Aan

De Voorzitter van de Tweede Kamer der
Staten-Generaal
Binnenhof 4
2513 AA ‘s-GRAVENHAGE

Datum	Uw kenmerk	Ons kenmerk	Bijlage(n)
6 april 2007		ET/IT / 7034250	

Onderwerp

Beantwoording, mede namens de Minister van Justitie, van kamervragen van het lid De Roon (PVV) aan de Staatssecretaris van Economische Zaken over het bericht dat 'Nederland een broeinest is van webcriminelen' (ingezonden 25 januari 2007)

1
Hebt u kennisgenomen van het artikel “Nederland als broeinest van webcriminelen”[1] alsmede van het Sophos Security Threat Report 2007[2], waaruit blijkt dat Nederland de vierde plaats inneemt op een wereldranglijst van landen met websites die zogenaamde “malware” bevatten?

Antwoord
Ja.

2
Klopt het beeld dat Nederland een vrijplaats is voor websites met agressieve en schadelijke malware door bevindingen van de opsporingsdiensten?

Antwoord
Neen. Dit beeld veronderstelt dat regelgeving, dan wel de handhaving daarvan, op dit terrein afwezig is of ernstig tekortschiet. Zowel bestuursrechtelijk als strafrechtelijk zijn er echter verschillende artikelen van toepassing die verspreiding van malware en spyware in Nederland, verbieden (art. 4.1 Besluit universele dienstverlening en

[1] http://www.planet.nl/planet/show/id=118880/contentid=805318/sc=32c979

[2] http://www.sophos.com/pressoffice/news/articles/2007/01/secrep2007.html

Bezoekadres		Doorkiesnummer	Telefax
Bezuidenhoutseweg 30		7280	
Hoofdkantoor	Telefoon 070-379 6106	Behandeld door	
Bezuidenhoutseweg 30	Telefax 070-379 6154	R. Volf	
Postbus 20101	Email f.heemskerk@minez.nl		
2500 EC 's-Gravenhage	Website www.minez.nl	*Verzoeke bij beantwoording van deze brief ons kenmerk te vermelden*	

eindgebruikersbelangen, Wetboek van Strafrecht art. 138a[3]). Navraag bij het Openbaar Ministerie en de Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA) leert dan ook dat dit beeld niet herkend wordt. De regels worden actief gehandhaafd door de OPTA. Gezien het complexe karakter van overtredingen wordt hiertoe structureel overleg tussen de verschillende toezichthouders gevoerd om relevante kennis en ervaringen uit te wisselen. Hierdoor kunnen wetsovertreders op de meest effectieve manier worden aangepakt. Deze methode sluit aan bij de opzet van de overheid om te komen tot een gezamenlijke (netwerk-)aanpak van cybercriminaliteit, in een Nationale Infrastructuur Cybercrime (NICC). Zo is begin 2006 een Notice and Take Down functie voor de bancaire sector gerealiseerd om phishing websites tegen te houden en/of te verwijderen. Daarnaast is een informatieknooppunt in ontwikkeling voor de vitale sectoren dat zich richt op de ontwikkeling en deling van kennis evenals op informatieverstrekking. In oktober 2006 is de bancaire sector als eerste aangesloten bij het informatieknooppunt. Internationaal is er nog weinig ervaring met dergelijke actieve handhaving van genoemde regelgeving. Nederland loopt voorop en wordt door de rest van de wereld nauwlettend gevolgd.

Naast wet- en regelgeving speelt ook het bedrijfsleven zelf een belangrijke rol bij de bestrijding van malware. Dankzij de hoge penetratie van breedbandaansluitingen, hoogwaardige koppelingen met het wereldwijde internet via onder meer de AMS-IX en kennis op het gebied van ICT, is Nederland een aantrekkelijke uitvalbasis voor internetondernemingen. Dit brengt echter ook met zich dat Nederland aantrekkelijk kan zijn voor providers/webhostingbedrijven die het minder nauw nemen met de naleving van de wet- en regelgeving. In de praktijk blijkt echter dat de meeste providers wel degelijk zelf hun verantwoordelijkheid nemen ten aanzien van de verwijdering van malware/spyware van de computers van hun klanten. Ook jegens consumenten neemt de branche haar verantwoordelijkheid, getuige het feit dat in mei van dit jaar een nieuwe internet geschillencommissie gelanceerd wordt.
Ten aanzien van het rapport van Sophos merk ik op dat deze onderneming heeft aangegeven een ruime opvatting van malware te hanteren. Het betreft bestanden waarvan niet met zekerheid vaststaat dat zij schadelijk zijn voor een PC, maar dit wel zouden kúnnen zijn. Het beeld van “vrijplaats” wordt dan ook niet door rapporten van andere bedrijven bevestigd.

3
Deelt u de mening dat, gelet op het intensieve internetgebruik van het overgrote deel van de Nederlandse bevolking, het schadelijk en schandelijk is dat de spreekwoordelijke

[3] Computervredebreuk

Nederlandse tolerantie ruimte biedt voor de beheerders van websites met malware en voor de exploitanten van webhostingbedrijven die de beheerders van websites met malware toegang verlenen tot het world wide web?

Antwoord
Neen. Onduidelijk is, waar Sophos haar bewering, dat Nederland nalatige webhostingbedrijven beschermt onder verwijzing naar de vrijheid van meningsuiting, op baseert. Van een te tolerante houding is geen sprake. De bestuursrechtelijke handhaving door OPTA in Nederland is recent door de Europese Commissie als voorbeeld gesteld voor andere Europese landen (COM(2006) 688 definitief).

4
Wat gaat u doen om de Nederlandse internetgebruiker te beschermen tegen dergelijke praktijken?

Antwoord
Als uitvloeisel van het Coalitieakkoord zal het Kabinet voor het verbeteren van de veiligheid komen met maatregelen tot meer preventie en ketensamenwerking, in samenwerking met het bedrijfsleven. In de eerste plaats wordt daartoe binnen het NICC publiek-privaat gewerkt aan een hechte samenwerking in de gehele keten, van aanbieder tot eindgebruiker. Het NICC heeft tot doel om kennisdeling te bevorderen, blinde vlekken op te sporen en te dichten en noodzakelijke functies in de bestrijding verder te ontwikkelen en structureel in te bedden. Een van de belangrijkste resultaten is het reeds genoemde informatieknooppunt voor de vitale sectoren. Daarnaast is bewustwording, ook aan de zijde van de eindgebruiker, een belangrijk element bij het verbeteren van de veiligheid. Hieraan wordt onder meer door middel van het programma “Digibewust” invulling gegeven. Eveneens heeft dit publiek- private samenwerkingsverband ten doel de internetgebruiker vertrouwd te maken met de technische mogelijkheden om zichzelf optimaal te kunnen beschermen tegen dergelijke praktijken. Zo is bijvoorbeeld het lespakket ‘Diploma Veilig Internet’ voor scholen gratis beschikbaar.
Samen met het bedrijfsleven zal “Digibewust” activiteiten ondernemen zoals het ontwikkelen van een tool voor het toetsen van websites op veiligheidrisico's, het aandragen van goede voorbeelden en het ontwikkelen van een veiligheidscertificaat.

5
Bent u bereid om prioriteit te geven aan de opsporing en vervolging van de beheerders en exploitanten als hiervoor bedoeld? Zo ja, welke concrete stappen zult u nemen en op welke termijn? Zo neen, waarom niet?

Antwoord

In de eerste plaats zij verwezen naar de beantwoording van vraag 2, 3 en 4. In de tweede plaats heeft OPTA aangegeven dat de aanpak van ongevraagde software een prioriteit is in 2007. Een team van digitaal rechercheurs en juristen doet op dit ogenblik onderzoeken, die zullen leiden tot sancties tegen wetsovertreders. Ook zal de OPTA internetaanbieders op hun verantwoordelijkheid aanspreken om een bijdrage te leveren aan de bevordering van internetveiligheid (artikel 11.3 Tw). Het Openbaar Ministerie heeft in zijn recente meerjarenplan “Perspectief op 2010” cybercriminaliteit als een van de prioritaire thema’s voor de komende jaren benoemd.

(w.g.) drs. F. Heemskerk