

Onderzoek verkeersgegevens: Interview vragen

Introductie

In het kader van het actieplan terrorismebestrijding heeft het ministerie van Justitie een onderzoek gestart naar het gebruik van verkeersgegevens uit de telecommunicatie in de opsporing. Het gaat hier om de behoefte aan verkeersgegevens binnen de opsporingsdiensten, en de beschikbaarheid van dergelijke gegevens bij de aanbieders van telecommunicatiediensten. De nadruk ligt bij het onderzoek op de mogelijkheden en de beperkingen die de aanbieders ondervinden bij het registreren, bewaren, en verstrekken van dergelijke gegevens. Daarbij richt het onderzoek zich zowel op de traditionele spraakdiensten als op het gebruik van het internet.

De onderzoeksresultaten zullen openbaar beschikbaar zijn, zonder vermelding van de bedrijven van wie de informatie afkomstig is. Referenties naar uw bedrijf of specifieke informatie die naar uw bedrijf verwijst zullen alleen met uw uitdrukkelijke toestemming in het eindrapport worden opgenomen.

Dit document heeft tot doel inzicht te creëren in de scope van de interviews. Alle vragen zijn gemarkeerd met een bullet.

1. Vragen: algemeen

1.1. Bedrijfsinformatie

Algemene bedrijfsinformatie wordt gebruikt om de beschikbaarheid van de verkeersgegevens te kunnen relateren aan het type bedrijf.

- Hoe kan de grootte van het bedrijf (qua aantallen klanten), getypeerd worden?
- Aan welk type klanten worden de diensten geleverd (MKB, particulieren, etc...)?
- Welke andere partijen of partners bestaan er in de keten van uw diensten?
- Welke voorvallen heeft het bedrijf meegemaakt op het gebied van digitaal rechercheren?
- Hoe groot (kostbaar) is de security operatie van het bedrijf als percentage van de operationele kosten?

1.2. Geïnterviewde(n)

- Wat is uw functie binnen bedrijf?

2. Toegangsdiensten

2.1. Algemeen

Scope van het onderzoek met betrekking tot toegangsdiensten:

Alle openbare diensten voor internet toegang: dial-up, trunk, ADSL, Cable Modem, Public Access WLAN, GPRS, etc. De nadruk ligt hier op de toegang, niet op de diensten die er overheen lopen zoals websurfen of e-mail.

- Welk type internet toegangsdienst(en) levert het bedrijf en welke staan op de roadmap? (Dial up, Trunk, ADSL, GPRS,...)
- Welke betalingsstructuur kennen deze diensten (gratis, flat-rate onbeperkt, flat-rate met een maximum, per kb or per uur)?

2.2. Architectuur

- Hoe ziet de architectuur er uit, waarover de diensten worden aangeboden? (Modembank, Radius vs DHCP, Routers, ...?)
- Zijn al deze elementen in eigen beheer?

2.3. Beschikbare gegevens per toegangsdienst

- Welke gegevens zijn beschikbaar (voor zover nog niet genoemd)?

Voorbeelden

- | | |
|--------------|---|
| - Gebruiker: | NAW gegevens, identiteit aansluiting (A-nummer, IMSI, MAC adres, etc...) |
| - Sessie: | identiteit transportdienst, begin- en eindtijd toegangsdienst, type dienst, volume |
| - Host: | source & target (IP adres, hostname) |
| - Routing: | transportdienst, applicaties (hosts in keten, re-mailers, mirror servers, VoIP gateway, etc...) |

- Op welke elementen uit de architectuur worden ze gelogd?
- Waarom worden deze gegevens gelogd (incentive, verplichting)?

2.4. Beperkingen aan beschikbaarheid

- Welke beperkingen bestaan er voor het beschikbaar maken van de verkeersgegevens (voor zover nog niet genoemd)?

Voorbeelden

- | | |
|-----------------|--|
| - Gebruiker: | Alleen de aansluiting bekend, niet de persoon; gegevens eenvoudig te vervalsen |
| - Sessie: | CLI niet bekend als de koppeling tussen access provider en ISP over ISDN loopt; GPRS biedt anonymous PDP access; Begin en eind sessie heeft geen betekenis; gebruik poortnummer inconsistent |
| - Host | IP adres niet eenduidig door gebruik proxy; IP adres niet traceerbaar wegens Network Address Translation |
| - Operationeel: | gebrek aan personeel, machinecapaciteit, of deskundigheid |
| - Log: | Niet bewaard, niet lang genoeg bewaard; log niet (goed) te doorzoeken; Nieuwe techniek/standaard niet geïmplementeerd |

- Op welk type medium wordt de log bewaard?
- Welk deel van de organisatie is verantwoordelijk voor het achterhalen van verkeersgegevens?
- Welke controles zijn er om de gegevens te verifiëren (m.n. NAW gegevens)

2.5. (Nog) niet beschikbare gegevens

- Welke gegevens zijn theoretisch mogelijk boven te halen?
- Waarom zijn deze gegevens nú nog niet beschikbaar?
- Wat is er voor nodig om ze beschikbaar te maken? (investeringskosten, organisatie, termijn)
- Welke gegevens zullen nooit beschikbaar komen? Waarom niet?

2.6. Ervaring met opsporing

- Welke gegevens zijn eerder opgevraagd?
- Hoe vaak worden dergelijke gegevens opgevraagd?

3. E-mail

3.1. Algemeen

Scope van het onderzoek met betrekking tot emaildiensten:

E-mail server (MTA) van ISP (POP3, Webmail, IMAP, SMTP); MTA van private partijen (bijvoorbeeld binnen een bedrijf); e-mail store and forward tussen "eigen" server gebruiker en andere servers (SMTP)

3.2. Architectuur

- Hoe ziet de architectuur er uit, waarover de diensten worden aangeboden?

3.3. Beschikbare gegevens

- Welke gegevens zijn beschikbaar?
- Op welke elementen uit de architectuur worden ze gelogd?

- Zijn de volgende gegevens beschikbaar (voor zover nog niet genoemd)

Voorbeelden	
- Gebruiker:	NAW: Identiteit zender / ontvanger, e-mail adressen (SMTP dan wel To, CC, BCC), IP adres
- Bericht:	datum / tijd, doorgifte, message-id (RFC-822), subject, status, volume
- Host:	source, target (IP adres en naam)
- Routing:	transportdienst, applicaties, naam & IP adres van eventuele SMTP Relays

- Waarom worden deze gegevens gelogd (incentive?)

3.4. (Nog) niet beschikbare gegevens

- Welke gegevens zijn theoretisch mogelijk boven te halen?
- Waarom zijn deze gegevens nú nog niet beschikbaar?
- Wat is er voor nodig om ze beschikbaar te maken? (investeringskosten, organisatie, termijn)
- Welke gegevens zullen nooit beschikbaar komen? Waarom niet?

3.5. Beperkingen aan beschikbaarheid

- Welke beperkingen bestaan er voor het beschikbaar maken van e-mail verkeersgegevens (voor zover nog niet genoemd)?

Voorbeelden	
- Diensten leverancier	Onbekend welke partij de e-mail dienst levert (niet noodzakelijkerwijs dezelfde aanbieder als de aansluitdienst (webmail); openbare aanbieder, bedrijf of een eigen server); Meervoudige opstellingen, mailexchange en fallback (DNS) in buitenland
- Gebruiker:	NAW van de zender en ontvanger niet bekend of niet geverifieerd (vb: hotmail), spoofen (SMTP server controleert vaak niet op IP adres & domain)
- Bericht:	Inconsequent gebruik van SMTP velden en message headers (MAIL FROM vs. Reply-To: of From:, RCPT TO vs. To:, Cc:, en Bcc: header velden); datum/tijd stempels incorrect
- Routing:	Anonymous re-mailers
- Log:	Gegevens niet (lang genoeg) gelogd; Logs niet (goed) te doorzoeken (op: e-mail id / domain zender, IP adres zender, datum/tijd, e-mail id / domain ontvanger, IP adres ontvanger); SMTP-sessie logs niet (goed) te correleren aan RFC-822 sessie logs

- Hoe lang worden deze gegevens bewaard? Welk medium?
- Hoe makkelijk (in tijdsduur) is het om de gegevens boven tafel te krijgen? Welk deel van de organisatie is hiervoor verantwoordelijk?
- Welke controles zijn er ingebouwd (reverse DNS lookup, mailback attempt, andere SPAM bestrijding)?

3.6. Ervaring met opsporing

- Welke gegevens zijn eerder opgevraagd?
- Hoe vaak worden dergelijke gegevens opgevraagd?