dialogic
innovatie • interactie

Mogelijkheden voor identificatie op internet op basis van IP-adres

Samenvatting

Projectnummer:
2018.115

Publicatienummer
2018.115-1907-MS v1.0.1

Datum:
Utrecht, 18 oktober 2019

Auteurs:
Ir. Tommy van der Vorst
Jessica Steur MSc
Ir. Nick Jelicic
Ir. Jan van Rees

Managementsamenvatting

Onderzoeksvraag

In het kader van de voorgenomen wetgeving omtrent de introductie van een beperkte bewaarplicht van telecommunicatiegegevens voor opsporing en vervolging is onderzocht hoe identificatie van individuele gebruikers op basis van een publiek IP-adres technisch te realiseren is. De vraagstelling van het onderzoek luidde:

> *Hoe kunnen (mobiele) internetaanbieders, tot twaalf maanden na het gebruik, een individuele gebruiker van een publiek IP-adres identificeren, ten behoeve van opsporing en vervolging, en wat zijn relevante (maatschappelijke) afwegingen daarbij?*

Wanneer het gaat om relevante maatschappelijke afwegingen onderscheiden we (1) bruikbaarheid voor opsporing en vervolging, (2) privacy van burgers, en (3) kosten voor de internetaanbieders. Voor het beantwoorden van de onderzoeksvraag zijn literatuuronderzoek en interviews (met mobiele internetaanbieders, politie, andere stakeholders/experts) ingezet. Op basis van de bevindingen zijn beleidsopties geformuleerd.

Achtergrond

Wanneer er een strafbaar feit plaatsvindt, maar dit niet op heterdaad wordt geconstateerd, moet de dader op basis van achtergelaten sporen worden gevonden, om uiteindelijk tot vervolging over te kunnen gaan. Om bijvoorbeeld de dader van een snelheidsovertreding te vinden, kunnen kentekens worden geregistreerd. Voor online criminaliteit geldt eenzelfde principe. Wanneer communicatie plaatsvindt op het internet is bij de ontvanger typisch het *IP-adres* van de afzender bekend – dit is immers nodig voor de communicatie in de tegengestelde richting. Dit IP-adres geeft daarmee een directe aanwijzing richting de aansluiting en/of het systeem vanaf waar een bepaalde strafbare handeling werd verricht. Het IP-adres wordt uitgegeven door een (mobiele) internetaanbieder. IP-adressen worden toegekend door internetaanbieders (ISP's). Opsporingsdiensten kunnen internetaanbieders verzoeken bekend te maken aan welke abonnee een bepaald IP-adres is uitgegeven.

Als gevolg van ontwikkelingen op het internet is de koppeling tussen individu en IP-adres niet meer zo evident als voorheen. Door de schaarste van IPv4-adressen (vierde versie van het internetprotocol), moeten de adressen worden gedeeld tussen abonnees. Dit kan door *dynamisch toewijzen*; abonnees delen hetzelfde IP-adres, maar nooit tegelijkertijd. Op basis van datum, tijd en publiek IP-adres is een individuele abonnee in dat geval nog steeds identificeerbaar. Deze situatie is vergelijkbaar met wanneer een bestuurder van een huurauto wordt gezocht op basis van kenteken: het kenteken behoort weliswaar tot het verhuurbedrijf, maar deze kan, op basis van de eigen administratie, de huurder achterhalen.

In situaties waarbij het aantal beschikbare IPv4-adressen *veel* kleiner is dan het aantal apparaten dat gelijktijdig online is, is het nodig IPv4-adressen *gelijktijdig* te delen tussen gebruikers. Dit is mogelijk door toepassing van *carrier grade network address translation* (CG-NAT). In de analogie met huurauto's betekent CG-NAT dat *verschillende* huurders landelijk in verschillende huurauto's rondrijden, maar allemaal met *hetzelfde* kenteken. Zodra de politie de bestuurder wil identificeren is, behalve datum en tijd, ofwel meer informatie over de auto nodig (bijvoorbeeld: de kleur en het type van de auto) ofwel over de route (wáár is de auto gesignaleerd, of wat was de bestemming?).

CG-NAT wordt op dit moment met name toegepast op mobiele netwerken. Afhankelijk van de operator wordt een publiek IP-adres gelijktijdig gedeeld met een handvol tot duizenden

andere abonnees. Aan alleen een IP-adres heeft de politie in geval van CG-NAT dan ook te weinig informatie om de voor opsporing relevante persoon te identificeren. Aanvullende informatie is daarom nodig om deze groep personen te verkleinen.

Bevindingen

Huidige stand van zaken

- Identificatie van abonneehouders op basis van IP-adres en datum/tijd is op Nederlandse vaste netwerken over het algemeen goed mogelijk.

- De mogelijkheden voor identificatie op basis van IP-adres verschillen sterk tussen de mobiele operators. Alleen in specifieke gevallen (afhankelijk van beschikbaarheid poortinformatie en de operator) kan tot één abonnee worden geïdentificeerd. In andere gevallen is de groepsgrootte tussen de 84 en 84.000 abonnees groot. Dit leidt tot problemen voor opsporingsinstanties.

Mogelijkheden tot verbetering

Om identificatie te verbeteren, zien we verschillende oplossingen. Deze verschillen netto nauwelijks in kosten voor de operators, maar wel sterk als het gaat om de bruikbaarheid voor opsporing en de mate van (mogelijke) privacyschending/juridische proportionaliteit van het bijhouden van informatie.

De meest voor de hand liggende oplossing om 1:1-identificatie te realiseren is uitrol van IPv6. De sector is het erover eens dat (om meer redenen dan identificatie alleen) uiteindelijk zal moeten worden gemigreerd naar IPv6. Er bestaat op dit moment echter nauwelijks een prikkel bij de Nederlandse mobiele internetproviders om dit te doen. Een enkele ISP heeft recent aangekondigd IPv6 te zullen uitrollen op haar netwerk. Mogelijk kan sterkere druk vanuit de overheid (als 'klant' van telecommunicatiediensten) een laatste zet in de juiste richting geven. Hoewel IPv6-adoptie enige tijd zal duren, en het IPv4-verkeer waarschijnlijk nooit volledig zal vervangen, leidt adoptie wel tot een lagere druk op CG-NAT, en daarmee ook tot verbeterde identificatiemogelijkheden op basis van een IPv4-adres.

Ook *zonder* IPv6 zou binnen enkele jaren identificatie tot een kleinere groepsgrootte realiseerbaar moeten zijn. We zien het toevoegen van IPv4-adressen als de meest eenvoudige oplossing. De ISP's lijken over afdoende IPv4-adressen te beschikken die zij zouden kunnen (her)inzetten op hun mobiele netwerk (naar schatting zo'n 4,2 miljoen in totaal). Wanneer voor alle abonnees CG-NAT wordt toegepast, leidt dit tot een groepsgrootte van circa vijf abonnees. Wanneer een ISP de eigen IPv4-adressen niet anders kan of wil inzetten, zou deze IPv4-adressen kunnen inkopen. Hierbij spelen (eenmalige) kosten en de vraag of deze IPv4-adressen in de gevraagde hoeveelheid beschikbaar zijn.

Een alternatieve oplossing is om de toewijzing van *source ports* aan abonnees te loggen. Hiermee is 1:1 identificatie mogelijk wanneer poortinformatie beschikbaar is bij opsporing. Dit is echter in een minderheid van de zaken het geval. Voor de overige zaken verbetert source port logging de situatie niet.

Een tweede alternatieve oplossing is om terug te keren naar een vorm van logging van verkeersgegevens, waarbij de gegevens worden gemaskeerd. Er is dan niet meer exact te achterhalen met wie een verbinding werd opgezet, maar het is wel mogelijk een (kleinere) groep abonnees te identificeren gegeven een bepaald IP-adres. Of deze oplossingsrichting voldoende verbetering biedt gegeven de te maken kosten, is echter twijfelachtig. De privacy-inbreuk wordt (vanwege de kleinere groepsgrootte bij identificatie) enerzijds verlaagd, maar (afhankelijk van de invulling van het maskeren) verhoogd.

De volgende tabel toont een vergelijking van de verschillende mogelijkheden.

Mogelijkheid	Bruikbaarheid voor opsporing en vervolging	Hoeveelheid te bewaren persoonsgegevens	Mate van privacy-inbreuk bij opsporing (groepsgrootte)	Kosten voor de aanbieder
1. Het uitrollen en adopteren van IPv6	Hoog. Minder inspanning nodig voor identificatie. Mogelijk kunnen meer zaken worden opgepakt. Het zal echter even duren voordat ook alle diensten gebruik maken van IPv6. Tot die tijd zullen veel sporen IPv4 zijn en is er geen verbetering.	Minimaal. Informatie over (semi)statische toewijzing IPv6-adresblok aan abonnee (analoog aan IPv4 op vaste netwerken) naar datum/tijd.	Minimaal. Een IPv6-adres is altijd specifiek voor één abonnee/aansluiting. Andere abonnees kunnen direct worden uitgesloten.	Maximaal enkele miljoenen euro. Investering in IPv6 lijkt (ook om andere redenen dan opsporing) uiteindelijk onafwendbaar. Er zijn verschillen tussen operators voor wat betreft reeds gedane investeringen.
2. Vergroten van het aantal publieke IPv4-adressen	Gemiddeld tot hoog, afhankelijk van de groepsgrootte (maximaal bij 1:1-toewijzing). Een IPv4-adres leidt in de meeste gevallen direct tot identificatie. Meer sporen leiden tot identificatie en meer zaken kunnen worden opgepakt.	Beperkt. Informatie over (semi)statische toewijzing IPv4-adres aan abonnee (wordt reeds als zodanig bijgehouden op vaste netwerken)	Gemiddeld. Afhankelijk van de verhouding tussen het aantal publieke IPv4-adressen en het aantal abonnees. Wanneer er één adres per abonnee beschikbaar is, is de inbreuk minimaal. Groepsgroottes vanaf 15 zijn haalbaar.	Maximaal enkele miljoenen euro. Te besteden aan het aankopen van (schaarse) IPv4-adressen en het aanpassen van configuratie.
3. Source port logging	Beperkt, tenzij het bijhouden van informatie over bronpoorten bij dienstaanbieders toeneemt.	Beperkt. Informatie over toewijzing van publiek IPv4-adres en poortreeks aan abonnee naar datum/tijd. Aan de zijde van de dienstaanbieder moeten poortnummers worden gelogd.	Minimaal wanneer een bronpoortnummer, IP-adres, datum en tijd bekend zijn bij opsporing. In alle andere gevallen gemiddeld tot groot, afhankelijk van het aantal abonnees dat het publieke IPv4-adres deelt.	Maximaal enkele miljoenen euro. De informatie wordt nu al (kortstondig) bijgehouden om CG-NAT te laten functioneren. Investeringen zijn nodig om de data te loggen, op te slaan en toegankelijk te maken.
4. Verkeersgegevens gemaskeerd loggen	Gemiddeld tot hoog, afhankelijk van de groepsgrootte en vorm van maskering.	Hoog. Er moet per opgezette verbinding informatie worden opgeslagen. Hieruit is in beperkte mate af te leiden met wie werd gecommuniceerd.	Gemiddeld. Afhankelijk van de verhouding tussen het aantal publieke IPv4-adressen en het aantal abonnees en de wijze waarop wordt gemaskeerd.	Maximaal enkele miljoenen euro. Het betreft opslag van grote hoeveelheden data.
5. Verhogen werkhoeveelheid politie	Laag. Sommige zaken kunnen niet worden opgelost zonder identificatie via IP-adres. In andere zaken is een significante tijdsinvestering nodig om een groep terug te brengen tot één verdachte.	Minimaal. Informatie over (semi)statische toewijzing IPv4-adres aan abonnee (wordt reeds als zodanig bijgehouden op vaste netwerken). Een enkele mobiele ISP houdt daarnaast bronpoortreeksen bij.	Minimaal (bij vaste IP-adressen), gemiddeld (bij mobiele waar gebruik kan worden gemaakt van bronpoortnummers) tot hoog (wanneer geen bronpoortnummer beschikbaar is; meerderheid van de gevallen).	Geen, anders dan de huidige kosten voor het bijhouden, opslaan en beschikbaar maken van de data.

Internationale vergelijking

Uit de internationale vergelijking zijn op hoofdlijnen drie lessen te trekken voor de Nederlandse situatie:

1. Nederland heeft een relatief zeer groot aantal IPv4-adressen ten opzichte van het aantal inwoners, waardoor er een kleinere prikkel bestaat voor ISP's om IPv6 uit te rollen dan in andere landen.

2. Nationale factoren, zoals nationaal beleid, zijn bepalend(er) dan de strategie van internationale ISP-conglomeraten bij het al dan niet adopteren van IPv6 door ISP's.

3. IPv6 op mobiele netwerken is volwassen en kan door operators binnen een afzienbare termijn worden uitgerold.

Beleidsopties

We zien een aantal beleidsopties:

1. **Een functionele verplichting voor ISP's tot 1:1-identificatie**. Gezien de aantallen (groeiend aantal apparaten/abonnees versus beschikbare hoeveelheid IPv4-adressen) betekent deze oplossing in de praktijk uiteindelijk een uitrol van IPv6. Desondanks worden de internetaanbieders in staat gesteld een eigen strategie te hanteren op de kortere termijn. Door implementatie van logging of het toevoegen van IPv4-adressen kan een operator ingrijpende wijzigingen enkele jaren uitstellen en hoeft zij investeringen in CG-NAT niet af te schrijven.

2. **IPv6-uitrol door ISP's stimuleren of verplichten.** Gelet op het aantal apparaten dat in de toekomst op internet zal zijn aangesloten, is uiteindelijke uitrol en adoptie van IPv6 onafwendbaar. Hoewel een verplichting tot uitrol van IPv6 zou kunnen worden opgelegd, is dit niet in lijn met de algemene beleidsvisie dat ISP's zelf verantwoordelijk zijn voor hun technische keuzes, en sluit het andere technische oplossingsrichtingen wellicht uit.

3. **Een functionele verplichting voor ISP's tot 1:N-identifcatie**. Aangezien de internetaanbieders waarschijnlijk niet direct kunnen voldoen aan 1:1-identificatie (daar is hun techniek immers nog niet klaar voor), kan overwogen worden om de 1:1-eis pas na, of geleidelijk in, een aantal jaar in te laten gaan.

4. **Geen nieuw specifiek beleid voeren; 'nudging'.** Eventueel kunnen 'zachtere' instrumenten worden ingezet, zoals websites/online diensten aan te sporen source ports op te slaan, en kunnen internetaanbieders worden aangesproken op hun (morele) verantwoordelijkheid. Autonome uitrol van IPv6 door de ISP's is waarschijnlijk, maar zal erg langzaam plaatsvinden.