Aan: «Ministerie»
«minister»
«adres»
«postcode_en_plaats»

Amsterdam, 11 juli 2005

Betreft: Reactie ISP's Erasmus onderzoek -bewaarplicht

Geachte leden van het kabinet,

Op 28 juni j.l. heeft in de Eerste Kamer een debat plaatsgevonden over het ontwerp kaderbesluit over het bewaren van verkeersgegevens in de elektronische communicatiesector. In dit debat heeft Minister Donner aangegeven dat hij na een kabinetsstandpunt over het Erasmus rapport, naar het nut en de noodzaak van een bewaarplicht voor verkeersgegevens, de Kamer schriftelijk zal informeren. Ondergetekende internetproviders willen u graag hun zienswijze geven op het Erasmus onderzoek. Daarnaast blijven wij van mening dat een algemene bewaarplicht onaanvaardbaar is vanuit privacy en kostenargumenten zoals wij ook reeds vermeld hebben in de brieven, welke verzonden zijn op 8 April 2005, 20 Juni 2005 en de presentatie van IS Interned Services van 13 Mei 2005 (zie bijlagen).

Onderzoeksmethode

In onze ogen kan het onderzoek op geen enkele wijze het nut en de noodzaak van een algemene bewaarplicht onderbouwen. Niet voor telefonie, maar zeker niet voor internet. In plaats van een onmiskenbare, concreet meetbare toegevoegde waarde van specifieke historische internet verkeersgegevens als bewijslast in rechtszaken over ernstige misdrijven presenteert het rapport een wensenlijst van anonieme 'internetdeskundigen van de politie'.

De toegevoegde waarde van beschikbare verkeersgegevens

Het onderzoek stelt dat er slechts weinig afgeronde strafzaken ter beschikking zijn en dat het om die reden dan ook niet mogelijk gebleken is een antwoord te geven op de vraag of historische verkeersgegevens van direct of wellicht van indirect belang voor het bewijs in strafzaken bleken te zijn. Het rapport is gebaseerd op 65 zaken die zijn voorgeselecteerd door de behoeftestellers, er is dus geen sprake van een a-selecte representatieve steekproef. Het onderzoek toont weliswaar aan dat er zaken zijn opgelost waarin verkeersgegevens een rol hebben gespeeld, maar laat een heleboel vragen onbeantwoord: waren er alternatieven voor verkeersgegevens, hebben verkeersgegevens een essentiële rol gespeeld bij opsporing en vervolging?

Onderbouwing voor uitbreiding van de bewaarplicht

Het rapport schiet volgens aanbieders echt te kort als het gaat om de vraag of een verruiming van de bewaarplicht een positieve invloed gehad zou hebben op het verloop van het opsporingsonderzoek. Het rapport gebruikt het volgende voorbeeld om een langere bewaarplicht

te onderbouwen.

In een van de onderzochte zaken kwam de Nationale Recherche een reeds afgerond drugstransport tegen waar al uitgebreid onderzoek naar was gedaan. Indien de historische verkeersgegevens op dat moment over een periode van één jaar beschikbaar waren geweest met betrekking tot de hoofdverdachte had men dit drugstransport naar alle waarschijnlijkheid direct aan deze verdachte kunnen koppelen

Het mag duidelijk zijn dat deze enkele constatering een wel erg magere onderbouwing biedt voor een ingrijpende maatregel als uitbreiding van de bewaarplicht. De overig aangedragen zaken tonen juist aan dat bij een heleboel zaken helemaal geen behoefte is aan een bewaarplicht. Omdat de onderzoekers stellen dat op grond van deze zaken de nut en noodzaak van een bewaarplicht verkeersgegevens niet kon worden aangetoond zijn er aanvullende interviews gehouden met medewerkers van politie en justitie, die bij deze eerdergenoemde zaken waren betrokken en daardoor niet objectief kunnen zijn.

Het rapport zegt over de gehanteerde onderzoeksmethode:

"Het is zeer de vraag of op basis van het onderzoek naar dossiers waar historische verkeersgegevens ontbreken conclusies te trekken zijn ten aanzien van het effect dat het wel aanwezig zijn van de verkeersgegevens zou hebben gehad op de bewijsgaring." (p.33)

en vervolgens

"*Derhalve kan geen wetenschappelijk onderbouwd oordeel worden gegeven met betrekking tot de binnen de politie bestaande behoefte... Daarbij geldt te meer dat Internet Service Providers geen verkeersgegevens bewaren ten behoeve van facturering.*" (p.34)

<u>Verdere conclusies uit het Erasmus rapport</u>

Wat wel uit rapport blijkt is dat er bij de opsporingsambtenaren behoefte is aan duidelijkheid en eenduidigheid over de bewaarplicht zodat zij weten wat kan worden gevorderd bij de aanbieders. Het spreekt voor zich dat deze constatering geen onderbouwing van de bewaarplicht kan zijn. Een mogelijke oplossing hiervoor is om gegevens een korte tijd te bewaren.

Voorts wordt in het rapport verondersteld dat vorderingen van opsporingsambtenaren meer afgewogen en specifiek zullen zijn als er een bewaarplicht is met een termijn van één jaar. Deze aanname is op een vooronderstelling gebaseerd en blijkt niet uit enig onderzoek of feit. Deze aanname wordt zelfs meteen tegengesproken omdat er in het onderzoek wordt aangegeven dat opsporingsambtenaren graag een standaardset van gegevens wensen op te vragen. Het opvragen van een standaardset is alles behalve een afgewogen en specifieke vordering en leidt bij een langere bewaartermijn enkel tot het opvragen van meer gegevens.

Daarnaast kan het nut van een langere bewaartermijn ter discussie worden gesteld, aangezien uit het rapport blijkt dat het verzamelen van (zeer) grote hoeveelheden informatie veelal niet van belang is voor het oplossen van een concrete strafzaak. Dit komt door de beperkte menskracht met betrekking tot de verwerking en analyse van de gegevens en de politieke druk om veel zaken te behandelen wat automatisch leidt tot een beperkte tijd om een onderzoek te verrichten (p.39).

Het Erasmus rapport kan alleen concluderen dat nut en noodzaak van een bewaarplicht ten enenmale onbewezen blijft:

"*Het is dan ook niet mogelijk gebleken een antwoord te geven op de vraag of historische verkeersgegevens van direct of wellicht van indirect belang voor het bewijs in strafzaken bleken te zijn.*" (p.37)

en:

"Nadrukkelijk moet worden opgemerkt dat de vraag naar de wenselijkheid van een bewaarplicht van gegevens gedurende een bepaalde termijn in het onderzoek slechts vanuit een oogpunt van behoefte van de opsporingspraktijk is onderzocht." (p.37)

Technische impact

Verder blijkt dat er in het Erasmus rapport sprake is van een groot aantal misverstanden over technische haalbaarheid en uitvoerbaarheid. Tot nu zijn deze aspecten onderbelicht gebleven mede doordat aanbieders nauwelijks hebben kunnen overleggen met de betrokken departementen. Een sprekend voorbeeld hiervan is het feit dat

"Door de politie wordt aangegeven dat de mogelijkheden die artikel 126n/u Sv momenteel geeft wellicht in de toekomst niet meer voldoende aanknopingspunten biedt voor de opsporing. Daarbij wordt door de deskundigen aangegeven dat steeds vaker gebruik wordt gemaakt van proxy-servers die zich in het buitenland bevinden. Het is dus van belang dat er op internationaal vlak regels worden gesteld ten aanzien van verplichtingen om deze gegevens te bewaren." (p.35).

Een bewaarplicht voor internetgegevens is volstrekt zinloos als niet met dergelijke technische beperkingen rekening wordt gehouden. Een nadere uiteenzetting van de technische belemmeringen vindt u in bijlage 1.

Economische impact

De economische schade voor de economie die dit slecht doordachte voorstel heeft, als naar alle 'wensen' in het rapport gekeken wordt, is voor de gehele branche niet te overzien. Wij verwachten dat een kleine toegangs- en hostingprovider, met ongeveer 1 GBit per seconde aan dataverkeer op jaarbasis 1 Petabyte aan opslagruimte nodig heeft. Op basis van harde offertes voor 1 provider bedraagt de initiële investering circa 7.5 miljoen euro. Daarbij komen structurele maandelijkse kosten aan afschrijving van 210.000 euro per maand en operationale kosten tussen de 25.000 en 35.000 euro per maand ten behoeve van personeel en infrastructuur (operationeel beheer, technische recherche en juridische ondersteuning, ruimte, koeling en stroombenodigdheden). Voor middelgrote providers dienen deze kosten met een factor 8 en voor grote providers zelfs met een factor 15 te worden vermenigvuldigd. De kostenraming in het KPMG rapport van november 2004 voldoet dan ook niet. Die houdt slechts rekening met opslagcapaciteit en niet met opvragen, beveiliging etc. Tevens is inmiddels de hoeveelheid internetverkeer waarop KPMG haar schatting baseert met een factor drie toegenomen, zodat ook de kosten voor een bewaarplicht navenant zijn gestegen.

De branche heeft al zeer aanzienlijke investeringen moeten doen in het aftapbaar maken en

houden van haar netwerken en diensten. Uit het Erasmus rapport blijkt dat er weinig tot geen gebruik wordt gemaakt van de mogelijkheden om individuele verdachten op internet af te tappen. Terwijl het gebruik van internet sinds 2002 explosief is toegenomen, heeft dit kennelijk niet geleid tot rechtzaken waarin historische verkeersgegevens een overtuigende rol hebben gespeeld als direct bewijs. Het niet

gebruiken van de huidige bevoegdheden mag geen reden zijn tot het vrijelijk uitbreiden naar een bevoegdheid om alle internetters systematisch in de gaten te houden.

Conclusie

Wij trekken drie conclusies uit het Erasmus rapport;

1. De aanbeveling dat een bewaarplicht van 1 jaar zinvol zou kunnen zijn, wordt in het geheel niet door het onderzoek onderbouwd.
2. Minister Donner van Justitie heeft geen enkel inzicht in de consequenties van de bewaarplicht voor de Internet Service Providers en lijkt doof voor de steekhoudende argumentatie vanuit zowel de telefonie als de ISP branche.
3. Een bewaarplicht in de EU is zinloos; de opsporingsautoriteiten nemen alleen genoegen met een wereldwijde registratie van ieders communicatiegedrag.

Aanvullend stellen wij vast dat het verbijsterend is dat de economische impact volstrekt onderbelicht blijft. Er zou tenminste een impactanalyse moeten worden uitgevoerd naar de economische effecten van een bewaarplicht en die zou door Minister Brinkhorst uitgelegd moeten kunnen worden. Daarbij zou men tenminste moeten doorrekenen wat de gevolgen zijn van een economische vlucht naar het buitenland van de huidige webhosting activiteiten van Nederlandse bedrijven. Ook zou er een effectrapportage moeten zijn over de gevolgen van de door Minister Donner bepleite inzet om communicatieaanbieders op geen enkele wijze te vergoeden voor deze investeringen, en dus op een scherpe stijging van de tarieven voor consumenten en een mogelijke dramatische afname van de keuzevrijheid.

Zowel de Eerste en de Tweede Kamer als het Europees Parlement hebben zich eerder openlijk uitgesproken tegen de voorgestelde bewaarplicht, vanwege het gebrek aan onderbouwing van nut, noodzaak en kosten. Dit rapport voegt in onze ogen geen waarde toe aan dit debat. Nut, noodzaak en proportionaliteit van de bewaarplicht zijn nog steeds niet aangetoond.

Daarom vragen wij u dringend niet akkoord te gaan met enige verdere stappen in de Europese onderhandelingen over dit voorstel, voordat een nader onderzoek naar nut, noodzaak en proportionaliteit en uit een economische impact analyse blijkt dat de bewaarplicht toegevoegde waarde heeft en de economische schade beperkt is.

Met vriendelijke groet,

namens ISPO (www.ISPO.nl):

Judith van Erve
XS4ALL Internet BV
Pb. 1848 , 1000 BV Amsterdam

mede op initiatief van:
Erik Bais
IS Interned Services B.V.

Ondertekenaars ISPO:
BIT B.V. - Dhr. A. Bik
KPN-i - Dhr. R. Niamat
Luna.nl – Dhr. R. Zenger
Thus PLC (Demon) – Dhr. Chris Willis
Tiscali B.V. – Dhr. E. Bogert
Wanadoo Nederland B.V. – Dhr. B. Heinink

Bijlagen (4):

1 - Technische bijlage
2 - Brief d.d. op 8 April 2005
3 - Brief d.d. 20 Juni 2005
4 - Presentatie van IS Interned Services van 13 Mei 2005.

CC :
Eerste Kamer - Commissie voor de JBZ Raad
Tweede kamer - Commissie voor de JBZ Raad

Bijlage 1 Technische bijlage

Betrouwbaarheid gegevens

De internetproviders kunnen niet instaan voor de correctheid en volledigheid van verkeersgegevens, alsmede een correcte herleidbaarheid tot een individu. Dit is het directe gevolg van de extreem grote verkeersstromen, steeds tegen de grenzen van de technische mogelijkheden aan werken, de defacto onbetrouwbare transport en verwerkingsmechanismen die gebruikt worden en het feit dat loggegevens primair slechts voor technische diagnostiek van het machinepark en de daarmee geleverde diensten gebruikt worden.

De techniek op dit punt is en blijft zeer feilbaar. Echter, voor het bedrijfsdoel van de internetproviders volstaat de huidige situatie. Daarbij zijn verkeersgegevens zeer eenvoudig voor misinterpretatie vatbaar, zo is inmiddels i de praktijk gebleken. Dit mede door het ontbreken van voldoende breed geaccepteerde internationale standaarden op dit punt, waardoor er ettelijke honderden verschillende opslagformaten in gebruik zijn bij Nederlandse internetproviders, elk met hun eigen specifieke betekenis van de opgeslagen data elementen. Het op p. 17 aangehaalde gebruik van verkeersgegevens om verdachten tijdens een verhoor tot een bekentenis te brengen of als "kennelijk leugenachtige getuige" te betitelen in de rechtszaal, is daarom naar onze mening omgeven met zeer ernstige risico's voor een correcte en eerlijke rechtsgang.

Technische onmogelijkheden

Er wordt bijvoorbeeld aangegeven dat er zogenaamde A en B analyses gedaan moeten kunnen worden op IP-nummers. Dat betekent dat een internetprovider voor elke klant moet registreren welk IP-nummer contact legt met de computer(s) van de klant, en met welk IP-nummer de klant verbinding maakt.
Providers hebben geen enkel bedrijfsdoel om een dergelijk hyper-gedetailleerd profiel van elke klant aan te leggen en zien natuurkundig ook geen enkele mogelijkheid om dit vast te leggen, anders dan via het zetten van een complete tap op de inhoud van al het verkeer van elke klant. Uit die tap zou dan vervolgens de 'inhoud' moeten worden verwijderd. Een dergelijke tap bevat ook alle ongewenste contacten die via internet met een computer worden gelegd, zoals portscans, virussen en spam.

Daarnaast zou van elke klant geregistreerd moeten worden hoe vaak en hoe intensief hij of zij gebruikt maakt van externe internetdiensten als Skype (gratis Voice over IP software), MSN (een Microsoft chat-achtige messengerdienst) en peer-to-peer uitwisseldiensten als KaZaa. Maar dergelijke software staat tussen de ontvanger en verzender in. De provider ziet dus vrijwel nooit de directe verbinding met de daadwerkelijke ontvanger en verzender.

In het geval van Skype, software om via internet te bellen, maken veel mensen gebruik (zonder dat ze zich hiervan bewust zijn) van zogenaamde supernodes, om het verkeer aan een andere gebruiker te kunnen geven, bijvoorbeeld omdat het eigen prive of zakelijke netwerk uit beveiligingsoverwegingen geen directe externe contacten toestaat. Iedere PC op het internet met deze software kan zichzelf als supernode uitroepen. (Wederom zonder dat de gebruiker hier weet van heeft.) Als de verbinding direct gelegd kan worden, verloopt het gesprek rechtstreeks, maar als dat niet kan, dan biedt de software onmiddellijk het gebruik aan van een zogenaamde netwerk hub. Juist omdat de telefoongesprekken over een openbaar netwerk lopen, gebruikt Skype standaard een stevige versleuteling van de gesprekken, dmv 256 bit AES encryptie. Hierdoor wordt het volume van de communicatie standaard op een gelijk niveau gehouden, zodat de provider geen idee heeft van het volume van het gesprek of aantallen betrokkenen.

MSN heeft een soortgelijke constructie. Al het chatverkeer gaat via de MSN servers en niet direct tussen de ontvangers. Alleen bij het uitwisselen van bestanden en webcam beelden kunnen twee mensen een directe verbinding met elkaar leggen, maar pas nadat er een uitnodiging is verstuurd via de centrale server. Als 1 van de betrokkenen geen directe verbinding toestaat (ivm beveiliging), kan de uitwisseling van bestanden bovendien overgenomen worden door de centrale server. Mochten opsporingsdiensten dus geïnteresseerd zijn in informatie over het MSN-gebruik van een verdachte, dan zouden zij zich in eerste instantie tot deze in de VS gevestigde dienst moeten wenden.

Internet als internationaal medium

Het rapport gaat vrijwel volledig voorbij aan een andere technische ontwikkeling die een eventuele bewaarplicht in Nederland en in de EU tot een heilloze weg maakt. Internet is een globaal netwerk, met talloze nuttige internetdiensten buiten Europa, zoals anonimiserings diensten als TOR (**http://tor.eff.org/**) of het gebruik van versleutelingstechnieken en tunnelmethode's om het dataverkeer buiten de EU te brengen en zo de bewaarplicht te ontlopen. Het rapport suggereert op blz. 35 dat de EU druk moet uitoefenen op de rest van de wereld om ervoor te zorgen dat in de hele wereld van alle internetters al het communicatiegedrag wordt bijgehouden.

"Door de politie wordt aangegeven dat de mogelijkheden die artikel 126n/u Sv momenteel geeft wellicht in de toekomst niet meer voldoende aanknopingspunten biedt voor de opsporing. Daarbij wordt door de deskundigen aangegeven dat steeds vaker gebruik wordt gemaakt van proxy-servers die zich in het buitenland bevinden. Het is dus van belang dat er op internationaal vlak regels worden gesteld ten aanzien van verplichtingen om deze gegevens te bewaren."

Een bewaarplicht in de EU is derhalve zinloos; de opsporingsautoriteiten nemen alleen genoegen met een wereldwijde registratie van ieders communicatiegedrag.