevens bij e-mail

Verkeersgegeven	Bewaard?	Opmerking
• E-mail adres zender	Vijf van zes aanbieders	
• IP adres zender	Drie van zes aanbieders	
• Datum / tijd verzending, doorgifte, etc	Vijf van zes aanbieders	
• Message-id	Drie van zes aanbieders	
• Onderwerp	Nee	Door aanbieders als

Verkeersgegeven	Bewaard?	Opmerking
		inhoud beschouwd
• Status	Ja	Alleen status doorgifte, niet eindresultaat
• Grootte (bytes)	Drie van zes aanbieders	
• Naam en IP adres van eventuele SMTP Relays	Nee	
• Mailbox server ontvanger	Nee	Is wel te herleiden uit e-mail adres ontvanger
• E-mail adres ontvanger(s)	Vijf van zes aanbieders	
• Datum / tijd opvragen e-mail	Ja	Eén aanbieder bewaart alleen datum/tijd laatste sessie

Internetcafés

Tabel 29: Verkeersgegevens bij diensten van internetcafés

Verkeersgegeven	Bewaard?	Opmerking
Identiteit gebruiker	Nee	Gebruik is anoniem
Datum / tijd /duur gebruik werkplek	Ja	Bij één van de twee aanbieders alleen op papier
Betalingsgegevens	Nee	Nee
Identiteit transportlaag (IP adres)	Eén van twee aanbieders	
Begin en eind aansluitsessie	N.v.t.	Internetcafés hebben permanent verbinding
Begin en eind dienstsessie	Nee	Deels te herleiden uit gegevens gebruik werkplek
Target host	Nee	
Source host	Nee	
Type dienst	Nee	
Routing transportlaag	Nee	
Routing dienst	Nee	
Volume	Eén van twee aanbieders	

Bijlage E: Voorbeelden van diverse logfiles

De volgende voorbeelden geven een beeld van de logs van veelgebruikte systemen. Het betreft nadrukkelijk slechts voorbeelden van de gegevens die de systemen kunnen genereren; in de praktijk komen vele variaties voor.

CDR[65] log vaste telefonie

Dit is een (enigszins gesimplificeerd) voorbeeld van een normaal, beantwoord telefoongesprek zoals dat in een moderne telefooncentrale geregistreerd wordt. In dit voorbeeld zijn de volgende (fictieve) identifiers gebruikt:

- **0123 444444** is het telefoonnummer van de beller
- **0123 555555** is het telefoonnummer dat gebeld werd

```
Rectype: 1
Host: Nx-C
Date: 20021202
Time: 100323
A-nr-plan: 1
A-nr-type: 3
A-nr: 123444444
Dialstring: 0123555555
B-nr-plan: 1
B-nr-type: 2
B-nr: 0123555555
Duration: 321
In-route: 0
Out-route: 4545
Cause-for-release: 0
Status-info: 0
```

Dit Call Detail Record kan men als volgt interpreteren: het betreft een CDR voor een normaal gesprek, geregistreerd door de centrale Nx-C, beantwoord op 2-12-2002 om 10:03:23. Het nummer van de beller volgens het gewone nummerplan is op nationaal niveau 0123444444, en dat van de gebelde 0123555555. Het gesprek duurde 321 seconden; het kwam binnen op een abonneelijn en werd doorgegeven over de route 4545.

CDR log mobiele telefonie

Dit is een (enigszins gesimplificeerd) voorbeeld van een normaal, beantwoord mobiel telefoongesprek zoals dat in de telefooncentrale geregistreerd wordt. In dit voorbeeld zijn de volgende (fictieve) identifiers gebruikt:

- **06 1122333** is het telefoonnummer van de beller
- **204151122334455** is de IMSI van de beller
- **35060620202020** is de IMEI van het toestel waarvandaan gebeld werd
- **06 1122444** is het telefoonnummer dat gebeld werd

```
Record Type: 0
Served IMSI: 204151122334455
Served IMEI: 35060620202020
Served MSISDN: 3161122333
Called Number: 3161122444
```

[65] CDR: Call Detail Record, gebruikelijke aanduiding voor een set verkeersgegevens vanuit een telefooncentrale. Een CDR beschrijft één gesprek of een deel ervan.

```
Recording Entity: 316123456789
Outgoing TKGP: 3021
Location: 1F1F2A2A
Change of Location: 1F1F2A2C; 021130094120+0100
Basic service: 11
MS Classmark: 3F2C
Event time stamp seizure: 021130094103+0100
Event time stamp answer: 021130094142+0100
Event time stamp release: 021130094430+0100
Call duration: 168
Radio Chan. Requested: 1
Radio Chan. Used: 1
Cause for termination: 0
```

Het record kan als volgt geïnterpreteerd worden: de gebruiker met IMSI 204151122334455 en telefoonnummer 06-1122333 belde op 30 november 2002 om 9:41:03, met behulp van een toestel met IMEI 35060620202020, naar het nummer 06-1122444. Het gesprek werd om 9:41:42 beantwoord en om 9:44:30 beëindigd. Aan het begin van het gesprek was de beller in het bereik van mast en antennesector 1F1F2A2A, en vanaf 9:41:20 van dezelfde mast maar een andere sector (1F1F2A2C). Het record geeft verder informatie over de centrale die het gesprek registreerde (recording entity), de interne route waarover het gesprek doorgeschakeld werd (outgoing TKGP), en het type dienst (Basic service: Teleservice 11 oftewel normale spraaktelefonie). Om nadere gegevens over de locatie en toestel van de gebelde te krijgen (mits deze hetzelfde netwerk gebruikte), kan de aanbieder op zoek gaan naar een ander record waarin het ontvangen gesprek werd geregistreerd. Overigens worden in sommige systemen deze records reeds in de *mediation* samengevoegd, waardoor de informatie direct beschikbaar is.

Internet Toegang

RADIUS log

Voorbeelden van logregels van een RADIUS server. RADIUS wordt gebruikt voor internet toegang via telefoon en ISDN, en voor sommige kabelnetten.

In dit voorbeeld zijn de volgende (fictieve) identifiers gebruikt:

- **`jan.jansen`** is het user-ID van de gebruiker
- **`0201234567`** is de nummeridentificatie (het telefoonnummer van de gebruiker)
- **`192.10.11.12`** is het tijdelijk toegekende IP adres.

```
Mon Mar 4 10:51:12 2002
       Acct-Session-Id = "2400020E"
       User-Name = "jan.jansen"
       NAS-IP-Address = 192.16.1.21
       NAS-Port = 12
       NAS-Port-Type = ISDN
       Acct-Status-Type = Start
       Acct-Authentic = RADIUS
       Called-Station-Id = "0676012345"
       Calling-Station-Id = "0201234567"
       Service-Type = Framed-User
       Framed-Protocol = PPP
       Framed-Address = 192.10.11.12
...
Mon Mar 4 12:50:49 2002
       Acct-Session-Id = "2400020E"
       User-Name = "jan.jansen"
```

```
NAS-IP-Address = 192.16.1.21
NAS-Port = 12
NAS-Port-Type = ISDN
Acct-Status-Type = Stop
Acct-Session-Time = 7177
Acct-Authentic = RADIUS
Acct-Input-Octets = 14994
Acct-Output-Octets = 90862
Called-Station-Id = "0676012345"
Calling-Station-Id = "0201234567"
Service-Type = Framed-User
Framed-Protocol = PPP
Framed-Address = 192.10.11.12
```

Deze regels betekenen het volgende: op 4 maart 2002, om 10:51 a.m., opende een gebruiker met de user-ID jan.jansen een toegangssessie door vanaf een ISDN lijn met het nummer 020-1234567 in te bellen op 06760-12345. Hij kreeg voor de duur van de sessie het IP adres 192.10.11.12 toegewezen. De verbinding werd op dezelfde dag om 12:50 beëindigd; tot die tijd had de gebruiker 14994 bytes verstuurd en 90862 bytes ontvangen.

DHCP log

Dit is een voorbeeld van een normale toegangssessie vanuit kabel of ADSL, die in dit geval vijf dagen open blijft staan. In dit voorbeeld zijn de volgende (fictieve) identifiers gebruikt:

- **`00:b1:b2:b3:b4:b5`** is het MAC adres van het modem
- **`192.10.11.12`** is het tijdelijk toegekende IP adres.

```
May  3 02:34:26 dh2 dhcpd: DHCPDISCOVER from 00:b1:b2:b3:b4:b5 via fxp0
May  3 02:34:26 dh2 dhcpd: DHCPOFFER on 192.10.11.12 to 00:b1:b2:b3:b4:b5 via
fxp0
May  3 02:34:34 dh2 dhcpd: DHCPREQUEST for 192.10.11.12 from
00:b1:b2:b3:b4:b5 via fxp0
May  3 02:34:34 dh2 dhcpd: DHCPACK on 192.10.11.12 to 00:b1:b2:b3:b4:b5 via
fxp0
May  8 03:04:50 dh2 dhcpd: DHCPRELEASE of 192.10.11.12 from 00:b1:b2:b3:b4:b5
via fxp0
```

Bovenstaande regels staan niet bij elkaar in de log, aangezien alle sessies door elkaar heen loggegevens produceren.

De gegevens hierboven kan men als volgt interpreteren: op 3 mei 2002, om 2:34 a.m., opende een computer een toegangssessie via het modem met het MAC adres 00:b1:b2:b3:b4:b5 op het netwerksegment fxp0, en kreeg voor de duur van de sessie het IP adres 192.10.11.12 toegewezen door server dh2. Op 8 mei om 3:04 a.m. werd de sessie beëindigd.

E-mail

POP3 log

Voorbeelden van logregels voor een POP3 server, voor een sessie waarbij één bericht wordt opgehaald.

In dit voorbeeld zijn de volgende (fictieve) identifiers gebruikt:

- **`jjansen@ispa.nl`** is het e-mail adres van de gebruiker
- **`192.10.11.12`** is het tijdelijk of permanent toegekende IP adres.

```
Mon Mar 11 12:50:49 2002 p_serv spop3d[12345]: connect from 192.10.11.12
Mon Mar 11 12:50:49 2002 p_serv spop3d[12345]: user jjansen authenticated -
192.10.11.12
Mon Mar 11 12:51:50 2002 p_serv spop3d[12345]: Stats: jjansen 20468 0 1 0
Mon Mar 11 12:51:56 2002 p_serv spop3d[12345]: session ended for user jjansen
- 192.10.11.12
```

In dit geval heeft de gebruiker met het e-mail adres jjansen@ispa.nl op 11 maart 2002 om 12:50 vanaf het IP adres 192.10.11.12 zijn postbus uitgelezen. Hij haalde één bericht op met een grootte van 20468 bytes; na de sessie waren er geen berichten meer in de postbus.

SMTP log

Voorbeelden van logregels van een SMTP server voor het doorgeven van één e-mail bericht. In dit voorbeeld zijn de volgende (fictieve) identifiers gebruikt:

- `jjansen@ispa.nl` is het e-mail adres van de ontvanger
- `bjansen@ispb.nl` is het e-mail adres van de zender
- **smtp.ispb.nl** is de naam van het zendende systeem (in dit geval de SMTP server van ISP B)
- `192.20.10.10` is het permanente IP adres van het zendende systeem

De gegevens worden als volgt bij ISP A (de provider van de ontvanger) gelogd.

```
Mon Mar 18 14:28:32 2002 s_serv postfix/smtpd[12345]: connect from
smtp.ispb.nl[192.20.10.10]
Mon Mar 18 14:28:32 2002 s_serv postfix/qmgr[12345]: id:
from=<bjansen@ispb.nl>, size=20468, nrcpt=1 (queue active)
Mon Mar 18 14:28:34 2002 s_serv postfix/smtp[12345]: id:
to=<jjansen@ispa.nl>, relay=local, delay=4, status=sent
Mon Mar 18 14:28:36 2002 s_serv postfix/cleanup[12345]: id: message-
id=<7a8b7d8e7b88eg@ispb.nl>
Mon Mar 18 14:28:52 2002 s_serv postfix/smtpd[12345]: disconnect from
smtp.ispa.nl[192.20.10.10]
```

In dit geval stuurde een server die zichzelf smtp.ispb.nl noemt, met IP adres 192.20.10.10, op 18 maart 2002 om 14:28 een bericht. De server meldde dat de afzender van het bericht bjansen@ispb.nl is. Het bericht was gericht aan jjansen@isp.nl en was 20468 bytes groot. ISP B heeft aan het bericht de message-id 7a8b7d8e7b88eg@ispb.nl toegekend.

De SMTP logregels staan niet bij elkaar in de log, aangezien de server een aantal activiteiten parallel uit kan voeren waarvan de logregels door elkaar in dezelfde log terecht komen.

Stratix

Bijlage F: Begeleidingscommissie

Het onderzoek is begeleid door een begeleidingscommissie, bestaande uit de volgende personen:

Prof. E.F. Michiels (voorzitter)	Universiteit Twente (Faculteit Informatica)
M. Jongeneel-van Amerongen	Ministerie van Justitie (DGWRR)
W.M. de Jongste	Ministerie van Justitie (WODC)
A.H.C. van Oosterhout	Ministerie van Justitie (DGRH)
K.M. Jaspers	Ministerie van Justitie (Bureau PIDS)
S.B. Bootsma	Ministerie van Justitie (Bureau PIDS)
T.W. Stein	Ministerie van Justitie
R. Verbeek	Ministerie van Economische Zaken (DGTP)
R.J.I. Dielemans	Ministerie van Economische Zaken (DGTP)
R. van der Berg	Ministerie van Economische Zaken (DGTP)
S.C. Klaver	Korps Landelijke Politie Diensten
G. Vleugel	Korps Landelijke Politie Diensten

Stratix

Bijlage G: Literatuurlijst

[1] "Terroristische aanslagen in de Verenigde Staten", Kamerstukken II 27 925, Nr. 10

[2] "Inzake opsporing", Rapport van de Enquêtecommissie Opsporingsmethoden (commissie van Traa), 1996;

[3] "Opsporing Locaties Verzocht", Research voor Beleid, Leiden, 2001;

[4] "Gegevensvergaring in strafvordering", Rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (commissie Mevis), Mei 2001;

[5] Wetsvoorstel "Vorderen Gegevens Telecommunicatie", Kamerstukken II 28 059, Nr. 1;

[6] "Meewerken aan strafvordering door Banken en Internet Service Providers", Eerste deel van het promotieonderzoek 'meewerken aan strafvordering door bedrijven', Rijks Universiteit Groningen, Vakgroep Strafrecht en Criminologie, 2000;

[7] "Telecommunicatiewet, Tekst & Commentaar", uitg. Kluwer, 2001

[8] "Klant in het web, Privacywaarborgen voor internettoegang", Registratiekamer, 2001