

**Speech Staatssecretaris van Economische Zaken,
Frank Heemskerk, bij de kickoff van het Platform
Internetveiligheid, op 8 december 2009 in Den Haag**

Dames en heren,

Allerlei activiteiten op het gebied van internetveiligheid samenbrengen. Dát was de wens van de overheid en van een aantal marktpartijen. Vandaag is die wens werkelijkheid geworden. We gaan samen werken aan een veiliger internet!

Internet is niet meer weg te denken uit ons leven. E-mail en andere vormen van telecommunicatie raken steeds nauwer verweven met onze economische activiteiten.

Voor de groei van internet is een blijvend vertrouwen in het gebruik ervan cruciaal. Incidenten treffen niet alleen de economie, maar ook het vertrouwen in digitale diensten en de netwerken via welke ze beschikbaar komen.

Dat vertrouwen bij burgers en bedrijven is essentieel voor een goed functionerende, steeds digitaler wordende economie. Vertrouwen dat op twee pijlers rust. Ten eerste moet ICT betrouwbaar zijn (het moet dus niet om de haverklap uitvallen). En ten tweede moet internet veilig zijn.

Mensen moeten dus veilig en vertrouwd gebruik kunnen maken van internetdiensten. Ik denk dan niet alleen aan internetbankieren zonder dat er sprake is van phishing. Maar je moet ook mail kunnen lezen zonder door allerlei spam heen hoeven te worstelen.

Of denk aan social networking-sites als Hyves of Facebook, zonder dat jouw privacy in het geding komt.

Niet minder belangrijk is, dat kinderen kunnen chatten met hun vrienden of informatie op kunnen zoeken voor een werkstuk, zonder dat ze lastiggevalen worden.

Gelukkig zijn er allerlei initiatieven om kinderen mediawijs te maken. Ze kunnen gebruikmaken van de kindveilige browser MyBee. En op diplomaveiliginternet.nl worden ze bewust gemaakt van de leuke dingen van het internet, maar ook van de minder leuke dingen zoals digitaal pesten of andere onaangename praktijken.

Deze en andere initiatieven om het internet veilig te maken, zijn broodnodig. Het internet biedt veel kansen, helaas ook aan mensen of organisaties die oneigenlijk verkregen informatie of gegevens misbruiken. Of zelfs criminelen activiteiten ontplooiën.

Steeds werken overheid en private organisaties samen om het internet veiliger te maken. Ik geef een paar voorbeelden.

Vorig jaar gaf ik de aftrap voor de gedragscode 'Notice-and-Take-Down'. Deze gedragscode maakt helder hoe internetbedrijven om moeten gaan met meldingen over illegale websites en websites met illegale content.

Ook de postbus 51 campagne “Veilig Internetten” van zomer 2009 heeft laten zien hoe groot de slagkracht kan zijn als alle publieke en private partijen de handen ineen slaan.

Voorbeelden die laten zien dat we in de online arena allemaal een taak hebben te vervullen. Niet alleen de ISP's, maar ook de aanbieders van online diensten. En de overheid natuurlijk.

Die moet zorgen voor randvoorwaarden, een klimaat scheppen waarin alle partijen in staat zijn hun verantwoordelijkheden te nemen. Denk daarbij aan samenhang, procesmanagement en wetgeving; hoewel dat laatste in mijn beleving niet het fundament, maar het sluitstuk van beleid moet zijn.

Het Platform Internetveiligheid, dat vandaag officieel wordt gelanceerd, is een bijzonder mooi voorbeeld van samenwerking tussen publieke en private organisaties. Ik ben trots op de partijen die bereid waren om het Platform samen met mij vorm te geven. Dat ze, samen met mij, hebben ingezien dat dit Platform een 'must' is als we samen het internet veiliger willen maken en houden.

Het Platform is de plek om maatschappelijke trends te signaleren, de inhoudelijke samenhang tussen de diverse onderwerpen te coördineren en de overlegstructuren tussen markt en overheid efficiënter te organiseren.

Dames en heren,

Deelname aan het Platform Internetveiligheid is niet vrijblijvend. Niet alleen praten maar ook doen! Het Platform is ook de plek om concrete afspraken met elkaar te maken over de aanpak van bijvoorbeeld filteren en blokkeren van kinderporno (waarover de minister zojuist sprak), botnets en invulling van een internetbrede zorgplicht.

Afspraken die leiden tot concrete oplossingen. En daarbij geldt: goed voorbeeld doet de rest volgen.

We verwachten van het Platform dat het lopende projecten oppakt en versnelt. Denk bijvoorbeeld aan verbreding en verdieping van de gedragscode 'Notice-and-Take-Down' waar ik net over sprak. Of aan de aanpak van botnets, zombiecomputers die veel PC's overheersen en daarmee ons het leven heel zuur kunnen maken.

Zo hebben de ISP's die consumenten bedienen in Nederland in augustus 2009 afspraken gemaakt over hoe ze zombiecomputers in hun netwerken beter kunnen aanpakken. Op initiatief van OPTA hebben bijna alle ISP's (> 95%) afgesproken dat zij informatie over botnets uitwisselen, bots in hun eigen netwerken isoleren en de gebruikers helpen om hun computer schoon te maken. Allemaal hebben ze zich aan deze aanpak gecommitteerd. Ook dit project zal worden ondergebracht bij het Platform Internetveiligheid

Voorlichting is en blijft daarin belangrijk. Vanuit het Platform sluiten we aan op bestaande initiatieven als het programma Digivaardig & Digibewust, met de bijbehorende website mijndigitalewereld.nl.

Naast lopende projecten zullen ook nieuwe thema's worden opgepakt. Ik verwacht de komende tijd veel aandacht voor privacy. Allerlei toepassingen als het EPD, de OV-chipcard of de slimme energiemeter roepen vragen over het gebruik van persoonsgegevens op.

Privacy is een onderwerp dat onlosmakelijk met ict-toepassingen verbonden is. In veel ict-toepassingen wordt gebruik gemaakt van persoonsgegevens. En dat geeft veel mensen het gevoel dat hun privacy wordt geschonden, meer dan bij de uitwisseling van papieren persoonsgegevens. Juist daarom moeten we de discussie over e-privacy heel zorgvuldig voeren. Dat kan aan de hand van het privacy-model.

Mijn privacy-model heb ik twee weken geleden gepresenteerd op het jaarcongres ECP-EPN. Dat model bestaat onder andere uit drie vragen:

Eén: is er sprake van een probleem rond privacy?

Twee: als er sprake is van een privacyrisico, kunnen we dan inschatten hoe groot dat risico is? Een medisch dossier van 1000 mensen op straat is immers iets anders dan dat u weet of ik gisteren een bloemkool of een prei heb gekocht.

En drie: als er risico's zijn, hoe kunnen we die dan wegnemen?

Het vierde onderdeel van het privacy-model is de afweging. Als we de drie vragen hebben beantwoord, dan kunnen we afwegen hoe belangrijk een dienst voor ons is en welk belang wij daarbij hechten aan onze privacy. Vaak wegen de voordelen van de dienst op tegen de nadelige gevolgen voor onze privacy, soms niet.

Ik hoop dat dit kan worden gebruikt in de discussie om het bewustzijn rond privacy te verhogen.

Dames en heren,

Ik rond af.

Laten we ervoor zorgen dat mensen vertrouwen houden in het internet en de diensten van de informatiemaatschappij, doordat zij hun foto's, netwerk, gegevens en kennis via internet veilig kunnen delen.

Dat bereiken we alleen als *wij* onze kennis delen, als we onze initiatieven samenvoegen. Ik heb er alle vertrouwen in dat het Platform Internetveiligheid hier een goede schakelfunctie in kan hebben. Volgend jaar zullen we terugkoppelen over de eerste resultaten.

Veel succes daarbij!