

# OPENBAAR

<b>Contactpersoon</b>	<b>Ons kenmerk</b>	<b>Uw kenmerk</b>	<b>Doorkiesnummer</b>
mr. H. Dries	OPTA/IPB/2007/200702		(070) 315 35 06
<b>Datum</b>	<b>Onderwerp</b>		<b>Bijlage(n)</b>
	Consultatie voorlopig standpunt OPTA over de 'zorgplicht' van internetaanbieders (art. 11.3Tw)		

Geachte heer, mevrouw,

## 1. Inleiding

Internet is niet meer weg te denken uit de moderne samenleving. OPTA, de Onafhankelijke Post en Telecommunicatie Autoriteit, heeft mede de taak internet veilig te maken en te houden. Zo is OPTA bijvoorbeeld verantwoordelijk voor de handhaving van het spam- en spywareverbod. Om de veiligheid en beveiliging op internet te waarborgen worden aanbieders van openbare elektronische diensten en netwerken verplicht in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers om passende technische en organisatorische maatregelen te treffen. OPTA heeft de taak om hierop toezicht te houden. Om invulling te geven aan deze toezichtstaak is OPTA eind vorig jaar gestart met het project 'artikel 11.3 Tw'. Het doel van dit project is tweeledig. Enerzijds wil OPTA een minimum niveau van veiligheid in de markt waarborgen. Anderzijds wil OPTA met de markt tot afspraken komen om boven dat minimum niveau best current practices te hanteren, die de internetveiligheid verder vergroten en daarmee de gehele markt ten goede zullen komen.

Uiteraard kan OPTA dit niet alleen. Een citaat uit het regeerakkoord mag dit verduidelijken:

*"Een veilige samenleving is niet alleen een kwestie van duidelijke regels en goede handhaving. Een respectvolle omgang van mensen met elkaar en fatsoen in het maatschappelijke verkeer zijn onmisbaar voor een veilig klimaat."*

Regeerakkoord 2007 (CDA, PvdA,CU) p. 33

OPTA wil mede daarom graag samen met de markt de Internetveiligheid voor de Nederlandse samenleving vergroten. Het bedrijfsleven heeft hierin een eigen verantwoordelijkheid. OPTA constateert dat de laatste tijd er ook steeds meer bedrijven blijf geven de wil om deze verantwoordelijkheid invulling te geven.

## OPENBAAR

De samenwerking die OPTA nastreeft is niet geheel vrijblijvend. Een belangrijk onderdeel van OPTA's wettelijke takenpakket is namelijk de handhaving van artikel 11.3 van de Telecommunicatiewet. OPTA is van plan deze zorgplicht nader in te vullen met de markt en ook daadwerkelijk te handhaven als nodig mocht blijken.

### 2. Artikel 11.3 Telecommunicatiewet

Artikel 11.3 van de Telecommunicatiewet (hierna: Tw) Tw schrijft twee verplichtingen voor:

1. Aanbieders van openbare elektronische communicatiediensten en netwerken treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.
2. Aanbieders hebben de zorgplicht om de abonnees te informeren over:
  - a. bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst;
  - b. de eventuele middelen waarmee de bijzondere risico's tegengegaan kunnen worden, voor zover het andere maatregelen betreft dan die welke de aanbieder op grond van het eerste lid gehouden is te treffen, alsmede een indicatie van de verwachte kosten.

Eenzijds is het artikel erg open geformuleerd. Maatregelen moeten bijvoorbeeld "passend" zijn. Anderzijds betreft dit artikel maar een beperkt aantal bedrijven: aanbieders van openbare elektronische communicatienetwerken en – diensten. OPTA kan deze bedrijven aanspreken op het nemen van adequate maatregelen. Andere bedrijven (in het oog springen bijvoorbeeld software- en hardwareleveranciers) vallen buiten deze bepaling. Dit betekent dat deze groep niet aanspreekbaar is door OPTA en dus buiten het primaire bereik van het project valt. OPTA verzoekt partijen om hiermee rekening te houden bij het geven van antwoorden.

### 3. Onderzoek

Om beter invulling te kunnen geven aan deze taak heeft OPTA in 2006 Stratix opdracht gegeven tot het doen van een onderzoek naar de bestaande en toekomstige dreigingen waar Nederlandse consumenten op internet mee worden geconfronteerd. Vervolgens heeft Stratix de maatregelen geïnterpreteerd die internet-serviceproviders tegen deze dreigingen nemen. Het resultaat van het onderzoek, het rapport getiteld "Onderzoek inzake 11.3 Tw - Concept-dreigingsbeeld" is vanaf heden te vinden op de website van OPTA.<sup>1</sup> Een korte samenvatting treft u aan als bijlage.

Naar aanleiding van het onderzoek heeft OPTA een voorlopig standpunt bepaald over de wijze waarop

---

<sup>1</sup> Het onderzoek is een weergave van de bevindingen van de onderzoeker en geeft geen opvattingen van het college van OPTA weer. Het is nadrukkelijk bestemd voor nadere discussie.

## OPENBAAR

zij haar taak wil invullen. Het onderzoek roept bij OPTA echter ook nog enkele belangrijke vragen op. Om deze vragen te beantwoorden wil OPTA u uitnodigen om deel te nemen aan de consultatie. OPTA wil u ook in de gelegenheid stellen om uw reactie te geven op haar voorlopige standpunt.

### 4. Voorlopig standpunt

#### 4.1 Inleiding

Naar aanleiding van het onderzoek constateert OPTA dat er belangrijke dreigingen zijn voor de persoonlijke levenssfeer van internetgebruikers. De voornaamste huidige dreigingen – spam en spyware - die het rapport noemt worden nu al door OPTA aangepakt.

Kort gezegd constateert OPTA dat de dreigingen zijn onder te verdelen in een aantal categorieën. De belangrijkste zijn:

- Dreigingen betreffende ongeautoriseerde toegang:
  - Tot verbindingen
  - Tot gegevens
- Dreigingen betreffende misbruik van:
  - Adressering (DNS)
  - Routing
- Dreigingen betreffende de aard of de status van bepaalde informatie (zoals spam, spyware en phishing).
- Dreigingen die samenhangen met onvoldoende informatie over de risico's van internetgebruik.

#### 4.2 Maatregelen

Uit het rapport blijkt dat er al diverse maatregelen worden genomen door aanbieders om dreigingen tegen te gaan. Hoewel het rapport geen volledige lijst van maatregelen lijkt te geven, beveelt het de volgende belangrijke infrastructurele maatregelen aan:

- Het niet naar andere netten routeren van verkeer vanaf IP-adressen die niet tot de eigen reeksen behoren.
- Het niet routeren van inkomend verkeer van IP-blokken die niet officieel zijn uitgegeven.
- Het aanbieden van virus- en spamfilters voor inkomende en eventueel uitgaande e-mail.
- Het blokkeren van de meest voor inbraken op pc's misbruikte poortnummers.
- Het adviseren van eindgebruikers om (personal) firewalls te installeren of activeren.

Met betrekking tot de te nemen maatregelen constateert OPTA dat de geïnterviewde aanbieders enkele maatregelen aandragen waarover een grote mate van unanimititeit bestaat.

Bij andere maatregelen is er enige discussie mogelijk over het effect en de voor- en nadelen van de betreffende maatregelen. In sommige gevallen betreft het inhoudelijke bezwaren tegen de maatregel. In andere gevallen wordt een maatregel om economische redenen niet haalbaar geacht.

## OPENBAAR

Gelet op deze maatregelen is OPTA voorlopig van mening dat zij maatregelen het beste kan indelen in drie categorieën:

- basismaatregelen;
- maatregelen die als best current practice kunnen gelden en
- additionele maatregelen die – om diverse redenen – te hoog gegrepen zijn om nu al marktbreed in te voeren.

### *4.3 Basismaatregelen: beleidsregel*

OPTA is van oordeel dat enkele maatregelen die het rapport noemt zodanig bijdragen aan de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van het internet en dat deze maatregelen als basis infrastructurele maatregel kunnen gelden.

OPTA is voornemens deze en vergelijkbare passende maatregelen, op te nemen in beleidsregels die inhoud moet geven aan het begrip “passende maatregelen” in artikel 11.3 lid 1 van de Tw. Het gaat ten minste om:

- Het niet naar andere netten routeren van verkeer vanaf IP-adressen die niet tot de eigen reeksen behoren (egress filter).
- Het niet routeren van inkomend verkeer van IP-blokken die niet zijn uitgegeven of in gebruik zijn (ingress filter).
- Het aanbieden van virus- en spamfilters voor inkomende en uitgaande e-mail
- Het geven van voorlichting aan gebruikers over concrete dreigingen en de bescherming tegen deze concrete dreigingen.
- Daar onder verstaat OPTA in ieder geval het wijzen van de eindgebruiker op de mogelijkheid van het installeren van:
  - Een firewall
  - Een anti-virus programma.

Met betrekking tot deze laatste maatregelen merkt OPTA op dat deze maatregelen overeenstemmen met de verplichting die op grond van het tweede lid van artikel 11.3 Tw geldt.

Tot slot merkt OPTA op dat alleen basismaatregelen die praktisch handhaafbaar zijn als “passende” maatregel worden opgenomen in beleidsregels.

### *4.4 Best practices*

Met betrekking tot andere maatregelen oordeelt OPTA dat deze weliswaar zeer nuttig en noodzakelijk kunnen zijn voor een meerderheid van gebruikers, maar dat deze niet in alle gevallen van de aanbieder geveerd kunnen worden.

Zo zijn er bijvoorbeeld categorieën van gebruikers denkbaar die deze maatregelen om diverse redenen liever zelf willen nemen. Ook kunnen maatregelen legitiem gebruik van de dienst verhinderen (denk

## OPENBAAR

bijvoorbeeld aan “false positives” bij spamfilters).

Wel zou iedere aanbieder naar het oordeel van OPTA deze maatregelen op toepasselijkheid moeten onderzoeken.

Gelet op deze criteria meent OPTA dat de volgende maatregelen die het rapport noemt als best current practise kunnen gelden:

- Het blokkeren van de meest voor inbraken op pc's of voor ander misbruik gebruikte poortnummers.
- Benaderen van eindgebruikers waarvan bekend is dat hun pc als zombie in een botnet functioneert om hieraan een eind te maken.
- Helpdeskondersteuning voor eindgebruikers – tegen redelijke kosten - om hun pc te beveiligen of “schoon” te maken.

Met betrekking tot deze en vergelijkbare maatregelen wil OPTA graag in overleg met marktpartijen bijdragen aan een brede acceptatie en implementatie.

Hoewel beleidsregels voor dergelijke maatregelen minder voor de hand lijkt te liggen vindt OPTA deze maatregelen wel zodanig belangrijk dat zij graag een best current practice wil vastleggen om de meest efficiënte en effectieve implementatie van deze maatregelen te bevorderen.

### *4.5 Additionele maatregelen die te hoog grepen zijn*

De overige maatregelen die het rapport bespreekt (zoals bijvoorbeeld de implementatie van DNSSec, quarantaine systemen voor geïnfecteerde of nieuwe hosts in het netwerk) zouden in voorkomende gevallen ook als best current practice kunnen gelden. OPTA sluit niet uit dat zij –mede gelet op de technische ontwikkeling - enkele van deze maatregelen op termijn ook als best current practice wil beschouwen.

OPTA acht deze maatregelen op dit moment echter zo specifiek dat zij de implementatie van deze maatregelen voorlopig aan de betrokken marktpartijen wenst over te laten.

### *4.6 Conclusie*

OPTA benadrukt dat dit standpunt een voorlopig karakter heeft en nodigt u graag uit om er op te reageren. Dit kan schriftelijk, door een reactie op deze brief te geven en vooral op de vragen die in het navolgende deel gecursiveerd zijn weergegeven.

Ook bestaat de mogelijkheid tot het geven van een mondelinge reactie. Daartoe zal OPTA in samenwerking met ECP.nl een ronde tafel bijeenkomst organiseren waarbij een grote hoeveelheid belangstellenden en deskundigen zal worden uitgenodigd. U ontvangt binnenkort een uitnodiging van OPTA om deel te nemen aan de ronde tafel bijeenkomst.

## OPENBAAR

### 5. Vragen van OPTA

Zoals reeds werd geconstateerd roept het rapport enkele belangrijke vragen op. OPTA verzoekt u dan ook uitdrukkelijk om deze te beantwoorden.

1. *Hoe beoordeelt u de in het rapport geschetste dreigingen: geeft het rapport alle relevante dreigingen voor Nederlandse internetgebruikers weer? Zo niet, welke dreigingen ziet u nog meer?*

Gelet op de door het rapport gesignaleerde dreigingen geeft een aantal aanbieders aan welke maatregelen genomen kunnen worden om deze dreigingen tegen te gaan. OPTA wil graag nagaan of dit beeld van de mogelijke maatregelen volledig is.

2. *OPTA wil u daarom verzoeken om aan te geven welke maatregelen u nog meer nuttig of noodzakelijk acht. U wordt verzocht daarbij eveneens aan te geven of u meent dat de maatregel dermate basaal is dat deze als "passende maatregel" moet worden gezien en waarom.*

Artikel 11.3 Tw beschermt in beginsel zowel zakelijke als particuliere abonnees. OPTA vindt het echter van belang om zich in eerste instantie vooral te richten op beveiligingsmaatregelen die de veiligheid van de consument direct ten goede komen.

3. *OPTA vraagt u daarom per maatregel (uit het rapport of door u zelf aangedragen) aan te geven in hoeverre u meent dat de betreffende maatregel een positief effect heeft cq. zal hebben op de veiligheid van de consument/gebruiker.*

De geïnterviewden geven aan dat OPTA op de hoogte moet zijn van de laatste dreigingen om te zorgen dat zij tijdig reageert. Ook is het lastig om concrete maatregelen op te leggen en te handhaven omdat snelle technologische vernieuwing een continue arms race tot gevolg heeft gehad.

OPTA is van mening dat het in ieder geval noodzakelijk is om steeds in overleg met de markt, passende maatregelen (basismaatregelen) of best current practices te benoemen waar dit kan. Gelet op haar wettelijke taak is OPTA daartoe zelfs gedeeltelijk verplicht. Daarom wil OPTA graag regelmatig in overleg treden met de aanbieders en overige belanghebbenden.

OPTA vindt het belangrijk om regelmatig de ontwikkelingen op het gebied van internetveiligheid te bespreken met een brede representatieve groep van gebruikers, aanbieders en andere belanghebbenden.

4. *OPTA vraagt u dan ook aan te geven hoe u meent dat een dergelijk overleg met aanbieders en belanghebbenden zou moeten worden ingericht. Welke bestaande fora liggen voor de hand? Hoe zou u een dergelijk overleg willen inrichten (denk aan aspecten als locatie, frequentie, agenda en*

## OPENBAAR

*de rol van het overleg)?*

Tot slot constateert OPTA een grote behoefte bij de geïnterviewde aanbieders om te reageren op de tekst en vooral de reikwijdte van artikel 11.3 Tw en de rol die daarbij wordt gedacht voor OPTA.

*5. Tot slot nodigt OPTA u graag uit om ook uw visie te geven op:*

- *het beschreven voorlopige standpunt*
- *de rol die OPTA blijkens dit standpunt wil innemen*
- *het doel en de reikwijdte van artikel 11.3 Tw*

### 6. Vervolg

OPTA verzoekt u uw schriftelijke reactie vóór 16 mei te richten aan de heer H. Dries ([h.dries@opta.nl](mailto:h.dries@opta.nl)) . Indien u vragen heeft of u wenst een individueel gesprek met OPTA dan kunt u contact opnemen met de heer H. Dries (070-315 3506) of mevrouw M.P. Man (070-315 3512). U ontvangt binnenkort een uitnodiging voor de deelname aan de ronde tafel bijeenkomst die OPTA in samenwerking met ECP.nl organiseert, waarin deze consultatie centraal staat. De reacties op deze consultatie en de te houden ronde tafel bijeenkomst worden gebruikt voor de totstandkoming van de beleidsregels.

Hoogachtend,

HET COLLEGE VAN DE ONAFHANKELIJKE POST EN TELECOMMUNICATIE AUTORITEIT,  
namens het college,  
plv. Sectorleider Integriteitstoezicht en Post

mr. D. Molenaar