

Terms of Reference Platform Internetveiligheid

Aangepast op basis van 2^e Premeeeting op 02-06-2009

Inleiding

Uit de diverse gevoerde gesprekken van de afgelopen periode is vanuit de overheid en marktpartijen de behoefte verkend en erkend om te komen tot een onafhankelijk platform op het gebied van Internetveiligheid, waarin verschillende initiatieven op dit terrein samen komen. De grote complexiteit en toenemende afhankelijkheid tussen actoren, technieken en functies, alsmede maatschappelijke trends, vragen om nadere afstemming en het nemen van verantwoordelijkheid door de gehele (internet-)keten, ISP's en andere service providers, softwareleveranciers, banken en andere bedrijven, overheid en consumenten/internetgebruikers. Het platform beoogt maatschappelijke trends te signaleren, inhoudelijke samenhang tussen diverse onderwerpen te coördineren en te komen tot efficiency in de bestaande overlegstructuren.

Het doel van het platform Internetveiligheid is om een structurele bijdrage te leveren aan het verbeteren van de internetveiligheid voor de consument via het bieden van een neutrale plaats waarin:

- Op strategisch niveau deze dialoog plaats kan vinden;
- Concrete afspraken en initiatieven tot stand komen

In de Terms of Reference (ToR) worden bepalingen met betrekking tot de inrichting en werkwijze van het platform omschreven. Deze schetst de prioriteiten voor de onderwerpen van het platform in 2009 evenals bijbehorende mogelijke acties in 2009. De prioriteiten zijn gekozen op basis van de achtergrondnotitie (bijlage), "rijpheid" (maturiteit) van mogelijke initiatieven en actualiteit van thema's. Naast dit inhoudelijke aspect (de "wat"-vraag), schetst deze notitie ook de proceskant (de "hoe"-vraag). Daarvoor is een ToR opgesteld, die inzicht geeft in de *scope*, *besturing*, *besluitvorming*, *communicatie en samenstelling* van het platform. De ToR zijn na overleg op 2 juni aangepast op basis van de inbreng van de aanwezige partijen.

Zoals in de achtergrondnotitie omschreven omvat internetveiligheid verschillende invalshoeken waaronder netwerk- en informatiebeveiliging, computercriminaliteit en vertrouwen. Om betrokken partijen beter inzicht te bieden in de scope van het platform Internetveiligheid, zal een omgevingschets worden voorbereid van reeds bestaande platformen, overlegstructuren en de onderwerpen/initiatieven die daar al behandeld worden.

In deze notitie worden behandeld:

- Terms of Reference
- Prioriteiten en acties voor het platform in 2009
- Voorraad Agenda 2009-2011

Terms of Reference

Scope

Het platform stelt zich ten doel een structurele bijdrage te leveren aan het verbeteren van de internetveiligheid voor de consument/internetgebruiker. Het platform richt zich op strategische onderwerpen in relatie tot internetveiligheid en streeft naar een agenderende en voorbeeldfunctie door maatschappelijke trends te signaleren en te vertalen naar concrete initiatieven. Hiervoor worden door deelnemende partijen afspraken gemaakt over verschillende onderwerpen rondom internetveiligheid. De focus van het platform ligt op het verhogen van internetveiligheid o.a. ter voorkoming van strafbare en/of onrechtmatige zaken gezien vanuit het perspectief van de consument/internetgebruiker. Onderwerpen als beschikbaarheid van de netwerken vallen buiten het bereik van dit platform.

Samenstelling, besluitvorming & inrichting van het platform

Het platform zal bestaan uit een vergadering van directievoorzitters en vertegenwoordigers van de deelnemende publieke partijen. Dit platform komt 2 keer per jaar bijeen. Het platform wordt ondersteund door een voorbereidende werkgroep die in principe vier keer per jaar bij elkaar komt. Het platform zal worden voorgezeten door een onafhankelijk externe voorzitter.

ECP-EPN zal het platform en de voorbereidende werkgroep organiseren en ondersteunen.

Het platform kan vaststellen dat bepaalde vraagstukken een gedetailleerde uitwerking of nadere bespreking behoeven in een of meerdere specifieke werkgroepen.

Bij de start van het platform wordt tevens gestreefd naar het zoveel mogelijk onderbrengen van, c.q. afstemming organiseren met, lopende werkgroepen op het gebied van veilig internet in Nederland zoals: de werkgroep NTD en het botnetproject.

In de werkgroepen wordt onder andere gewerkt aan specifieke afspraken, codes of richtlijnen. Deze groepen kunnen een bredere en andere samenstelling hebben dan het platform en kunnen eigen werkwijzen en procedures hanteren. Voorstellen voor een aanpak of oplossing dan wel resultaten van de werkgroepen worden besproken en daarna voorgelegd aan het platform.

De afspraken die het platform maakt/vaststelt met betrekking tot het verhogen van internetveiligheid zijn bindend voor de partijen, die participeren in het platform. Partijen zien toe op voldoende mandaat bij afgevaardigden in zowel het platform zelf als in de voorbereidende werkgroep. Afspraken worden zoveel mogelijk op basis van consensusvorming gemaakt.

Om het platform de gewenste daadkracht en slagkracht te geven is gekozen om van start te gaan met een beperkt aantal partijen die zullen deelnemen in het platform. De samenstelling van het platform is in samenspraak met de partijen gemaakt op basis van de positie van partijen in de markt, diversiteit wat betreft positie in de keten, bereidheid tot actieve participatie en “netwerk” met andere partijen die betrokken kunnen worden bij de werkzaamheden. Uitbreiding van het platform geschiedt door coöptatie op voorstel van de leden waarover bij meerderheid van de zittende leden wordt besloten.

De voorlopige samenstelling voor het platform in 2009 bestaat uit de volgende partijen:

- ECP-EPN, platform voor de informatiesamenleving (facilitator)
- KPN
- UPC
- Ziggo
- Vodafone Nederland
- Stichting Internet Domeinregistratie Nederland
- Dutch Hosting Provider Association
- Microsoft Nederland

- Ministerie van Economische Zaken
- Ministerie van Justitie

Communicatie

In november 2009 zal een officiële ‘kick-off’-bijeenkomst worden georganiseerd, waar elk van de partijen zich bij monde van een vertegenwoordiger van het hoogste bestuurlijke niveau uitspreekt actief bij te zullen dragen aan het welslagen van het platform.

Het platform is transparant in de gemaakte afspraken en communiceert de genomen afspraken, besluiten en/of initiatieven ook naar niet-deelnemende partijen van het platform en andere geïnteresseerden.

De strategische doelstelling van het platform alsmede de ambitie van het platform om een voortrekkersrol te vervullen, betekent dat het platform duidelijk zichtbaar zal zijn in de buitenwereld en actief aandacht zal vragen voor de gemaakte afspraken. Beoogd effect van het platform is dat andere partijen onder het mom ‘goed voorbeeld doet volgen’ ook maatregelen treffen of deelnemen aan de maatschappelijke discussie. Het zal hierbij gebruik maken van diverse communicatiekanalen waaronder het programma Digibewust en Digivaardig.

Prioriteiten 2009

1. Gedragscode Notice and Takedown (NTD)

Het platform stelt zich ten doel de strafbare en onrechtmatige content terug te dringen. Een middel daarvoor is de gedragscode Notice and Takedown welke in 2008 in werking is getreden en de procedures beschrijft welke dienen te worden gevolgd bij klachten over onrechtmatige inhoud.

De acties van het platform voor 2009 zullen gericht zijn op het beheer van de gedragscode en de verbreding ervan naar andere partijen. Een onderdeel daarvan zal zijn het verhogen van het bewustzijn van het bestaan van de code.

Het werken met de code zal in de praktijk uitwijzen in hoeverre de code in deze gevallen voldoende toereikend is en of (en welke) aanpassingen in de toekomst nodig zijn. Het laten aansluiten van meer ISP's en andere dienstverleners zal de effectiviteit ten goede komen.

2. Filteren/blokkeren van kinderpornografisch materiaal

Het platform stelt zich ten doel de aanwezigheid van kinderpornografisch materiaal op internet terug te dringen. Met het Ministerie van Justitie en de ISP's zijn afspraken gemaakt over het filteren en blokkeren van kinderporno uit het buitenland. Dit traject zal in nauwe samenspraak worden ontwikkeld met het platform gezien de grote overlap van participerende partijen en voorzover het de overlegstructuur raakt onder worden gebracht bij dit Platform.

3. Aanpak van botnets

Het platform stelt zich ten doel de verspreiding van malware – o.a. via botnets – terug te dringen. In het kader van de zorgplicht wordt op het moment van schrijven een convenant opgesteld met betrekking tot de aanpak van botnets en of er daaropvolgend tijdelijke afsluiting van klanten plaatsvindt met geïnfecteerde pc's (quarantaine) totdat deze zijn schoongemaakt. In de komende maanden bepaalt een communicatiegroep hoe er precies met het convenant naar buiten wordt getreden. Na overleg en overdracht van de OPTA kan naar verwachting in september met een werkgroep worden gestart.

4. Voorlichting

Het platform zal aandacht besteden aan voorlichting aan de consument/internetgebruiker met betrekking tot verschillende onderwerpen rondom internetveiligheid. Doel is om de onderlinge

initiatieven op elkaar af te stemmen en bijvoorbeeld voeding te geven aan het programma Digivaardig en Digibewust. Het is nadrukkelijk niet de bedoeling dat het platform Internetveiligheid de rol en het kanaal van Digibewust & Digivaardig overneemt.

Voorraad Agenda 2009-2011

Naast deze prioriteiten zijn er ook andere onderwerpen mogelijk die het platform in 2009 of in komende jaren op zou kunnen pakken. Te denken valt aan:

- Toepassen van *Deep Packet Inspection* (vragen rondom aansprakelijkheid, kwaliteit van dienstverlening en mogelijke effecten op concurrentie en privacy);
- Procedures rondom eliminatie en blokkeren van malware (bijvoorbeeld standaardisatie van procedures en gebruikte methoden en technieken zoals het gebruik van *egress-filtering*, of afspraken rondom melding beveiligingsincidenten);
- Beveiliging van nieuwe internet- en web 2.0 diensten (de beveiliging van deze diensten vormt in toenemende mate de zwakste schakel voor de veiligheid op internet en vereist een gezamenlijke aanpak van content providers, software vendors, ISP's en overheid);
- Afspraken rondom implementatie en gebruik van DNSSEC en IPv6;
- Privacy en databescherming (beveiliging van systemen/databases, mogelijkheden en voorwaarden commercieel gebruik persoonsgegevens, preventie phishing, identiteitsfraude e.d.).
- Filesharing/auteursrechten.

Mits deze onderwerpen binnen de gedefinieerde scope van het platform kunnen worden opgepakt.