OPTA
T.a.v. de heer H. Dries
Postbus 90420
2509 LK 's-Gravenhage

Public Affairs:
Tel: 020 398 7686
E-mail:nveen@xs4all.nl

XS4ALL Internet B.V.
Postbus 1848
1000 BV Amsterdam
Eekholt 42
1112 XH Diemen

KvK Amsterdam 33287534
Bank 66 35 71 847
Postbank 4683839

Datum 15 mei 2007
Onderwerp Consultatie OPTA over de 'zorgplicht' van internetaanbieders

Geachte heer Dries,

Hieronder treft u de reactie aan van XS4ALL Internet B.V. (hierna: XS4ALL) op het voorlopige standpunt van OPTA met betrekking tot de 'zorgplicht' van internet-aanbieders. Deze schriftelijke reactie bevat een algemeen deel, een voorstel voor een alternatieve aanpak en de beantwoording van de vijf vragen van OPTA uit haar brief van 17 april jl.

1 Algemene opmerkingen

XS4ALL heeft hetzelfde doel voor ogen als OPTA: een veiliger internet. XS4ALL is het ook eens met OPTA dat er maatregelen moeten worden genomen. Wij menen echter dat de voorgestelde maatregelen niet zullen bijdragen aan een veiliger internet, om de volgende redenen.

OPTA grijpt te snel naar haar wettelijke bevoegdheden. Om de veiligheid op internet te bevorderen moet in de eerste plaats onderzocht worden waar de problemen spelen en welke maatregelen nu al worden genomen. Vervolgens komt de vraag aan de orde of aanvullende maatregelen nodig zijn, en zo ja, welke. Als aanvullende maatregelen nodig zijn is tenslotte de vraag of regulering onontbeerlijk is. Vanzelfsprekend mag een kosten-batenanalyse niet ontbreken en moet het probleem in zijn internationale context worden bezien.

OPTA draait de zaken om: eerst zoekt OPTA naar een juridische kapstok om haar bevoegdheid aan op te hangen: artikel 11.3 van de Telecommunicatiewet.

Vervolgens onderzoekt OPTA welke maatregelen zij kan opleggen op grond van dat artikel. De kosten-batenanalyse ontbreekt, en ook de internationale context van het probleem wordt uit het oog verloren. XS4ALL steunt deze aanpak niet, om verschillende redenen.

De benadering van OPTA richt zich eenzijdig op ISP's en telecommunicatie-aanbieders

Het voorlopige standpunt van OPTA gaat te veel uit van het klassieke onderscheid tussen producenten en gebruikers. De gedachte bij OPTA lijkt te zijn dat alle veiligheidsproblemen die gebruikers ervaren moeten worden opgelost door de producenten. Dit onderscheid tussen producenten en gebruikers is bij internet niet te maken. Internet wordt juist gemaakt door de gebruikers.

XS4ALL wil hiermee niet zeggen dat ISP's op het gebied van veiligheid geen verantwoordelijkheid hebben, integendeel. XS4ALL benadrukt dat de verantwoordelijkheid bij een groot aantal partijen ligt: bij ISP's, maar ook bij (onder meer) gebruikers, leveranciers van hard- en software, producenten van financiële producten en de overheid. De veiligheid op internet kan alleen worden verbeterd door een gezamenlijke, strak geregisseerde inspanning van al deze partijen.

XS4ALL denkt dat de introductie van een veiligheidskeurmerk kan bijdragen aan de oplossing. Dit keurmerk wordt toegekend aan partijen (ISP's, leveranciers van hard- en software, etc.) die voldoen aan een best practice die is geformuleerd door onafhankelijke deskundigen. De best practices zoals beschreven in de brief van OPTA zijn wat XS4ALL betreft op zichzelf acceptabel. De best practices moeten gelden als ondergrens, die met de stand van de techniek van dag tot dag opschuift naar boven.

Ook de gebruiker heeft een belangrijke eigen verantwoordelijkheid. Gebruikers dienen in elk geval de meest voor de hand liggende actie te ondernemen, zoals het gebruik van een personal firewall, anti-spyware software en het (automatisch laten) installeren van beveiligings-updates voor de computer. Zij moeten daarbij worden geholpen door ISP's en leveranciers van hard- en software. Het kan niet zo zijn dat alle problemen op het bordje van ISP's worden gelegd, net zo min als het voorkomen van inbraken uitsluitend op het bordje van de fabrikant van voordeuren kan worden gelegd.

De overheid heeft een publieke taak bij het voorlichten van gebruikers over dit onderwerp. Het gebruik van internet is niet in alle opzichten veilig en zal dat vermoedelijk ook nooit zijn. Het zou helpen wanneer ook de overheid meer zou bijdragen aan dit besef, door middel van meer goede voorlichting over de risico's die inherent zijn aan het gebruik van internet. Tevens zou de overheid incident response teams online kunnen faciliteren. Tenslotte zou het helpen wanneer de overheid in internationaal verband de opsporing van cybercrime zou opvoeren.

Nu OPTA geheel voorbij gaat aan de rol van al deze partijen is het voorlopig standpunt van OPTA gebaseerd op een onvolledige analyse van het probleem en daardoor onjuist.

Artikel 11.3 Tw. is niet van toepassing

Het standpunt is bovendien gebaseerd op een twijfelachtige uitleg van de wet. Artikel 11.3 van de Telecommunicatiewet is niet geschreven voor dit doel. Dit artikel geeft OPTA de bevoegdheid om bij internet- en telecommunicatieaanbieders 'passende maatregelen' op te leggen om persoonsgegevens te doen beveiligen. Het artikel vindt zijn oorsprong in de privacyrichtlijn uit 1997[1] en lijkt niet bedoeld om malware, spyware, botnets etc. te bestrijden. Afgezien daarvan is het bereik van dit artikel onmiskenbaar te beperkt. Het artikel beoogt bijvoorbeeld wel particuliere, maar niet zakelijke gebruikers te beschermen. XS4ALL ziet niet in waarom zakelijke gebruikers geen recht op veilig internet zouden hebben. Het artikel voorziet niet in een rol voor de overige stakeholders, maar richt zich uitsluitend op internet- en telecommunicatie-aanbieders.

Het is opmerkelijk dat OPTA in haar voorstel voorbij gaat aan de twijfel over de toepasselijkheid van dit artikel. Zowel Stratix als de door Stratix geïnterviewde partijen hebben stilgestaan bij het feit dat deze bepaling aan OPTA geen duidelijke bevoegdheid verleent. OPTA wil dit kennelijk niet horen onder het motto: bij twijfel reguleren. OPTA neemt de wet zoals die is, en als dat betekent dat belangrijke stakeholders niet aanspreekbaar zijn dan is dat maar zo. Als OPTA de problemen serieus wil aanpakken kan en mag OPTA niet voorbij gaan aan de rol van partijen die toevallig niet in artikel 11.3 Tw. worden genoemd.

Is regulering nodig?

XS4ALL is geen principieel tegenstander van regulering op dit terrein, maar meent wel dat dit initiatief te vroeg komt. Eerst moet een beter beeld worden gekregen van de inspanningen die nu al worden geleverd.

XS4ALL benadrukt dat zij, net als een grote meerderheid van ISP's, nu al een zeer adequaat niveau van beveiliging biedt aan haar gebruikers. Waar mogelijk is XS4ALL haar klanten behulpzaam. XS4ALL neemt hiermee haar maatschappelijke verantwoordelijkheid. Vanzelfsprekend is veiligheid ook inzet van de hevige concurrentiestrijd in deze markt. ISP's werken permanent aan oplossingen voor telkens nieuwe bedreigingen op het gebied van veiligheid. XS4ALL claimt een leidende positie op dit terrein. Gebruikers moeten de keuze hebben tussen

---

[1] Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector

aanbieders met verschillende kwaliteitniveaus, al dan niet met verschillende prijskaartjes.

Net als een grote meerderheid van ISP's heeft XS4ALL alle maatregelen die OPTA verplicht wil stellen reeds genomen (op onderdelen gaat XS4ALL zelfs verder). Dit betekent niet dat ISP's nu achterover kunnen leunen. Dit betekent wel dat men terughoudend moet zijn met het opleggen van maatregelen.

XS4ALL onderkent dat niet alle ISP's een adequaat niveau van beveiliging bieden. De vraag is dan of een hele sector gereguleerd moet worden om het beveiligingsniveau bij een kleine minderheid van ISP's te verhogen. XS4ALL volgt OPTA hierin niet. Internet wordt gekenmerkt door een groot zelfoplossend vermogen. De onderhavige problemen zijn weliswaar nog niet allemaal opgelost, maar in de regel komen gebruikers zelf een heel eind, zonder dat regulering nodig is. De basis van internet, de protocollen en toepassingen zijn door collectieve inspanningen van gebruikers tot stand gekomen, zonder regulering. Partijen spreken elkaar ook aan op het gebied van veiligheid. Wanneer een bepaalde ISP door zijn collega's wordt beschouwd als bron van veiligheidsproblemen wordt die ISP daarop aangesproken. In de praktijk worden op die manier oplossingen gevonden voor problemen.

Kortom, marktpartijen zijn nu al creatief met het bedenken van oplossingen. Het hiervoor genoemde veiligheidskeurmerk kan dit versterken en zou een kans moeten krijgen. De extra voorlichting moet er komen. Alleen wanneer dan nog geen verbetering optreedt of valt te verwachten kan gedacht worden aan regulering. Daarbij moet wel worden bedacht dat dit probleem een internationale dimensie heeft. Een groot deel van de bedreigingen is afkomstig uit verre streken waar de Nederlandse wetgever en Nederlandse toezichthouders geen invloed hebben. Tevens is in geval van regulering een goede kosten-batenanalyse nodig, die ontbreekt in de analyse van OPTA.

2 Vragenlijst

Na de algemene opmerkingen hierboven zal XS4ALL ingaan op de vragen van OPTA uit haar brief van 17 april jl.

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?*

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.*

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 eerste drie vragen worden tezamen beantwoord. XS4ALL heeft meegewerkt aan het rapport van Stratix en kan zich goed vinden in het beeld dat in het rapport wordt geschetst van relevante dreigingen voor Nederlandse internetgebruikers. Een nadere aanvulling is wellicht mogelijk maar is op dit moment minder van belang. Wel van belang is een integrale benadering van de problematiek, zie hierboven. De vraag welke maatregelen 'passend' zijn in de zin van artikel 11.3 Tw. is niet relevant, aangezien artikel 11.3 Tw. niet van toepassing is.

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 de rol van het overleg)?*

EZ zou het initiatief moeten nemen, waarbij aangesloten kan worden bij bestaande initiatieven voor samenwerking, zoals GovCERT en NICC.

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*

Samenvattend komt XS4ALL tot de volgende slotsom:

1.) OPTA ontleent haar bevoegdheid aan een bepaling in de Telecommunicatie-wet die hiervoor niet is geschreven;
2.) OPTA richt zich ten onrechte alleen op internetaanbieders;
3.) de voorgestelde maatregelen zijn door een grote meerderheid van de aanbieders al genomen;
4.) additionele maatregelen kunnen nuttig zijn mits deze worden ondersteund door alle betrokkenen.

XS4ALL beschouwt dit initiatief van OPTA als overregulering. Overregulering kost de gemeenschap meer dan het oplevert en is niet bevorderlijk voor innovatie. Overregulering draagt ook niet bij aan het creëren van een gunstig investeringsklimaat. XS4ALL geeft OPTA daarom in overweging om haar voorlopig standpunt te herzien en licht deze reactie graag nader toe tijdens de ronde tafel bijeenkomst op 1 juni as.

Met vriendelijke groet,
XS4ALL Internet B.V.

Niels van Veen
Public Affairs Officer a.i.