Reactie van Stichting DHPA op het concept wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten: Versie juni 2015

Leidschendam, 30-8-2015

Excellentie,

De Dutch Hosting Provider Association ('DHPA') is een samenwerking van de 30 marktleidende hosting- en cloud providers in Nederland. De DHPA vertegenwoordigt een Nederlandse groep van bedrijven in een sector die in de afgelopen decennia is uitgegroeid van een startersmarkt naar één van de belangrijkste ter wereld. De Nederlandse hosting industrie is wereldwijd actief en faciliteert alleen al meer dan 20% van de gehele e-commerce omzet in Europa. Met het hanteren van kernwaarden als professionaliteit, kwaliteit en transparantie dragen de DHPA en haar deelnemers bij aan het vertrouwen in Nederlands als de ideale vestigingsplaats voor op Cloud gebaseerde IT, sites, applicaties e-commerce en daarmee voor de nieuwe digitale economie.

DHPA deelt de zorgen van de Stichting Digital Infrastructuur Nederland ('DINL') over de impact van het conceptwetsvoorstel voor de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV). Het wetsvoorstel wordt gepresenteerd als een louter technische wijziging waarbij de ruimte van de dienst om gegevens te verzamelen wordt uitgebreid, maar uit de concept wettekst blijkt dat de bevoegdheden van de veiligheidsdiensten in aanzienlijke mate worden uitgebreid.

De potentiele impact op de Nederlandse economie en meer specifiek de technologiesector is groot en DHPA vreest dat de concurrentiepositie van de Nederlandse hostingsector ernstig zal verslechteren. DHPA ziet daarom graag een grondige onderbouwing van nut en noodzaak van de specifieke wijzigingen en uitbreidingen van bevoegdheden.
Net als bij de andere wetgeving op het gebied van handhaving en opsporing in het domein van de Online industrie, komt de uitvoering ervan voor een belangrijk deel terecht bij hosting en cloud bedrijven. In de praktijk betekent het dat deze bedrijven moeten opdraaien voor de kosten van het plaatsen van taps, het moeten bewaren en ter beschikking stellen van gegevens, de interactie met politie, justitie en de veiligheidsdiensten, en meer. Het wetsvoorstel voegt hier nog weer andere en nieuwe verplichtingen en dus kosten aan toe, terwijl er geen rekening wordt gehouden met de potentieel grote impact op de bedrijfsvoering van die bedrijven.
Naar het oordeel van DHPA ontbreekt dan ook een proportionaliteitstoetsing, die wel noodzakelijk zou zijn als de kosten door de diensten zelf zouden worden gedragen. Het komt er nu op neer dat de veiligheidsdiensten van informatie worden voorzien op kosten van deze ondernemers.

Verder acht DHPA het noodzakelijk dat een degelijke analyse wordt uitgevoerd van de economische impact van de nieuwe wet, dat wil zeggen een heldere berekening van de met

de uitvoering van de wet gemoeide directe en indirecte kosten en de gevolgen daarvan voor de bedrijven die het treft. DHPA maakt zich zorgen dat de gevolgen van deze kostenstijging- zowel vanuit het oogpunt van de directe kosten voor individuele bedrijven in de hostingsector, als de concurrentiepositie van Nederland als technologie- en internethub - zeer groot zullen zijn.

Verder ziet DHPA een 5 tal specifieke, ernstige problemen met de uitvoerbaarheid van de in het voorstel genoemde bevoegdheden, voor Nederlandse Hosting en cloud bedrijven. Wij lichten deze hier toe.

1. Inbeslagname (art 27 lid 1 sub a en lid 2 en art 42)

Bij gedeelde servers, zoals virtuele servers of cloud servers, zal inbeslagname en fysiek wegnemen van servers leiden tot onderbreking van de dienstverlening aan non-targets (i.e. organisaties of personen die geen onderwerp van onderzoek zijn). Door zo'n ingreep van de diensten zullen andere sites of toepassingen, ook kritische of die met een maatschappelijk belang, gemakkelijk onbeschikbaar kunnen raken. Het behoeft geen betoog dat dit tot een onacceptabele inbreuk op economische en maatschappelijke processen kan leiden.
De proportionaliteit van in beslag nemen van servers zal daarom vooraf moeten worden getoetst en daarbij moet rekening worden gehouden met de impact op de bedrijfsvoering van het betreffende hostingbedrijf en de belangen van andere gebruikers.
De diensten zouden naar de mening van DHPA moeten worden verplicht om bij hun interne proportionaliteitstoetsing rekening te houden met de impact op non-targets van het wegnemen van een server. Dit zou een verduidelijking van art. 43 lid 3 zijn.

2. Ontsleuteling (art 32 lid 1, 33 lid 1 en 41 lid 5)

Iedereen waarvan de diensten het redelijk vermoeden heeft dat zij kunnen meewerken aan het ontsleutelen van communicatie of berichten, kan worden gedwongen daaraan mee te werken. Concreet betekent dit dat hostingbedrijven kunnen worden verplicht de private delen van SSL-certificaten van hun klanten aan de diensten te verstrekken, het betreft dan de diensten waarvoor zij het SSL-certificaat verzorgen.
Naar het oordeel van de DHPA is dit een onacceptabele inbreuk op het vertrouwen in het certificaten systeem. Wij roepen in herinnering wat er gebeurde toen Diginotar werd gecompromitteerd – het gevolg van het feit dat (vermoedelijk) een buitenlandse inlichtingendienst over sleutels kon beschikken en zelf certificaten kon maken.
Het vrijgeven van SSL sleutels betekent ook dat verkeer van non-targets zichtbaar wordt, aangezien ook dat verkeer leesbaar wordt voor de diensten.

De plicht tot het verlenen van medewerking aan ontsleutelen zou moeten worden beperkt tot de aanbieder wiens verkeer wordt versleuteld zodat niet de hosting provider hierop kan worden aangesproken (hoewel hiermee het probleem slechts wordt verplaatst). Daarnaast zou de proportionaliteit van een dergelijke opvraging door (bij voorkeur vooraf) moeten worden getoetst.

3. Hacking (art 30 lid 1 sub a en b, art 30 lid 2 sub b en c)

Allereerst tekent de DHPA aan dat de term 'Terughacken' soms onterecht wordt gebruikt. Het betreft immers niet de bevoegdheid voor het hacken van systemen van hackers, maar het mogen inbreken op willekeurige gecomputeriseerde apparaten, ook die van non-targets, om informatie te kunnen vergaren. Dat hacken kan dus ook gericht zijn op gedeelde servers, waarbij de diensten gebruik kunnen maken van kwetsbaarheden op delen van non-targets. Ook dit kan gemakkelijk leiden tot onderbreking van de dienstverlening van hosting providers aan die non-targets. Gedeelde servers kunnen daarnaast extra kwetsbaar worden indien de diensten daar ook backdoors installeren in het kader van de installatie van monitoringsoftware (bugs).

Het hacken van/via non-targets zou moeten worden uitgesloten door in artikel 30 *"of door tussenkomst van het geautomatiseerd werk van een derde"* te verwijderen. Daarnaast zou het installeren van backdoors verboden moeten zijn.

4. Gericht en ongericht aftappen van verkeer (artikel 32 resp. 33)

De bevoegdheden maken het voor de diensten mogelijk om in het netwerk van hosting bedrijven ongericht interceptiemiddelen in te zetten. Hosting bedrijven hebben in de regel honderden tot (tien)duizenden klanten en beheren een veelvoud aan servers. De DHPA vreest dat uitbreiding van de mogelijkheid tot (ongerichte) interceptie op deze infrastructuren een significante impact op de bedrijfsvoering van hosting providers zal hebben.

De proportionaliteit van - met name de ongerichte - aftapbevoegdheid dient dan ook te worden gewaarborgd, onder meer door een gedegen voorafgaande toetsing en door de reikwijdte, opslagtermijn en toegang te beperken en, vooral, niet zonder onafhankelijk toezicht. Verder zou naar de mening van DHPA de mogelijkheid moeten worden geboden om de uitkomst van een dergelijke proportionaliteitstoets – dus ook achteraf - via een formele procedure te betwisten.

5. Kosten

Hosting providers zullen flinke kosten moeten maken om mee te werken aan verzoeken van de diensten, zoals het begeleiden van opsporingsambtenaren bij inbeslagnames. Nu worden alleen de directe kosten van aftappen en vorderingen vergoed, het betreft marginale vergoedingen voor administratieve inspanning.

DHPA is van mening dat de door hosters gemaakte kosten bij alle medewerkingsplichten volledig dienen te worden vergoed. Het kan niet zo zijn dat een specifieke sector disproportioneel moet opdraaien voor de kosten van de verzamelwoede van de inlichtingendiensten.

6. Medewerkingsplicht

Daarnaast merkt DHPA op dat hosting providers vaak niet kunnen inloggen op de servers van haar klanten, simpelweg omdat zij niet altijd over de inloggegevens beschikken. Dit is bijvoorbeeld het geval als de klant hardware (fysieke servers) afneemt. Dit gegeven mag niet worden geïnterpreteerd als het niet voldoen aan de medewerkingsplicht. Zie artikel 40 lid 3, dat een onderzoeksplicht suggereert bij vorderingen inzake verkeers- en abonneegegevens.

7. Rechtstreekse Toegang (artikel 22)

De inlichtingendiensten mogen hosting providers verzoeken om op vrijwillige basis rechtstreekse geautomatiseerde toegang tot gegevens te verlenen en bestanden te verstrekken. Dat is een wat eigenaardige bevoegdheid, die strijdig is met onder andere de WBP.

DHPA deelnemers zullen nimmer de door hun klanten aan hen toevertrouwde data delen of vrijwillig beschikbaar stellen aan de overheid of aan enige andere partij, zonder dat daar een wettelijke basis voor bestaat. Dat zou neerkomen op het overtreden van de WBP.

DHPA is van mening dat verzoeken van opsporingsdiensten altijd een wettelijke basis moeten hebben, en moeten zijn onderbouwd. Verder zouden verzoeken met betrekking tot persoonsgegevens alleen gericht mogen worden tot het bedrijf dat verantwoordelijke is in de zin van de Wet Bescherming Persoonsgegevens.

De DHPA is ten allen tijde bereid over deze onderwerpen in gesprek te gaan

Leidschendam, 30-8-2015
Namens het bestuur

M. Steltman
Directeur