KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, 15.11.2006
KOM(2006) 688 endelig

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

om bekæmpelse af spam, spyware og skadeligt software

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

om bekæmpelse af spam, spyware og skadeligt software

(EØS-relevant tekst)

1. MEDDELELSENS FORMÅL

Ingen kan længere være i tvivl om, hvor stor en betydning de moderne elektroniske kommunikationsnetværk og –tjenester har for vores hverdag, både på arbejdspladsen og i hjemmet. For at få alle til at anvende disse tjenester kræves der imidlertid troværdige, sikre og pålidelige teknologier. Kommissionens meddelelse om en strategi for et sikkert informationssamfund[1] har til formål at forbedre net- og informationssikkerheden, og den opfordrer den private sektor til at se nærmere på de svagheder i netværk og informationssystemer, der kan udnyttes til at sprede spam og skadeligt software. I Kommissionens meddelelse om revurderingen af EU's regelsæt for elektroniske kommunikationsnet og tjenester foreslås der nye regler for at øge sikkerheden og beskyttelsen af privatlivets fred inden for elektronisk kommunikation[2].

Nærværende meddelelse handler om udviklingen inden for spam[3] og andre trusler som spyware og skadeligt software. Der gøres rede for de bestræbelser, man indtil videre har gjort sig for at bekæmpe disse trusler, og der foreslås yderligere foranstaltninger, herunder:

- styrkelse af fællesskabslovgivningen

- retshåndhævelse

- samarbejde i og mellem medlemsstater

- politisk og økonomisk dialog med tredjelande

- brancheinitiativer

- forsknings- og udviklingsinitiativer.

---

1 KOM(2006) 251 endelig
2 KOM(2006) 334 endelig.
3 KOM(2004) 28.endelig

2. PROBLEMET – SIKKERHEDSTRUSLERNE ÆNDRER SIG KONSTANT

Spam[4] har bredt sig meget i løbet af de sidste 5 år[5], og ifølge kilder fra branchen udgør spam i dag 50-80 % af de meddelelser, der sendes til slutbrugere[6]. Selv om størstedelen af spam kommer fra lande uden for EU, står de europæiske lande nu for 25 % af de videresendte spammeddelelser[7]. På verdensplan anslås omkostningerne som følge af spam til 39 mia. EUR i 2005, og i de større europæiske økonomier er disse omkostninger blevet vurderet til omkring 3,5 mia. EUR for Tyskland, 1,9 mia. EUR for Det Forenede Kongerige og 1,4 mia. EUR for Frankrig[8]. Spamming betragtes som en "erhvervsaktivitet" som sådan. Spammere udlejer eller sælger lister over indsamlede e-mail-adresser til virksomheder med henblik på marketing. Spam over internettet er særlig indtægtsgivende, fordi dette medie gør det muligt at komme i kontakt med et stort antal personer, og fordi omkostningerne ved fremsendelse af store mængder meddelelser er forholdsvis lave. På den anden side kan en beskeden investering i bekæmpelsen af spam også give betydelige resultater. I Nederlandene har man således nedbragt mængden af spam med 85 % ved at investere **570 000 EUR** i passende udstyr.

Fra blot at være et irriterende fænomen har de uønkede e-mails antaget en mere og mere svigagtig og kriminel karakter. Et godt eksempel er anvendelsen af phishing e-mails, der lokker slutbrugeren til at afgive følsomme oplysninger til "falske" websteder, som giver sig ud for at repræsentere rigtige virksomheder, hvilket medfører identitetsmisbrug og skader virksomhedernes omdømme. Udbredelsen af spyware via e-mail eller gennem software til at spore og registrere en brugers onlineadfærd fortsætter i stadig større omfang. Spyware kan også indsamle personoplysninger som kodeord og kreditkortnumre.

Det er blevet betydeligt nemmere at fremsende store mængder uønsket e-mail på grund af spredningen af skadelige koder som orme og vira. Når de først er installeret, kan hackeren tage kontrol over en inficeret computer og gøre den til en "botnet"[9], der skjuler spammerens egentlige identitet. Botnets udlejes af spammere, phishers og spyware-sælgere til svigagtige og kriminelle formål**.** Eksperter fra branchen vurderer, at "botnets" videreformidler over 50 % af de uønskede e-mails[10]. Spredningen af spyware og andre typer skadelige koder, der angriber forbrugere og virksomheder, har betydelige økonomiske konsekvenser. De samlede finansielle konsekvenser af malware er således blevet vurderet til omkring 11 mia. EUR i 2005[11].

---

4 Spam er uønskede meddelelser, der fremsendes – f.eks. via e-mail – til kommercielle formål. Uønsket e-mail kan imidlertid også indeholde skadelig software og spyware.

5 I 2001 udgjorde spam 7 % af den samlede e-mail-kommunikation.

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

7 1. kvartal 2006 (Sophos) Asien 42,8 %, Nordamerika 25,6 %, Europa 25,0 %, Sydamerika 5,1 %, Australasien 0,8 %, Afrika 0,6 %, andre 0,1 %.

8 Ferris research, 2005.

9 "Botnets" er inficerede computere, som anvendes af spammere til masseforsendelse af e-mail ved at installere skjult software, der gør computerne til postservere uden brugerens viden.

10 De lande, der er mest inficerede med botnets, er ifølge Symantec (3.-4. kvartal 2005): USA 26 %, Det Forenede Kongerige 22 %, Kina 9 %, Frankrig, Sydkorea og Canada 4 %, Taiwan, Spanien og Tyskland 3 %, Japan 2 %.

11 Computer Economics: the 2005 Malware Report.

3. HIDTIDIG INDSATS—FORANSTALTNINGER SIDEN 2004

EU vedtog i 2002 et **direktiv om databeskyttelse inden for elektronisk kommunikation, der forbyder spam**[12] ved at indføre princippet om samtykke-baseret markedsføring til fysiske personer. I januar 2004 fremlagde Kommissionen en meddelelse om spam med en række foranstaltninger, der supplerer direktivet[13]. Det understreges i meddelelsen, at en række forskellige aktører bør træffe foranstaltninger med henblik på bedre information, anvendelsen af selvregulering og tekniske løsninger, samarbejde og retshåndhævelse. Kommissionen er begyndt at inddrage bekæmpelsen af spam, spyware og malware i sin dialog med tredjelande. Herudover beskytter direktivet om urimelig handelspraksis[14] forbrugerne mod aggressiv handelspraksis. Det grænseoverskridende samarbejde til bekæmpelse af en sådan praksis er omfattet af forordningen om forbrugerbeskyttelsessamarbejde[15].

3.1. Information

Kommissionens meddelelse har bidraget til at øge opmærksomheden om problematikken omkring spam på nationalt og internationalt niveau over hele verden. På EU-niveau fremmer **Safer Internet *plus*-programmet** en mere sikker anvendelse af internet og de nye onlineteknologier, særlig for børn, som en del af EU's samlede indsats på området.

Medlemsstaterne har iværksat eller givet deres støtte til **kampagner**, der har til formål at gøre brugerne mere opmærksomme på problematikken og eventuelle løsninger. Internettjenesteudbyderne har generelt sørget for at rådgive og hjælpe deres kunder med at beskytte sig selv mod spyware og vira. Kommissionen var vært for en OECD-**workshop** om spam i februar 2004. Kommissionen bidrog ligeledes aktivt til udarbejdelsen af OECD's **Anti-Spam Toolkit**, som er en omfattende pakke af forskriftsmetoder, tekniske løsninger og brancheinitiativer til bekæmpelse af spam.

Det blev på FN's verdenstopmøde om informationssamfundet (WSIS) [16] **konstateret**, at spam skal bekæmpes på passende nationalt og internationalt niveau. Den Internationale Telekommunikationsunion (ITU) afholdt i 2004 og 2005 en række tematiske konferencer i forbindelse med verdenstopmødet. I Tunis-agendaen, der blev vedtaget på verdenstopmødet i november 2005, opfordres der til, at man griber effektivt ind over for det betydelige og voksende spamproblem[17].

3.2. Internationalt samarbejde

Spam er et grænseoverskridende problem, hvorfor der er iværksat en række samarbejdsinitiativer og mekanismer til grænseoverskridende retshåndhævelse. Kommissionen har etableret et kontaktnetværk for myndigheder med ansvar for spam (**Contact Network of Spam Authorities** - CNSA), der mødes på regelmæssig basis, udveksler eksempler på god praksis og samarbejder om retshåndhævelse på tværs af

---

12 Artikel 13 i direktiv 2002/58.
13 Se fodnote 3.
14 Punkt 26 i bilag 1 til direktiv 2005/29/EF.
15 Forordning (EF) nr. 2006/2004.
16 WSIS, Geneve, december 2003.
17 Tunis-agendaen, punkt 41.

grænserne. CNSA har udarbejdet en samarbejdsprocedure[18] for at fremme den grænseoverskridende behandling af spamklager. Kommissionens tjenestegrene støtter og deltager som observatører i **London Action Plan** (LAP), der er et forum af retshåndhævelsesmyndigheder fra 20 lande, og den har ligeledes vedtaget en procedure for samarbejde på tværs af grænserne. Der blev afholdt en fælles EU-CNSA-LAP-workshop i november 2005. **OECD** vedtog en henstillling om grænseoverskridende samarbejde med henblik på håndhævelse af lovgivningen om spam (Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam) i april 2006, hvor retshåndhævelsesmyndighederne opfordres til at udveksle information og arbejde sammen[19].

Kommissionen støtter endvidere en række **internationale samarbejdsinitiativer**. USA og EU er blevet enige om at samarbejde med henblik på at bekæmpe spam gennem fælles retshåndhævelsesinitiativer og finde løsninger til bekæmpelse af ulovligt spyware og malware. Kommissionen deltager desuden i arbejdsgruppen om spam inden for rammerne af Canadian International Collaboration. Der afholdes drøftelser med en række store internationale partnere, herunder Kina og Japan. Hvad angår Asien tog Kommissionen initiativ til en fælles erklæring om internationalt antispamsamarbejde (Joint Statement on International Anti-spam Cooperation), der blev vedtaget på ASEM-konferencen om e-handel i februar 2005[20].

Det understreges i Tunis-agendaen, som verdenstopmødet vedtog i november 2005, at internetsikkerhed er et område, hvor der er behov for et bedre internationalt samarbejde, og at dette problem skal behandles inden for rammerne af modellen for udvidet samarbejde vedrørende internetforvaltning, som skal gennemføres som opfølgning på topmødet[21].

3.3. Forskning og teknologisk udvikling

Kommissionen har under det 6. rammeprogram for forskning og teknologisk udvikling iværksat en række projekter for at hjælpe de berørte parter med at bekæmpe spam og andre former for malware. Disse projekter[22] spænder lige fra generel overvågning af netværk og sporing af angreb til specifik teknologisk udvikling og fremstilling af filtre til sporing af spam, phishing og malware. Af resultater kan nævnes etableringen af et forskningsfællesskab med fokus på bekæmpelse af malware og udviklingen af en europæisk infrastruktur til overvågning af internettrafikken. De seneste aktiviteter vedrører justerbare phishingfiltre, der kan spore ukendte trusler og internetangreb. De finansielle midler, der er afsat til disse aktiviteter, beløber sig til 13,5 mio. EUR.

3.4. Brancheinitiativer

Kommissionen konstaterer med tilfredshed, at branchen har indtaget en proaktiv rolle i bekæmpelsen af spam. De forskellige tjenesteudbydere har som regel truffet **tekniske foranstaltninger** til at bekæmpe spam, herunder bedre spamfiltre. Internettjenesteudbyderne har etableret **helpdesk-support** og forsyner brugerne med software til bekæmpelse af spam,

---

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-agendaens punkt 39-47. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

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

spyware og malware. Mange internettjenesteudbydere anvender **aftalebestemmelser**, der forbyder uredelig onlinepraksis. I en nyere dom i et civilt søgsmål i Det Forende Kongerige blev en spammer idømt en bøde på 68 800 EUR for aftalebrud. Brancheorganisationer har vedtaget regler om god praksis med henblik på at forebygge onlinephishing og forbedre filtreringsmetoderne[23].

Mobiloperatørerne har udarbejdet adfærdskodekser for branchen, der foreskriver foranstaltninger til bekæmpelse af uønskede meddelelser. Sammenslutningen GSM har i 2006 offentliggjort en adfærdskodeks vedrørende mobilspam. Kommissionen samfinansierer løbende Spotspam-initiativet, som er et partnerskab mellem private og offentlige organer, der har til formål at udvikle en database til fremme af grænseoverskridende efterforskning og retsforfølgelse af spamsager[24].

3.5. Retshåndhævelse

Bekæmpelsen af spam giver åbenlyse resultater. I Finland, hvor der er blevet indført obligatoriske filterforanstaltninger, er andelen af spam i de fremsendte e-mails blevet reduceret fra 80 % til omkring 30 %. En lang række myndigheder har iværksat retshåndhævelsesforanstaltninger for at sætte en stopper for spammere[25].

Der er imidlertid betydelige forskelle mellem medlemsstaterne med hensyn til antallet af sager, hvor der sker retsforfølgelse. Visse myndigheder har iværksat over hundrede undersøgelser, hvor de pågældende spamaktiviteter effektivt er blevet standset og straffet. I andre medlemsstater har man ikke foretaget retsforfølgelse i mere end en håndfuld sager, og i nogle lande slet ikke.

De fleste sager har drejet sig om de **traditionelle former** for spam, mens **andre former for trusler næsten ikke er blevet retsforfulgt**, selv om de skaber betydelige problemer.

4. VEJEN FREM: ARBEJDSOPGAVER

4.1. Foranstaltninger på medlemsstatsniveau

Dette afsnit omfatter foranstaltninger, der er rettet mod regeringer og nationale myndigheder, særlig med hensyn til retshåndhævelse og samarbejde.

4.1.1. Succeskriterier

Fordi problemet er af vedvarende karakter og konstant under udvikling, bør medlemsstaterne i højere grad inddrages og give dette problem større prioritet. Foranstaltningerne bør især tage sigte på "professionelle" spammere, phishere samt spredningen af spyware og malware. Succeskriterierne er:

– at de offentlige myndigheder forpligter sig til at bekæmpe enhver uredelig onlinepraksis

– at ansvaret for retshåndhævelse er organisatorisk klart defineret

---

[23] http://www.asemec-london.org/

[24] http://www.spotspam.net

[25] Det fremgår af en CNSA-undersøgelse, at der hos 15 ud af 18 responderende medlemmer skete retsforfølgelse i perioden 2003-2006.

– at retshåndhævelsesmyndighederne råder over passende ressourcer.

Disse kriterier er i øjeblikket ikke opfyldt i alle medlemsstater.

4.1.2. Koordination og integration på nationalt plan

De nationale myndigheder har i henhold til direktivet om e-kommunikation og databeskyttelsesdirektivet[26] myndighed til at gribe ind over for følgende ulovlig praksis:

- fremsendelse af uønskede henvendelser (**spam**)[27]

- ulovlig adgang til terminaludstyr enten med henblik på at lagre information – herunder **adware-** og **spyware-**programmer - eller få adgang til information, der er lagret i dette udstyr[28]

- inficering af terminaludstyr ved at anbringe **malware** i form af orme og vira og omdanne computere til **botnets** eller til brug for andre formål[29]

- misinformering af brugerne for at få dem til at afgive følsomme oplysninger[30], f.eks. kodeord og kreditkortoplysninger, ved hjælp af såkaldte **phishingmeddelelser**.

En række af disse praksisser er ligeledes omfattet af straffeloven, herunder *rammeafgørelsen om angreb på informationssystemer*[31]. Medlemsstaterne skal i henhold til denne rammeafgørelse træffe de nødvendige foranstaltninger for at sikre, at de strafbare handlinger kan straffes med fængsel af en maksimal varighed på mindst to til fem år, når de er begået inden for rammerne af en kriminel organisation.

På nationalt plan kan disse bestemmelser gennemføres af administrative organer og/eller strafferetlige myndigheder. Når dette er tilfældet, skal de forskellige myndigheders **ansvar** og procedurerne for samarbejde klart defineres. Dette forudsætter beslutninger på højeste niveau hos de nationale myndigheder.

De strafferetlige og forvaltningsmæssige aspekter af spam og andre trusler er i stadig højere grad tæt forbundet, men medlemsstaterne har endnu ikke i samme grad udviklet passende samarbejdsprocedurer, der forener de forskellige myndigheders tekniske og efterforskningsmæssige kompetencer. Der er behov for samarbejdsprotokoller for at dække områder som f.eks. udveksling af information og efterretninger, kontaktoplysninger, bistand og overdragelse af sager.

Et tæt samarbejde mellem retshåndhævelsesmyndigheder, netværksoperatører og internettjenesteudbydere på nationalt plan vil ligeledes fremme udvekslingen af information, teknisk ekspertise og efterforskningen af uredelig onlinepraksis. Myndigheder fra Norge og Nederlandene har således rapporteret om de gavnlige virkninger af sådanne partnerskaber mellem den private og den offentlige sektor.

---

26 Direktiv 95/46/EF.
27 Artikel 13 i direktivet om e-kommunikation.
28 Artikel 5, stk. 3, i direktivet om e-kommunikation.
29 Jf. fodnote 28.
30 Artikel 6, litra a), i databeskyttelsesdirektivet.
31 Rådets rammeafgørelse 2005/222/RIA.

4.1.3. Ressourcer

Det kræver ressourcer at samle beviser, efterforske og rejse tiltale. Myndighederne har behov for tekniske og retlige ressourcer, og de skal hele tiden holde sig ajour med, hvorledes lovovertrædere opererer for at gennemføre deres aktiviteter.

Onlineklagemekanismer med tilknyttede systemer til registrering og analyse af uredelig praksis kan være meget nyttige værktøjer. Erfaringen har vist, at selv en **beskeden investering** kan give **betydelige resultater**. Nedbringelsen af spam i Nederlandene blev opnået ved at etablere en gruppe på 5 fuldtidsansatte i den nederlandske databeskyttelsesmyndighed OPTA med udstyr til en værdi af **570 000 EUR** til at bekæmpe spam. Det har med udgangspunkt i denne investering været muligt at opbygge en erfaring, der nu anvendes inden for problemområder.

4.1.4. Grænseoverskridende samarbejde

Spam er et globalt problem. De nationale myndigheder vil således ofte behøve hjælp fra myndigheder i andre lande til at retsforfølge spammere, og de vil omvendt blive anmodet om at efterforske sager, der er indledt i andre lande.

Der kan være en vis tilbageholdenhed med hensyn til afsætte de i forvejen sparsomme nationale ressourcer til at efterforske andres problemer, men det er vigtigt for medlemsstaterne at anerkende, at et effektivt grænseoverskridende samarbejde er et vigtigt element i bekæmpelsen af spam. De australske og nederlandske myndigheder med ansvar for spambekæmpelse har for nylig samarbejdet for at bringe en omfattende spamoperation til ophør.

21 europæiske myndigheder har indtil videre anerkendt CNSA's samarbejdsprocedure[32] for grænseoverskridende klagebehandling. De resterende myndigheder opfordres til at gøre det samme inden for de næste måneder. Medlemsstaterne og de kompetente myndigheder opfordres især til at gøre en aktiv indsats for at fremme anvendelsen af:

- de fælles CNSA-LAP standarddokumenter

- OECD's henstilling og "Toolkit on spam enforcement".

[32] Jf. fodnote 18.

4.1.5 Forslag til foranstaltninger

Medlemsstaterne og de kompetente myndigheder opfordres til: - klart at definere ansvarsområderne for de nationale organer, der arbejder med bekæmpelse af spam - at sikre et effektivt samarbejde mellem de kompetente myndigheder - at inddrage markedsdeltagere på nationalt plan og drage fordel af deres ekspertise og oplysninger - at sikre passende ressourcer til retshåndhævelse - at tilslutte sig internationale samarbejdsprocedurer og imødekomme anmodninger om grænseoverskridende bistand.

4.2. Foranstaltninger på brancheniveau

I dette afsnit beskrives de aktiviteter, som branchen kan iværksætte for at fremme forbrugernes tillid og begrænse fremsendelsen af uønskede e-mails.

4.2.1. Levering og installation af software

Spyware udgør en alvorlig trussel for brugernes privatliv. Tilbud om onlinelevering af software er blevet en meget anvendt metode til at **levere og installere spyware** på brugernes terminaludstyr. Spyware kan ligeledes være skjult i software, der distribueres gennem andre medier, f.eks. cd-rommer, der installeres på en computer. Uønskede spionprogrammer installeres ofte sammen med det software, som brugeren køber.

I det efterfølgende beskrives en række specifikke aktiviteter til at forhindre, at spyware når frem til slutbrugerne.

4.2.2. Forbrugeroplysning

Der skal ved køb af nyt software ofte installeres supplerende programmer. Når dette supplerende software fungerer som spyware ved at overvåge slutbrugerens adfærd (f.eks. til marketingformål), indebærer det behandling af personoplysninger, hvilket er ulovligt uden brugerens informerede samtykke. Ofte indhentes brugerens tilladelse til at installere dette software slet ikke, eller de relevante oplysninger står med småt i en lang licensaftale.

Virksomheder, der sælger softwareprodukter, opfordres til klart og tydeligt at beskrive alle vilkår og betingelser, særlig hvis softwarepakkerne indeholder overvågningsudstyr, som behandler personoplysninger.

Det vil være muligt ved hjælp af selvregulering og anvendelsen af en slags kvalitetsstempel at adskille troværdige fra ikke-troværdige virksomheder. Adfærdskodekser, der har til formål at informere brugeren om behandlingen af personoplysninger, kan forelægges Artikel 29-Gruppen vedrørende Databeskyttelse med henblik på godkendelse.

4.2.3. Aftalebestemmelser i leveringskæden

Ofte er virksomhederne **ikke klar over**, hvorledes reklamer for deres produkter og tjenester rent teknisk distribueres til forbrugerne. Lovligt software kan således være tilført spyware, som anvendes til at få adgang til følsomme oplysninger, herunder kreditkortoplysninger, fortrolige dokumenter osv.

Virksomheder, der reklamerer og/eller sælger produkter, skal sikre, at deres samarbejdspartneres aktiviteter er lovlige. Det er nødvendigt, at virksomhederne danner sig et overblik over de forskellige produktions- og distributionsled, kontrollerer lovligheden af de enkelte aktiviteter og sikrer, at enhver uredelig praksis fører til kontraktopsigelse, således at det videre samarbejde med virksomheder, der er skyldige i uredelig praksis, kan afbrydes øjeblikkeligt.

4.2.4. Sikkerhedsforanstaltninger iværksat af tjenesteudbyderne

Det bekræftes i en ENISA-undersøgelse fra 2006[33], at tjenesteudbyderne generelt har truffet foranstaltninger til at bekæmpe spam. Det konstateres imidlertid også, at tjenesteudbyderne kunne bidrage yderligere til netværkets generelle sikkerhed, og det anbefales at sætte større fokus på filtreringen af e-mails, der forlader en tjenesteudbyders netværk (**egress-filtrering)**. Kommissionen opfordrer tjenesteudbyderne til at følge denne anbefaling.

Artikel 29-Gruppen vedrørende Databeskyttelse har vedtaget en udtalelse om beskyttelse af privatlivets fred i relation til tilrådighedsstillelse af e-mail-screeningtjenester[34], der indeholder retningslinjer for kommunikationshemmelighed i forbindelse med e-mail-korrespondance og mere specifikt om filtrering af onlinekommunikation imod vira, spam og ulovligt indhold.

4.2.5. Forslag til foranstaltninger

Kommissionen opfordrer:

- virksomhederne til at sikre, at kvaliteten af de oplysninger, der gives ved køb af software-applikationer, er i overensstemmelse med databeskyttelseslovgivningen

- virksomhederne til i deres aftalebestemmelser at forbyde ulovlig anvendelse af software i reklamer, kontrollere, hvorledes reklamerne når frem til forbrugerne, og følge op på tilfælde af uredelig praksis

- e-mail-tjenesteudbydere til at anvende en filtreringspolitik, der sikrer overensstemmelse med anbefalingen og retningslinjerne vedrørende e-mail-filtrering.

4.3. Foranstaltninger på europæisk niveau

Kommissionen vil fortsat gøre en aktiv indsats vedrørende de forskellige aspekter af spam, spyware og malware i internationale fora, på bilaterale møder og i givet fald gennem aftaler med tredjelande, og den vil fortsat fremme samarbejdet mellem berørte parter, herunder

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

[34] Udtalelse nr. 2/2006, WP 118.

medlemsstaterne, de kompetente myndigheder og branchen. Den vil ligeledes træffe nye initiativer på lovgivnings- og forskningsområdet for at give nye impulser til bekæmpelsen af uredelig praksis, der underminerer informationssamfundet. Kommissionen arbejder i øjeblikket med at videreudvikle en sammenhængende politik for bekæmpelse af internetkriminalitet. Denne politik vil blive fremlagt i en meddelelse, som skal vedtages primo 2007.

4.3.1. Gennemgang af det nuværende regelsæt

I Kommissionens meddelelse[35] om rammebestemmelserne for elektronisk kommunikation foreslås det at skærpe reglerne vedrørende sikkerhed og beskyttelse af privatlivets fred. Netoperatører og tjenesteudbydere vil i henhold til dette forslag være forpligtet til:

- at underrette den kompetente myndighed i den pågældende medlemsstat om ethvert brud på sikkerhedsbestemmelserne, der fører til tab af personoplysninger og/eller afbrydelser i leverancen af serviceydelser

- at underrette deres kunder om ethvert brud på sikkerhedsbestemmelserne, der fører til tab, ændring, adgang eller destruktion af personlige kundeoplysninger.

De nationale forvaltningsmyndigheder skal have mulighed for at pålægge operatørerne at implementere passende sikkerhedspolitikker, og der skal kunne fastsættes nye regler om **specifikke retsmidler** eller en **strafferamme** for overtrædelser.

4.3.2. ENISA's rolle

Forslagene indeholder også en bestemmelse, hvormed ENISA gives en rådgivende rolle i sikkerhedsanliggender. De øvrige opgaver, som ENISA skal varetage, er beskrevet i Kommissionens meddelelse om en sikkerhedsstrategi[36] og omfatter:

- etableringen af et tillidsbaseret partnerskab med medlemsstaterne og de berørte parter med henblik på at udforme en passende **ramme for dataindsamling** om sikkerhedshændelser og forbrugertillid. ENISA vil nøje koordinere denne rammestruktur med Eurostat med henblik på udarbejdelse af fællesskabsstatistik om informationssamfundet og i2010-benchmarkingrammerne[37]

- **undersøgelse af muligheden** for at oprette et **europæisk informationsudvekslings- og varslingssystem**, der skal gøre det lettere at reagere effektivt på eksisterende og kommende trusler mod elektroniske net.

4.3.3. Forskning og udvikling

Det kommende 7. rammeprogram tager sigte på den løbende udvikling af viden og teknologi til sikring af informationstjenester og –systemer i tæt koordination med de politiske initiativer. De emner, der forventes at blive behandlet i forbindelse med malware, er skjulte botnets og vira samt angreb på mobil- og taletelefoni.

---

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

36 Jf. fodnote 1.

37 Benchmarkingramme af 20. april 2006 fra Gruppen på Højt Niveau om i2010.

4.3.4. Internationalt samarbejde

Internet er et globalt netværk, og det er derfor nødvendigt, at man på verdensplan forpligter sig til at bekæmpe spam, spyware og malware. Kommissionen agter derfor at styrke dialogen og samarbejdet med tredjelande om bekæmpelse af disse trusler og hertil knyttede kriminelle aktiviteter. Kommissionen agter til dette formål at sikre, at der i aftaler mellem EU og tredjelande tages højde for problematikken omkring spam, spyware og malware; den agter at få de mest berørte tredjelande til at forpligte sig til at samarbejde med EU-medlemsstaterne for at bekæmpe disse trusler så effektivt som muligt; og den agter at følge op på gennemførelsen af fælles målsætninger.

4.3.5. Forslag til foranstaltninger

Kommissionen agter:
- fortsat at gøre en aktiv indsats for at informere og gøre opmærksom på problemet samt fremme samarbejdet mellem de berørte parter
- fortsat at indgå aftaler med tredjelande, der tager højde for problematikken omkring bekæmpelse af spam, spyware og malware
- at indføre nye lovgivningsforslag primo 2007, der skærper reglerne vedrørende sikkerhed og beskyttelse af privatlivets fred inden kommunikationssektoren, samt fremlægge en politik vedrørende internetkriminalitet
- at drage fordel af ENISA's ekspertise i sikkerhedsanliggender
- at støtte forskning og udvikling inden for rammerne af sit 7. rammeprogram.

5. KONKLUSION

Trusler såsom spam, spyware og malware underminerer tilliden til og sikkerheden i informationssamfundet, og de har betydelige finansielle konsekvenser. Selv om visse medlemsstater allerede har truffet en række initiativer, bliver der i EU som helhed **ikke gjort en tilstrækkelig indsats for at løse dette problem.** Kommissionen udnytter sin rolle som mellemled til at gøre mere opmærksom på behovet for, at man på politisk plan i højere grad forpligter sig til at bekæmpe disse trusler.

Indsatsen inden for retshåndhævelse skal intensiveres for at stoppe de personer, der bevidst overtræder loven. Branchen skal træffe yderligere foranstaltninger for at supplere indsatsen inden for retshåndhævelse. Der er behov for samarbejde på nationalt plan, både mellem nationale myndigheder og mellem den offentlige og den private sektor. Kommissionen vil styrke dialogen og samarbejdet med tredjelande samt undersøge muligheden for at fremsætte nye lovgivningsforslag, og den vil iværksætte forskningsaktiviteter med henblik på yderligere at styrke beskyttelsen af privatlivets fred og sikkerheden inden for elektronisk kommunikation.

Hvis de aktionslinjer, der er beskrevet i denne meddelelse, gennemføres sideløbende og i indbyrdes sammenhæng, kan det medvirke til at nedbringe omfanget af de trusler, der ødelægger vores økonomier og spolerer fordelene ved informationssamfundet. Kommissionen

agter at overvåge implementeringen af disse aktionslinjer og i 2008 at foretage en vurdering af, hvorvidt en yderligere indsats er påkrævet.