COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 15.11.2006
COM(2006) 688 definitief

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITE VAN DE REGIO'S

betreffende de strijd tegen spam, spyware en kwaadaardige software

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITE VAN DE REGIO'S

betreffende de strijd tegen spam, spyware en kwaadaardige software

(Voor de EER relevante tekst)

1. DOEL VAN DE MEDEDELING

De samenleving is zich er steeds meer van bewust hoe essentieel de moderne netwerken en diensten voor elektronische communicatie zijn geworden voor het dagelijks leven, in de bedrijfswereld en thuis. Een breed spectrum van diensten hangt af van betrouwbare en veilige technologieën. De mededeling van de Commissie inzake een strategie voor een veilige informatiemaatschappij[1] heeft een algemene verbetering van de netwerk- en informatie-veiligheid ten doel en in bedoelde mededeling verzoekt de Commissie de particuliere sector om kwetsbare plekken in de netwerken en de informatiesystemen aan te pakken die kunnen worden geëxploiteerd om spam en kwaadaardige software te verspreiden. In de mededeling van de Commissie over de herziening van het regelgevingskader van de EU voor elektronische communicatienetwerken en diensten[2] worden nieuwe regels voorgesteld om de veiligheid en de bescherming van de persoonlijke levenssfeer te verbeteren.

De huidige mededeling heeft betrekking op spam (ongevraagde commerciële informatie)[3] en bedreigingen zoals spyware (spionagesoftware) en kwaadaardige software. Er wordt een overzicht gegeven van de inspanningen die tot dusverre zijn geleverd om deze bedreigingen tegen te gaan en er worden voorstellen gedaan voor verdere actie, zoals:

- versterking van de communautaire wetgeving;

- betere wetshandhaving;

- samenwerking binnen en tussen de lidstaten;

- politieke en economische dialoog met derde landen;

- initiatieven van de bedrijfswereld;

- O&O-activiteiten.

---

1 COM(2006) 251.definitief
2 COM(2006) 334 definitief.
3 COM(2004) 28.definitief

2. HET PROBLEEM - DE ZICH STEEDS ONTWIKKELENDE AARD VAN DE BEDREIGINGEN

De hoeveelheid spam[4] is in de afgelopen 5 jaar aanzienlijk toegenomen[5]. Volgens bronnen uit de bedrijfswereld maakt spam momenteel 50 tot 80% uit van de aan de eindgebruikers gerichte berichten[6]. Hoewel het grootste deel van die spamberichten van buiten de EU komt, zijn Europese landen nu verantwoordelijk voor 25% van de doorgestuurde spamberichten[7]. De wereldwijde kosten van spam worden geraamd op 39 miljard € in 2005. De kosten van spam in de grootste Europese economieën zijn geraamd op 3,5 miljard € voor Duitsland, 1,9 miljard € voor het Verenigd Koninkrijk en 1,4 miljard € voor Frankrijk[8]. Spamming wordt beschouwd als 'een bedrijf' op zich. Spammers huren of verkopen lijsten van 'geoogste' e-mailadressen voor marketingdoeleinden aan ondernemingen. Spam over het internet is bijzonder winstgevend. Dit heeft te maken met het enorme bereik van het medium en de lage kosten voor het versturen van massale hoeveelheden berichten. Tegelijkertijd kunnen bescheiden investeringen met het oog op de bestrijding van spam significante resultaten opleveren. In Nederland bijvoorbeeld werd de Nederlandse spam met 85% verminderd dankzij een investering van **570 000 €** in spambestrijdingsapparatuur.

Ongevraagde e-mail was oorspronkelijk alleen maar een plaag, maar heeft steeds meer een frauduleus en crimineel karakter gekregen. Een bekend voorbeeld daarvan is het gebruik van zogenaamde 'phishing'-e-mails die eindgebruikers ertoe lokken om gevoelige informatie door te sturen via websites die de websites van legitieme ondernemingen imiteren, wat kan resulteren in identiteitsfraude en schade aan de reputatie van bedoelde ondernemingen. De verspreiding van spyware via e-mail of software die het on-linegedrag van een gebruiker bespioneert, blijft toenemen. Spyware wordt ook gebruikt om persoonlijke informatie zoals paswoorden en kredietkaartnummers te verzamelen.

De verzending van massale hoeveelheden ongevraagde e-mails wordt aanzienlijk vergemakkelijkt door de verspreiding van kwaadaardige software zoals wormen en virussen. Zodra die zijn geïnstalleerd kan de aanvaller de controle over een besmet computersysteem overnemen en dit omvormen tot een 'botnet',[9] waardoor de identiteit van de echte spammer verborgen kan blijven. Botnets worden voor frauduleuze en misdadige doeleinden gehuurd door spammers, phishers en spywareverkopers. Deskundigen uit de bedrijfswereld schatten dat botnets goed zijn voor meer dan 50 percent van de ongewenste e-mails[10]. De verspreiding van spyware en andere types van kwaadaardige software die de systemen van gebruikers en ondernemingen aanvallen, heeft een aanzienlijke economische impact. De wereldwijde financiële impact van malware (kwaadaardige software) wordt geraamd op 11 miljard € in 2005[11].

---

4 Met spam wordt ongevraagde informatie, bv. via e-mail, voor commerciële doeleinden bedoeld. Ongevraagde e-mails kunnen echter ook een vector voor kwaadaardige software en spyware zijn.

5 In 2001 maakte spam 7% van het totale e-mailverkeer uit.

6 Symantec 54%; Messagelabs 68,6 MAAWG 80-85.

7 Q1 2006 (Sophos): Azië 42,8%, N. Amerika 25,6%, Europa 25,0%, Z. Amerika 5,1%, Australazië 0,8%, Afrika 0,6%, overige 0,1%.

8 Ferris research, 2005.

9 Botnets zijn besmette computers die door spammers worden gebruikt om op grote schaal e-mails te versturen via illegaal geïnstalleerde software die de desbetreffende computers omvormt tot mailservers zonder dat de eigenaars van die computers daar kennis van hebben.

10 Meest door botnets geïnfecteerde landen volgens Symantec, (Q 3-4 2005): VS 26 %, VK 22%, China 9%, Frankrijk, Z. Korea, Canada 4%, Taiwan, Spanje, Duitsland 3%, Japan 2%.

11 Computer Economics: the 2005 Malware Report.

3. HET TOT DUSVERRE GEDANE WERK - ONDERNOMEN ACTIES SINDS 2004

De EU heeft in 2002 een **richtlijn betreffende de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie** vastgesteld waarbij **spam wordt uitgebannen**[12] door invoering van het beginsel van op toestemming gebaseerde marketing jegens natuurlijke personen. Ter aanvulling van de richtlijn heeft de Commissie in januari 2004 een mededeling inzake spam[13] gepubliceerd met een overzicht van relevante acties. In deze mededeling werd de noodzaak beklemtoond van actie door de verschillende betrokken partijen op het gebied van bewustmaking, zelfregulering/technische acties, samenwerking en handhaving. De Commissie is begonnen het aspect van de strijd tegen spam, spyware en malware in te passen in haar dialoog met derde landen. Voorts worden de consumenten krachtens de richtlijn betreffende oneerlijke handelspraktijken[14] beschermd tegen agressieve commerciële praktijken. Grensoverschrijdende samenwerking om dergelijke praktijken te bestrijden valt onder de verordening betreffende samenwerking met het oog op de consumentenbescherming[15].

3.1. Bewustmakingsacties

De mededeling van de Commissie heeft bijgedragen tot een grotere bewustmaking op nationaal en internationaal niveau betreffende het probleem van spam wereldwijd. Op EU-niveau is een '**Safer Internet *plus*'-programma** aangenomen dat tot doel heeft een veiliger gebruik van het internet en van de nieuwe on-linetechnologieën, met name voor kinderen, te bevorderen als onderdeel van een samenhangende aanpak door de Europese Unie.

De lidstaten hebben campagnes gelanceerd of ondersteund om de gebruikers bewust te maken van het spamprobleem en hen te helpen spam te bestrijden. In het algemeen hebben de ISP's (Internet Service Providers) hun verantwoordelijkheid genomen en hebben zij hun klanten advies en bijstand verleend inzake methoden om zichzelf tegen spyware en virussen te beschermen. In februari 2004 heeft de Commissie een OESO-**workshop** inzake spam georganiseerd. Zij heeft ook een actieve rol gespeeld bij de samenstelling van de **Anti-Spam Toolkit** van de OESO die een geheel van regelgevingsmaatregelen, technische oplossingen en ondernemingsinitiatieven ter bestrijding van spam omvat.

De 'World Summit on the Information Society' van de VN[16] **heeft erkend** dat spam moet worden aangepakt op de passende nationale en internationale niveaus. In 2004 en 2005 heeft de ITU thematische WSIS-conferenties (Wereldtop over de informatiemaatschappij) gehouden. De in november 2005 aangenomen Tunis-agenda van de WSIS bevat een oproep om het belangrijke en aanzwellende probleem van spam krachtdadig aan te pakken[17].

3.2. Internationale samenwerking

Spam is een grensoverschrijdende kwestie en er zijn dan ook diverse samenwerkings-initiatieven en grensoverschrijdende handhavingsmechanismen ingesteld. De Commissie heeft een **Contact Network of Spam Authorities** (CNSA) opgezet dat op gezette tijden

---

12 Richtlijn 2002/58/EG, artikel 13.
13 *Supra* 3.
14 Richtlijn 2005/29/EG, bijlage 1, punt 26.
15 Verordening (EG) nr. 2006/2004.
16 WSIS, Genève, december 2003.
17 Tunis-agenda, punt 41.

samenkomt, beste praktijken uitwisselt en samenwerkt op het gebied van grens-overschrijdende handhaving. Het CNSA heeft een samenwerkingsprocedure[18] uitgewerkt om de afhandeling van klachten waarbij verschillende landen betrokken zijn te vergemakkelijken. De Commissiediensten zijn waarnemer bij en ondersteunen het **London Action Plan** dat de handhavingsinstanties van 20 landen bijeenbrengt en dat een grensoverschrijdende samenwerkingsprocedure heeft uitgewerkt. In november 2005 heeft een gemeenschappelijke EU/CNSA – LAP-workshop plaatsgehad. In april 2006 heeft de OESO een aanbeveling betreffende grensoverschrijdende samenwerking bij de handhaving van wetgeving tegen spam aangenomen, waarin de handhavingsautoriteiten ertoe worden aangespoord informatie uit te wisselen en nauwer samen te werken[19].

De Commissie bevordert voorts **internationale samenwerkingsinitiatieven**. De VS en de EU zijn overeengekomen samen te werken om spam via gezamenlijke handhavingsinitiatieven aan te pakken en actief naar middelen te zoeken om illegale "spyware" en "malware" te bestrijden. De Commissie neemt ook deel aan de Canadese internationale samenwerkings-groep inzake spam. Er worden gesprekken gevoerd met de voornaamste internationale partners, zoals China en Japan. In verband met Azië heeft de Commissie de aanzet gegeven tot een gemeenschappelijke verklaring over internationale samenwerking ter bestrijding van spam, die in februari 2005 is aangenomen op de ASEM-conferentie (Asia-Europe Meeting) inzake elektronische handel[20].

In de in november 2005 op de Wereldtop over de informatiemaatschappij aangenomen Tunis-agenda wordt beklemtoond dat de veiligheid van het internet een gebied is waarop een betere internationale samenwerking vereist is en dat deze kwestie moet worden aangepakt in het kader van een versterkt samenwerkingsmodel voor internet-governance dat in het raam van de follow-up van de wereldtop ten uitvoer zal worden gelegd[21].

3.3. Onderzoek en technologische ontwikkeling

In het kader van het zesde OTO-kaderprogramma heeft de Commissie projecten opgezet om de betrokken partijen te helpen spam en andere vormen van malware te bestrijden. Deze projecten[22] bestrijken gebieden die gaan van de algemene monitoring van netwerken en de detectie van aanvallen tot de specifieke ontwikkeling van technologieën voor de bouw van filters om spam, phishing en malware op te sporen. Tot de resultaten behoren de oprichting van een onderzoeksgemeenschap die zich specifiek bezighoudt met de opsporing en bestrijding van malware en de ontwikkeling van een Europese infrastructuur om het internetverkeer meer van nabij te volgen. Recentelijk zijn activiteiten gestart op het gebied van adaptieve phishingfilters die tot dusver onbekende bedreigingen en cyberaanvallen kunnen detecteren. De financiële inspanning ten behoeve van deze activiteiten beloopt 13,5 miljoen €.

---

18 http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf

19 http://www.oecd-antispam.org/

20 http://www.asemec-london.org/

21 Tunis-agenda punt 39-47. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

22 www.diademhttp://cordis.europa.eu/fp6/projects.htm#search

3.4. Acties van de bedrijfswereld

De Commissie verheugt zich erover dat de bedrijfswereld inzake spam een proactieve rol speelt. De dienstenleveranciers hebben doorgaans **technische maatregelen** genomen om spam aan te pakken, waaronder betere spamfilters. De ISP's hebben **help desk-ondersteuning** opgezet en hebben de gebruikers software tegen spam, spyware en malware ter beschikking gesteld. Vele ISP's hebben **contractuele clausules** die wangedrag on-line verbieden. In een recent burgerlijk rechtsgeding in het VK werd een boete van omgerekend 68 800 € wegens contractbreuk opgelegd aan een spammer. Groepen uit de bedrijfswereld hebben beste praktijken aangenomen om phishing on-line te voorkomen en hun filtermethoden te verbeteren[23].

De exploitanten van mobiele netwerken hebben gedragscodes uitgewerkt die actie omvatten tegen ongevraagde berichten. In 2006 heeft de GSMA een gedragscode inzake mobiele spam uitgewerkt. De Commissie cofinanciert momenteel het Spotspam-initiatief, een partnerschap tussen particuliere en overheidsinstanties met het oog op de oprichting van een gegevensbank met grensoverschrijdend onderzoek en grensoverschrijdende handhaving inzake spam[24].

3.5. Handhavingsacties

Het is duidelijk dat de strijd tegen spam resultaten oplevert. Door Finland opgelegde filtermaatregelen hebben het aandeel van spamberichten in het e-mailverkeer teruggebracht van 80% tot ongeveer 30%. Vele autoriteiten hebben inspanningen ondernomen om spammers te stoppen[25].

Wat het aantal vervolgingen betreft, zijn er echter aanzienlijke verschillen tussen de lidstaten. Sommige autoriteiten hebben honderd tot meer onderzoeken gestart waarmee bepaalde spam-activiteiten een halt zijn toegeroepen en zijn bestraft. In andere lidstaten zijn slechts een handvol gevallen onderzocht, soms zelfs geen enkele.

De meeste acties werden toegespitst op **'traditionele' vormen** van spam. **Andere ernstige bedreigingen zijn nauwelijks vervolgd**, ook al houden zij grote risico's in.

4. DE WEG VOORUIT: WAT ER MOET WORDEN GEDAAN

4.1. Actie op lidstaatniveau

In dit hoofdstuk worden de acties van regeringen en nationale autoriteiten besproken, met name op het gebied van handhaving en samenwerking.

4.1.1. Kritieke succesfactoren

Gezien de hardnekkigheid en de evoluerende aard van het probleem is een grotere betrokkenheid van de lidstaten vereist, die bovendien duidelijke prioriteiten moeten stellen.

---

23 http://www.maawg.org/home/

24 http://www.spotspam.net

25 Uit een CNSA-overzicht blijkt dat vijftien van de achttien antwoordende leden in de periode 2003-2006 rechtszaken aanhangig hebben gemaakt.

De acties moeten voornamelijk worden gericht op de 'professionele' spammers, phishers en verspreiders van spyware en malware. De kritieke succesfactoren zijn:

– een sterke vastberadenheid van centrale regeringen om kwalijke praktijken te bestrijden;

– een duidelijke organisationele afbakening van de verantwoordelijkheden voor de handhavingsactiviteiten;

– adequate middelen voor de handhavingsautoriteit.

Momenteel zijn deze factoren niet in alle lidstaten aanwezig.

4.1.2. Coördinatie en integratie op nationaal niveau

Krachtens de richtlijn betreffende de bescherming van de persoonlijke levenssfeer bij elektronische communicatie en de richtlijn betreffende de bescherming van persoonsgegevens[26] hebben de nationale autoriteiten de bevoegdheid op te treden tegen de volgende illegale praktijken:

- de verzending van ongevraagde berichten (**spam)**[27];

- onwettige toegang tot eindapparatuur, hetzij om informatie, zoals **adware-** en **spyware-programma's**, te introduceren, hetzij om toegang te krijgen tot op die eindapparatuur opgeslagen informatie[28];

- het infecteren van eindapparatuur door de introductie van **malware** zoals wormen en virussen en het omvormen van pc's tot **botnets** of voor andere doeleinden[29]**;**

- het misleiden van gebruikers om hen bepaalde gevoelige gegevens, zoals paswoorden en kredietkaartdetails, te ontfutselen[30] via zogenaamde **phishing**-berichten.

Bepaalde van deze praktijken vallen ook onder het strafrecht, met inbegrip van het *kaderbesluit van de Raad over aanvallen op informatiesystemen*[31]. Overeenkomstig dit kaderbesluit moeten de lidstaten voorzien in een maximumgevangenisstraf van ten minste 3 jaar, of zelfs 5 jaar waneer het om georganiseerde criminaliteit gaat.

Op nationaal niveau kan op de naleving van deze bepalingen worden toegezien door administratieve instanties en/of door de strafrechtautoriteiten. Wanneer dit het geval is moeten de respectieve **verantwoordelijkheden** van de verschillende autoriteiten en de samenwerkingsprocedures duidelijk worden afgebakend. Dit kan inhouden dat op hoog regeringsniveau besluiten moeten worden genomen.

Tot dusverre heeft de toenemende verstrengeling van de criminele en administratieve aspecten van spam en andere bedreigingen niet geleid tot hechtere samenwerkings-procedures tussen de lidstaten waarbij de technische en onderzoeksbekwaamheden van

---

26 Richtlijn 95/46/EG.
27 Artikel 13 van de richtlijn betreffende de bescherming van de persoonlijke levenssfeer.
28 Artikel 5, lid 3, van de richtlijn betreffende de bescherming van de persoonlijke levenssfeer.
29 *Supra* 28.
30 Artikel 6, onder a), van de richtlijn betreffende de bescherming van persoonsgegevens.
31 Kaderbesluit 2005/222/JHA van de Raad.

diverse instanties worden samengebracht. Er moeten samenwerkingprotocols worden gesloten met betrekking tot gebieden zoals de uitwisseling van gegevens en informatie, contactdetails, bijstand en de overdracht van rechtszaken.

Een nauwe samenwerking tussen de handhavingsautoriteiten, de netwerkexploitanten en de ISP's op nationaal niveau is nuttig voor de uitwisseling van informatie en technische deskundigheid en de rechtsvervolging van kwaadaardige praktijken. De autoriteiten van Noorwegen en Nederland hebben gerapporteerd over het nut van dergelijke publiekprivate partnerschappen.

4.1.3. Middelen

Er zijn middelen vereist om bewijzen te verzamelen, laakbare praktijken te onderzoeken en rechtszaken in te leiden. De autoriteiten hebben technische en juridische middelen nodig en moeten kennis verwerven over de manier waarop overtreders optreden om hun praktijken daadwerkelijk een halt toe te roepen.

Mechanismen om on-line klacht in te dienen, met de daarmee verbonden systemen om kwalijke praktijken te registreren en te analyseren, kunnen een belangrijk instrument zijn. De ervaring heeft uitgewezen dat **bescheiden investeringen aanzienlijke resultaten** kunnen opleveren. De vermindering van de Nederlandse spamlawine werd bewerkstelligd met behulp van een team van vijf voltijdse werknemers van OPTA **(**Onafhankelijke Post en Telecommunicatie Autoriteit), de relevante Nederlandse instantie, die beschikten over apparatuur ter waarde van **570 000 €** om spam te bestrijden. Voortbouwend op deze investering wordt de bij de bestrijding van spam opgedane ervaring nu gebruikt om andere probleemgebieden aan te pakken.

4.1.4. Grensoverschrijdende samenwerking

Spam is een wereldwijd probleem. Om spammers te vervolgen zullen de bevoegde nationale instanties vaak een beroep moeten doen op de autoriteiten van andere landen; omgekeerd zal hen worden verzocht om in andere landen ingeleid onderzoek af te ronden.

Hoewel er enige terughoudendheid kan bestaan om schaarse nationale middelen te besteden aan onderzoek betreffende problemen van andere landen, is het belangrijk dat de lidstaten inzien dat effectieve grensoverschrijdende samenwerking een onmisbaar onderdeel uitmaakt van de spambestrijding. Recentelijk hebben Oostenrijkse en Nederlandse spambstrijdings-instanties samengewerkt om een einde te maken aan een grote spamoperatie.

Tot dusverre hebben 21 Europese autoriteiten de CNSA-samenwerkingsprocedure[32] betreffende de grensoverschrijdende behandeling van klachten onderschreven; de overige autoriteiten worden uitgenodigd dit in de komende maanden eveneens te doen. De lidstaten en de bevoegde instanties worden met name verzocht actief het gebruik te ondersteunen van:

- de gemeenschappelijke pro forma-documenten van CNSA-LAP;

- de OESO-aanbeveling en -toolkit inzake spambestrijding.

---

32 *Supr*a 18.

4.1.5 Voorgestelde acties

De lidstaten en de bevoegde instanties worden verzocht:

- duidelijk de verantwoordelijkheden van de nationale spambestrijdingsagentschappen af te bakenen;

- een effectieve samenwerking tussen de bevoegde instanties te bewerkstelligen;

- de marktdeelnemers op nationaal niveau bij de zaak te betrekken, voortbouwend op hun deskundigheid en beschikbare informatie;

- voldoende middelen voor de handhaving ter beschikking te stellen;

- zich actief in te zetten in de internationale samenwerking en in te gaan op verzoeken voor grensoverschrijdende bijstand.

4.2. Actie door de bedrijfswereld

Hieronder worden de acties behandeld die door ondernemingen kunnen worden opgezet om het consumentenvertrouwen te vergroten en de verzending van ongewenste e-mails te verminderen.

4.2.1. Levering en installatie van software

Spyware vormt een ernstige bedreiging voor de privacy van gebruikers. Aanbod van software via het internet is een veelgebruikte methode geworden voor de **levering en installatie van spyware** op de eindapparatuur van de gebruikers. Spyware kan ook worden verborgen in software die wordt verspreid via andere media, zoals installatie-cd-roms. Ongewenste spionageprogramma's kunnen voorts worden geïnstalleerd samen met de software die door consumenten wordt aangekocht.

Om te verhinderen dat de computers van de eindgebruikers met spyware worden besmet, zijn de hieronder omschreven specifieke acties vereist.

4.2.2. Voorlichting van de gebruiker

Wanneer nieuwe software wordt aangeboden, kunnen tegelijk aanvullende programma's worden geïnstalleerd. Als deze extra software werkt als spyware die het gedrag van de eindgebruikers bespioneert (bijvoorbeeld voor marketingdoeleinden) houdt dit de verwerking van persoonsgegevens in, wat illegaal is tenzij de gebruiker daarvoor op geïnformeerde wijze toestemming heeft verleend. In vele gevallen wordt die toestemming van de gebruiker niet gevraagd of is de desbetreffende vraag verborgen in de kleine lettertjes van een lange licentieovereenkomst.

Ondernemingen die software aanbieden worden aangemoedigd om duidelijk en opvallend alle voorwaarden van hun aanbod te omschrijven, vooral als hun softwarepakket monitoringssoftware voor de verwerking van persoonsgegevens omvat.

Zelfregulering en het gebruik van een soort kwaliteitslabel ('seal of approval') kunnen een middel zijn om betrouwbare ondernemingen te onderscheiden van ondernemingen die dat niet

zijn. Gedragscodes voor de informatie van de gebruiker over de voorwaarden met betrekking tot de verwerking van persoonsgegevens kunnen ter goedkeuring worden voorgelegd aan de Groep voor de bescherming van persoonsgegevens overeenkomstig artikel 29.

4.2.3 Contractuele voorwaarden in de leveranciersketen

Vaak zijn ondernemingen zich er **niet van bewust** hoe advertenties voor hun producten en diensten technisch gesproken worden afgeleverd aan het publiek. Reguliere software kan verstuurd worden samen met spyware die toegang verleent tot gevoelige gegevens, zoals kredietkaartgegevens, vertrouwelijke documenten, enz.

Ondernemingen die producten verkopen en daarvoor reclame maken, moeten erover waken dat de activiteiten van hun contractuele partners legitiem zijn. Een onderneming moet inzicht hebben in de contractuele keten van de desbetreffende relaties, moet toezien op de naleving van de relevante wetgeving en moet ervoor zorgen dat kwalijke praktijken in het geheel van de keten worden stopgezet zodat onmiddellijk een einde kan worden gemaakt aan enige samenwerking met ondernemingen die zich in dergelijke praktijken specialiseren.

4.2.4. Beveiligingsmaatregelen door de dienstenleveranciers

Uit een ENISA-enquête van 2006[33] **blijkt** dat dienstenleveranciers in het algemeen maatregelen hebben getroffen om spam te bestrijden. In het desbetreffende verslag wordt evenwel gemeld dat bedoelde leveranciers verder kunnen bijdragen aan de algemene veiligheid van het netwerk en wordt aanbevolen een krachtiger filterfunctie in te voeren voor de elektronische post die het netwerk van dienstenleveranciers verlaat (**'egress filtering'**). De Commissie verzoekt de dienstenleveranciers om deze aanbeveling ten uitvoer te leggen.

De Groep voor de bescherming van persoonsgegevens overeenkomstig artikel 29 heeft een advies inzake privacykwesties met betrekking tot de levering van screeningsdiensten voor elektronische post[34] gepubliceerd, waarin aanbevelingen worden gedaan inzake het probleem van de vertrouwelijkheid van e-mailberichten en meer bepaald inzake de bescherming van on-line-communicatie tegen virussen, spam en illegale inhoud.

4.2.5. Voorgestelde acties

De Commissie verzoekt:

- ondernemingen ervoor te zorgen dat de informatie die wordt verstrekt bij de verkoop van softwaretoepassingen in overeenstemming is met de wetgeving betreffende gegevens-bescherming;

- ondernemingen contractueel het illegale gebruik van software in advertenties te verbieden en hen te verplichten te monitoren hoe advertenties de consument bereiken, alsook kwalijke praktijken te vervolgen;

- leveranciers van e-maildiensten een filterbeleid toe te passen dat overeenstemming waarborgt met de aanbeveling en de richtsnoeren inzake 'e-mail filtering'.

33 http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

34 Advies 2/2006, WP 118.

4.3. Actie op Europees niveau

De Commissie zal voortgaan met het probleem van spam, spyware en malware aan de orde te stellen op de internationale fora, op bilaterale vergaderingen en waar mogelijk via overeenkomsten met derde landen en zij zal de samenwerking blijven bevorderen tussen de diverse betrokken partijen, zoals de lidstaten, de bevoegde instanties en de bedrijfswereld. Zij zal ook nieuwe initiatieven nemen op het gebied van wetgeving en onderzoek, bedoeld om een nieuwe impuls te geven aan de strijd tegen kwalijke praktijken die de informatiemaatschappij ondermijnen. De Commissie werkt momenteel aan een de verdere ontwikkeling van een samenhangend beleid voor de strijd tegen computercriminaliteit. Dit beleid zal nader worden omschreven in een mededeling die naar planning begin 2007 zal verschijnen.

4.3.1. Herziening van het regelgevingskader

In haar mededeling betreffende het regelgevingskader voor elektronische communicatie[35] stelt de Commissie voor om de regels op het gebied van de privacy en de veiligheid te versterken. Krachtens haar voorstel zouden de netwerkexploitanten en dienstenleveranciers verplicht worden om:

- de bevoegde instanties van de lidstaten in kennis te stellen van elke bres in de beveiliging die heeft geleid tot een verlies van persoonsgegevens en/of onderbreking van de continuïteit van de dienstverlening;

- hun gebruikers te verwittigen van elke inbreuk op de beveiliging die resulteert in het verlies, de wijziging en de vernietiging van en de toegang tot persoonlijke gegevens van de gebruikers.

De nationale regelgevende instanties zouden de bevoegdheid krijgen om de exploitanten te verplichten een adequaat beveiligingsbeleid in te stellen en er zouden nieuwe regels worden ingevoerd die **specifieke oplossingen** mogelijk maken of die een maatstaf geven voor het **niveau van de straffen** die kunnen worden verwacht bij inbreuken op de beveiliging.

4.3.2. Rol van ENISA

De voorstellen omvatten ook een bepaling betreffende de erkenning van de adviserende rol van ENISA inzake beveiligingskwesties. Andere taken van ENISA worden omschreven in de mededeling van de Commissie betreffende een strategie voor een veilige informatie-maatschappij[36] en zijn onder meer:

- het uitbouwen van een betrouwbaar partnerschap met de lidstaten en de belanghebbenden met het oog op de ontwikkeling van een geschikt **gegevensverzamelingskader** inzake beveiligingsincidenten en het niveau van consumentenvertrouwen.

ENISA zal dit kader nauw coördineren met Eurostat om een input te geven aan de communautaire statistieken betreffende de informatiemaatschappij en het i2010-benchmarkingskader[37];

---

35 http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm

36 *Supra* 1.

37 I2010-Benchmarkingskader van de werkgroep op hoog niveau van 20 april 2006.

- het onderzoeken van **de haalbaarheid van een Europees informatiedelings- en waarschuwingssysteem** om een doeltreffend antwoord te bieden op bestaande en nieuwe bedreigingen voor elektronische netwerken.

4.3.3. Onderzoek en ontwikkeling

Het komende zevende kaderprogramma is onder meer gericht op de verdere ontwikkeling van kennis en technologie inzake de beveiliging van informatiediensten en -systemen, in nauwe samenwerking met beleidsinitiatieven. Wat malware betreft, zal er onder meer gewerkt worden op thema's zoals verborgen botnets en virussen en aanvallen op mobiele en spraaktelefoniediensten.

4.3.4. Internationale samenwerking

Aangezien het internet een wereldwijd netwerk is, moet de verbintenis om spam, spyware en malware te bestrijden wereldwijd gedeeld worden. De Commissie is dan ook van plan om de dialoog en de samenwerking met derde landen inzake de strijd tegen deze bedreigingen en de daarmee verbonden criminele activiteiten te versterken. Daartoe zal de Commissie ernaar streven het probleem van spam, spyware en malware op te nemen in overeenkomsten tussen de EU en derde landen, zal zij de meest betrokken landen met klem verzoeken zich duidelijk te verbinden tot samenwerking met de EU-landen om deze bedreigingen op een meer doeltreffende wijze te bestrijden en zal zij nauw toezien op de handhaving van de gezamenlijk aangegane verbintenissen.

4.3.5. Voorgestelde acties

De Commissie zal:

- haar inspanningen voortzetten om het bewustzijn te verhogen en tot meer samenwerking te komen tussen de diverse betrokken partijen;

- overeenkomsten blijven sluiten met derde landen waarin het aspect van de strijd tegen spam, spyware en malware is opgenomen;

- zich inspannen om tegen begin 2007 nieuwe wetgevingsinitiatieven voor te stellen die tot doel hebben de regels op het gebied van de bescherming van de persoonlijke levenssfeer en de veiligheid in de communicatiesector te versterken en een beleid tegen computercriminaliteit vorm te geven;

- blijven gebruik maken van de ENISA-deskundigheid inzake beveiligingskwesties;

- in haar zevende kaderprogramma relevant onderzoek en ontwikkeling ondersteunen.

5. CONCLUSIE

Bedreigingen zoals spam, spyware en malware ondermijnen het vertrouwen in en de veiligheid van de informatiemaatschappij en hebben een aanzienlijke financiële impact. Hoewel sommige lidstaten daadwerkelijk initiatieven hebben genomen, is er in de EU als geheel **onvoldoende actie om deze ontwikkeling een halt toe te roepen.** De Commissie speelt haar rol als bemiddelaar om een groter bewustzijn te creëren inzake de noodzaak van politieke vastberadenheid om deze bedreigingen te bestrijden.

De handhavingsinspanningen moeten worden opgedreven om personen die doelbewust de wet overtreden tegen te houden. De bedrijfswereld moet meer actie ondernemen ter ondersteuning van de handhavingsinspanning. Op nationaal niveau is er samenwerking nodig zowel binnen de regering als tussen de regering en de bedrijfswereld. De Commissie zal de dialoog en de samenwerking met derde landen versterken en zal ook nagaan of er nieuwe wetgevingsvoorstellen moeten worden ingediend. Zij zal voorts onderzoeksacties opzetten om de bescherming van de persoonlijke levenssfeer en de veiligheid in de sector van de elektronische communicatie te versterken.

Een goed geïntegreerde en waar mogelijk parallelle tenuitvoerlegging van de in deze mededeling genoemde acties kan ertoe bijdragen de bedreigingen te verminderen die momenteel de voordelen van de informatiemaatschappij en de economie aantasten.
De Commissie zal toezien op de tenuitvoerlegging van deze acties en zal in 2008 evalueren of ingrijpender actie nodig is.