Regeringskansliet
Faktapromemoria 2006/07:FPM26

Meddelande om skräppost, spionprogram och sabotageprogram

Näringsdepartementet

2007-01-11

Dokumentbeteckning

KOM(2006) 688 slutlig
MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN om skräppost, spionprogram och sabotageprogram

Sammanfattning

Kommissionen skriver i sitt meddelande att skräppost, spion- och sabotageprogram och liknande hot undergräver förtroendet för informationssamhället och leder till minskad säkerhet och stora kostnader. Vissa medlemsstater har tagit initiativ i frågan, men i EU som helhet är insatserna för att ta itu med denna utveckling bristfälliga enligt kommissionen. Kommissionen vill utnyttja sin roll för att skapa större medvetenhet om behovet av ett ökat politiskt engagemang i kampen mot dessa hot.

Tillsynsinsatserna måste enligt kommissionen intensifieras för att stoppa de som medvetet bryter mot lagen. Näringslivet måste göra mer för att komplettera tillsynsinsatserna. Det behövs samarbete på nationell nivå, både inom förvaltningen och mellan förvaltning och näringsliv. Kommissionen vill förstärka dialogen och samarbetet med länder utanför EU och undersöka möjligheterna att lägga fram nya lagförslag. Den kommer också att främja forskning som leder till skydd för personuppgifter och höjd säkerheten i sektorn för elektronisk kommunikation.

Ett samordnat och i möjligaste mån samtidigt genomförande av de åtgärder som presenteras i detta meddelande skulle, enligt kommissionen, kunna bidra till att minska de faror som i dag hotar informationssamhällets och vår ekonomiska säkerhet. Kommissionen skriver att man kommer att övervaka genomförandet av dessa åtgärder och senast 2008 bedöma om det krävs ytterligare insatser.

Regeringen ser positivt på att stärka informationssäkerheten för myndigheter, företag och enskilda inom EU. Meddelandet är bra som en signal för fortsatt arbete. Regeringen noterar dock att inga konkreta förslag presenteras. Kommissionen hänvisar till en kommande strategi om nätbrottslighet. Vidare skall frågorna hanteras genom förslag i översynen av regelverket för elektroniska kommunikationer. Regeringen har varit kritisk till de förslag som kommissionen hittills har presenterat om säkerhet liksom förslag till arbetsuppgifter för Europeiska byrån för nät- och informationssäkerhet (Enisa).

1 Förslaget

1.1 Innehåll

1.1.1 Problemet

Kommission redogör för problemet med och kostnader för skräpposten (oönskade e-post med t.ex. reklam som även kan innehålla sabotage- och spionprogam). Problemet har tilltagit avsevärt under de senaste fem åren. Enligt uppgifter är mellan 50 och 80 procent av e-posten skräppost. Kommissionen menar att skräppost är en lönsam verksamhet. Den har stor räckvidd till låga kostnader. Europeiska länder svarar för 25 procent av vidarebefordrade skräppostmeddelanden. Kommissionen anser att det går att göra något åt problemet, t.ex. så har man i Nederländerna minskat skräpposten med 85 procent med en insats om ca 5 miljoner kr i utrustning.

Oönskad e-post har övergått till att var ett redskap för brottslighet. Massutskick underlättas genom spridningen av sabotageprogram som används för att skapa nät av kapade datorer (s.k. botnets). Dessa används av skräppostspridare och av spionprogram för bedrägeri och brottsliga ändamål.

1.1.2 Åtgärder sedan 2004

Inom EU antog man 2002 ett direktiv om integritet och elektronisk kommunikation där användningen av elektronisk post för direkt marknadsföring utan föregående samtycke från abonnenten förbjöds.[1] I januari 2004 presenterade kommissionen ett meddelande om skräppost i vilket åtgärder fastställs för att komplettera direktivet.[2] I meddelandet betonades behovet av åtgärder när det gäller ökad medvetenhet, självreglering, tekniska lösningar, samarbete och kontroll av lagens efterlevnad. Genom direktivet reglerades även att användningen av elektroniska kommunikationsnät, för att lagra information eller för att få tillgång till information som är lagrad i en abonnents eller användares terminalutrustning, endast är tillåten på villkor att abonnenten eller använda-

[1] Artikel 13 i direktiv 2002/58/EG.

[2] KOM(2004) 28 slutlig.

ren i fråga har tillgång till klar och fullständig information. Det kan gälla om ändamålen med behandlingen och rätten att vägra sådan behandling.[3]

Kommissionen tar i meddelandet upp *åtgärder för ökad medvetenhet* och menar att kommissionens tidigare meddelanden och andra EU-program har bidragit till ökad medvetenhet om skräppost i hela världen. Medlemsstaterna har genomfört kampanjer för att göra användarna medvetna om problemen. Kommissionen anser att det är vanligt att Internetleverantörerna själva ger sina kunder råd rörande problemen. Kommissionen har vidare arbetat med frågan i internationella organisationer som OECD och FN.

I det *internationella samarbetet* har kommissionen bl.a. inrättat ett kontaktnät för myndigheter med ansvar inom området (Contact Network of Spam Authorities, CNSA). Kommissionen deltar som observatör i London Action Plan (LAP), som samlar myndigheter från 20 länder. Kommissionen har också samarbeten med USA, Kanada, Kina och Japan.

Inom sjätte ramprogrammet för *forskning och teknisk utveckling* har kommissionen inlett projekt som handlar om att bekämpa skräppost och sabotageprogram (budgeten är ca 124 miljoner kronor).

Om *näringslivets åtgärder* skriver kommissionen att tjänsteleverantörerna i allmänhet vidtagit åtgärder, bl.a. uppförandekoder, bättre skräppostfilter, hjälpcentraler och särskilda kontraktsvillkor.

Kommissionen tar också upp *kontroll av efterlevnaden* av regler på området och menar att insatserna mot skräpposten ger resultat. Filtreringsinsatser i Finland ledde till att andelen skräppost bland e-breven minskade från 80 procent till cirka 30 procent. Många länder har vidtagit rättsliga åtgärder, men det finns stora skillnader mellan medlemsstaterna.

1.1.3 Framtida utveckling: vad återstår att göra?

Insatser på medlemsstatsnivå

Åtgärder bör i första hand inriktas på professionella skräppostspridare, s.k. nätfiskare (eng. phishers) och spridningen av spion- och sabotageprogram. *Viktiga förutsättningar för framgång* är *engagemang* för att bekämpa nätbaserad brottslighet, en klar *ansvarsfördelning* för tillsynsverksamheten och *tillräckliga resurser* för tillsynsmyndigheter.

Enligt kommissionen behövs *samordning och integration på nationell nivå*. Enligt direktivet[4] om integritet och elektronisk kommunikation och direktivet[5] om skydd för enskilda personer med avseende på behandling av

[3] Artikel 5.3 i direktiv 2002/58/EG.

[4] Direktiv 2002/58/EG.

[5] Direktiv 95/46/EG.

personuppgifter och om det fria flödet av sådana uppgifter har nationella myndigheter befogenhet att agera mot flera typer av olaglig verksamhet. Vissa av dessa olagliga verksamheter omfattas även av rådets rambeslut om angrepp mot informationssystem.[6] Ett nära samarbete mellan tillsynsmyndigheter, nätoperatörer och Internetleverantörer främjar, enligt kommissionen, även utbytet av information och tekniskt kunnande, samt bekämpandet av nätbrottslighet.

Kommissionen påpekar att det krävs *resurser* för att samla bevis, följa upp undersökningar och inleda domstolsmål. Även begränsade investeringar kan få betydande resultat.

Kommissionen menar att det *gränsöverskridande samarbetet* försvåras av att det kan vara svårt att förklara varför nationella resurser används på undersökningar av andra länders problem. Kommissionen understryker att ett effektivt gränsöverskridande samarbete är av avgörande betydelse.

Hittills har 21 europeiska myndigheter, inklusive Konsumentverket i Sverige, godkänt CNSA:s samarbetsförfarande för hantering av klagomål över gränserna.

Medlemsstaterna uppmanas av kommissionen att

- fastställa klara ansvarsområden för nationella organ som sysslar med skräppostbekämpning
- se till att behöriga myndigheter samordnas effektivt
- låta marknadens berörda parter på nationell nivå bidra med synpunkter, utnyttja deras sakkunskap och all övrig tillgänglig information
- se till att tillräckliga resurser frigörs för tillsynsverksamheten
- ansluta sig till internationella samarbetsförfaranden och efterkomma begäran om hjälp över gränserna.

Näringslivets insatser

Programerbjudanden på nätet har enligt kommissionen blivit en mycket vanlig metod för *leverans och installation* av spionprogram. Oönskade spionprogram installeras tillsammans med de program som konsumenten valt. För att undvika att spionprogram når slutanvändarna krävs särskilda insatser, som behandlas nedan.

Information till konsumenterna – särskilt om hantering av personuppgifter och om det finns övervakningsfunktioner i programmen. Självreglering, uppförandekoder m.m. skulle också kunna bidra.

Avtalsklausuler i leveranskedjan – kommissionen anser att företagen inte alltid känner till hur reklamen för deras produkter och tjänster tekniskt leve-

[6] Rådets rambeslut 2005/222/RIF.

reras till allmänheten. Företagen måste ha en överblick över avtalskedjan och se till att lagstiftningen följs.

Tjänsteleverantörernas säkerhetsinsatser – en undersökning som gjordes av Enisa under 2006[7] bekräftar att tjänsteleverantörer i allmänhet har vidtagit åtgärder för att bekämpa skräppost. De skulle, enligt kommissionen, kunna bidra ännu mer till den allmänna nätsäkerheten. Kommissionen uppmuntrar tjänsteleverantörerna till kraftigare insatser för att filtrera e-post enligt rekommendationen i rapporten.

Arbetsgruppen för uppgiftsskydd, den s.k. Artikel 29-gruppen, har antagit en ståndpunkt[8] om kontroll av e-post och skyddet av privatlivet som skall ge vägledning om filtrering av kommunikation för att avlägsna t.ex. datavirus och skräppost.

Kommissionen uppmuntrar

- företag att se till att informationen vid köp av program uppfyller kraven i fråga om skydd av personuppgifter
- företag att i avtal förbjuda olaglig användning av program i t.ex. nätannonser, övervaka hur annonser når konsumenterna och följa upp missbruk
- e-post-tjänsteleverantörer att tillämpa riktlinjer för filtrering som garanterar att rekommendationen och vägledningen om kontroll av innehållet i e-brev följs.

Åtgärder på europeisk nivå

Kommissionen skriver att man kommer att fortsätta att ta upp frågor rörande skräppost, spion- och sabotageprogram i internationella sammanhang. Kommissionen avser också att ta nya initiativ på lagstiftnings- och forskningsområdet. Kommissionen avser att publicera en strategi för kampen mot nätbrottsligheten i början av 2007.

Kommissionen föreslår i sitt meddelande[9] om *översynen av regelverket för elektroniska kommunikationsnät* rörande kommunikationstjänster att nätoperatörer och tjänsteleverantörer skall vara skyldiga att meddela myndigheterna och sina kunder om säkerhetsbrott som lett till förlust av personuppgifter. Tillsynsmyndigheterna skulle enligt förslaget få befogenhet att se till att operatörerna har tillräckliga säkerhetsriktlinjer m.m.

---

[7] Se <http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf>.

[8] Yttrande 2/2006 från artikel 29-gruppen om kontroll av e-post och skyddet av privatlivet (WP 118).

[9] Se <http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm>.

Kommissionens förslag om regelverket för elektronisk kommunikation innehåller också bestämmelser som skulle ge *Enisa* en rådgivande roll i informationssäkerhetsfrågor. I kommissionens meddelande om en strategi för ett säkert informationssamhälle[10] finns också förslag om att Enisa skall bygga upp ett samarbete för insamling av uppgifter om säkerhetsincidenter och konsumenternas förtroendenivå. Vidare skall Enisa enligt förslaget undersöka försättningarna för ett EU-system för informationsutbyte och varningar i syfte att underlätta åtgärder vid hot mot elektroniska nät.

Frågor rörande sabotageprogram förväntas omfattas av det sjunde ramprogrammet för *forskning*, t.ex. dolda botnet och datavirus, men också attacker mot mobil- och rösttjänster.

I det *internationella arbetet* vill kommissionen öka samarbetet med tredjeländer och kommer därför att försöka se till att skräppost och spion- och sabotageprogram tas upp i avtal mellan EU och tredjeländer.

Kommissionen kommer att

- arbeta för att öka medvetenheten och stärka samarbetet mellan berörda parter
- utveckla överenskommelser med tredjeländer om skräppost, spion- och sabotageprogram
- lägga fram lagförslag med strängare regler om skydd av personuppgifter och säkerhet inom kommunikationssektorn, och lägga fram en strategi om nätbrottslighet
- utnyttja Enisas sakkunskap i säkerhetsfrågor
- främja forskning och utveckling genom sjunde ramprogrammet.

1.2 Gällande svenska regler och förslagets effekt på dessa

Kommissionens meddelande innehåller inte några förslag som skulle ge direkt effekt på svenska regler. Vissa förslag kan dock förväntas och får analyseras när de presenteras (t.ex. i översynen av direktiven om elektronisk kommunikation).

Det finns begränsningar i på vilket sätt operatörer i dag får filtrera trafik. Dessa begränsningar har inget undantag avseende säkerhetsfrågor och det krävs därmed i princip ett samtycke från användarna för att filtrering skall kunna användas.

E-postreklam är reglerat i marknadsföringslagen (1995:450) med ett tillägg (2004:103). Enligt lagen får en näringsidkare vid marknadsföring till en fysik person använda elektronisk post bara om den fysiska personen har samtyckt på förhand. Har näringsidkaren fått den fysiska personens uppgifter om

[10] KOM(2006) 251 slutlig.

elektronisk adress för elektronisk post i samband med försäljning av en produkt till personen gäller inte kravet på samtycke, om inte den fysiska personen motsatt sig att uppgiften om elektronisk adress används i marknadsföringssyfte.

Vid marknadsföring av elektronisk post skall meddelandet alltid innehålla en giltig adress till vilken mottagaren kan sända en begäran om att marknadsföringen skall upphöra. Detta gäller även marknadsföring till en juridisk person.

För dataintrång döms, enligt 4 kap. 9 c § brottsbalken, den som olovligen bereder sig tillgång till en upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in en sådan upptagning. Med upptagning avses även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling. Straffet är böter eller fängelse i högst två år.

Regeringen fastställde en strategi för ökad säkerhet i Internets infrastruktur den 7 december 2006 (dnr N2006/5335/ITFoU). En övergripande svensk strategi inom informationssäkerhetspolitiken redovisades av den dåvarande regeringen år 2002 i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158) där Försvarets materielverk, Försvarets radioanstalt, Krisberedskapsmyndigheten och Post- och telestyrelsen fick nya uppgifter inom området. Flera andra myndigheter som Säkerhetspolisen, Datainspektionen och Verket för förvaltningsutveckling (Verva) har också ansvar för informationssäkerhetsfrågor. I propositionen Samverkan vid kris – för ett säkrare samhälle (prop. 2005/06:133) angav den tidigare regeringen att strategin, som också tar hänsyn till den internationella dimensionen, bör utvecklas och breddas.

1.3 Budgetära konsekvenser

Kommissionen redogör inte för några kostnader i meddelandet. Förslagen som rör dialog och samverkan bör inte vara allt för omfattande och hör till viss del till budgeten för kommissionen. Flera av förslagen kan innebära kostnader, men bereds i en annan ordning: översynen av direktiven om elektronisk kommunikation, uppdrag som Enisa skall utföra (Enisas budget och arbetsprogram). Kommissionen uppmanar även medlemsstaterna och den privata sektorn att vidta egna åtgärder.

2 Ståndpunkter

2.1 Svensk ståndpunkt

Nedan kommenteras kommissionens förslag till åtgärder på europeisk nivå (avsnitt 4.3.5, s. 12). Kommissionen lämnar inga nya förslag utan hänvisar till pågående och kommande arbete.

Kommissionens avsikt att lägga fram nya lagförslag i början av 2007 med strängare regler om skydd av personuppgifter och säkerhet inom kommunikationssektorn bereds inom ramen för **översynen av direktiven för elektronisk kommunikation**. Regeringen anser att man skall vara försiktig med att skapa särskilda dataskyddskrav för aktörer inom marknaden för elektronisk kommunikation utöver de som gäller genom nuvarande dataskyddsreglering. Syftet bör vara att få operatörerna att vidta åtgärder så att en allmän konfidentialitet och säkerhet kan upprätthållas och inte enbart vad gäller personuppgifter.

Att **lägga fram en strategi mot nätbrottslighet** kan i sig var intressant, men kommissionen har här, liksom tidigare, kopplat nätbrottslighet till den bredare frågan om informationssäkerhet. Detta bör enligt regeringen göras med en viss försiktighet. IT-relaterad brottslighet utgör i många fall traditionella brott (bedrägeri, utpressning etc.) som underlättas av eller genomförs med IT. Brotten kan vara nog så allvarliga men det är inte alltid IT-komponenten som är avgörande för brottsligheten. I många fall bidrar dock ett bra informationssäkerhetsarbete till att minska risken för olika slags brott (t.ex. dataintrång). Många problem inom IT-området uppstår till följd av IT-systemens komplexitet, misstag, olyckor och oklara regelverk.

Regeringen ser positivt på att **utnyttja Enisas sakkunskap i säkerhetsfrågor.** Arbetsuppgifter för **Enisa** (se avsnitt 4.3.2, s. 11) skall beslutas enligt förordningen om Enisa. Det är byråns styrelse (där kommissionen har tre platser) som beslutar om arbetsprogrammet. Att kommissionen här, och i andra sammanhang, presenterar nya arbetsuppgifter, utanför processen i byrån, blir problematiskt att hantera.

Regeringen är tveksam till förslaget att bygga upp ett samarbete med medlemsstater och andra intressenter för **insamling av uppgifter om säkerhetsincidenter** och konsumenternas förtroendenivå. Regeringen delar kommissionens syn att vi behöver öka kunskapen om informationssäkerhet. Att basera kunskapen på uppgifter om IT-incidenter är otillräckligt och inte ändamålsenligt för att få en tillräcklig förståelse för problem och lösningar inom informationssäkerhetspolitiken.

Förslaget om **ett EU-system för informationsutbyte och varning** om hot mot elektroniska nät framstår enligt regeringen som oklart. Ett omfattande internationellt arbete pågår inom CSIRT-området (t.ex. varningar om nya säkerhetsbrister i program). Kommissionen har inte i sitt förslag[11] särskilt motiverat vad vare sig EU-nivån eller flerspråkigheten tillför. Vidare finns det företag som driver affärsmässig verksamhet på området. Arbetet skulle däremot kunna inriktas på att stödja och utbyta erfarenheter mellan medlemsstaterna, något som Sverige har framfört till Enisa. I Sverige har Post- och telestyrelsen sedan 2003 i uppdrag att driva en rikscentral för hantering

[11] Se kommissionens meddelande En strategi för ett säkert informationssamhälle – ”Dialog, partnerskap och användarinflytande” (KOM(2006) 251 slutlig) och fakta-PM 2005/06:FPM116.

av uppgifter (t.ex. varningar) om IT-incidenter – det görs i Sveriges IT-incidentcentrum (Sitic).

Regeringen välkomnar ansatserna att **främja forskning och utveckling** inom området, men betonar att det är viktigt att resultaten sprids och kommer till praktisk användning.

2.2 Medlemsstaternas ståndpunkter

För närvarande finns inga uppgifter om andra medlemsstaters ståndpunkter.

2.3 Institutionernas ståndpunkter

För närvarande finns inga uppgifter om institutionernas ståndpunkter.

2.4 Remissinstansernas ståndpunkter

Meddelandet har inte remissbehandlats.

3 Övrigt

3.1 Fortsatt behandling av ärendet

Kommissionen skriver att den kommer att övervaka genomförandet av åtgärder som förslås i meddelandet och senast 2008 bedöma om det krävs ytterligare insatser.

3.2 Rättslig grund och beslutsförfarande

Meddelandet innehåller inga konkreta förslag till beslut.

3.3 Fackuttryck/termer

Artikel 29-gruppen
För att EG-direktivet om personuppgifter skall tillämpas på ett enhetligt sätt i EU har det bildats en arbetsgruppen för uppgiftsskydd – den s.k. Artikel 29-gruppen. Den är rådgivande och oberoende och har också till uppgift att yttra sig till kommissionen om skyddsnivån i länder utanför gemenskapen. Dessutom skall gruppen avge yttranden om branschöverenskommelser som utarbetas inom EU.

Botnet
Nät av kapade datorer som kan fjärrstyras och utnyttjas för t.ex. spridande av skräppost och tillgänglighetsattacker.

CNSA
Contact Network of Spam Authorities – ett av kommissionen inrättat kon-

taktnät för myndigheter, avseende skräppost. Medlemskap är frivilligt. Syftet är att göra det lättare att hantera klagomål över gränserna.

CSIRT
Engelsk förkortning för *Computer Security Incident Response Team*. En organisation som har till uppgift att stödja arbetet med att förebygga IT-incidenter och varna för nya säkerhetsbrister, ofta också att lämna stöd under och efter en incident. Ibland kallat *Computer Emergency Response Team (CERT)*.

Datamaskar
Datamaskar är ett samlingsbegrepp på ett spridningssätt som innebär att ett program genom att utnyttja olika säkerhetsbrister automatiskt sprider sig över ett nätverk. En datamask kräver ingen aktiv åtgärd från användaren för att sprida sig.

Datavirus
Datavirus är program som installeras på datorn mot användarens vilja och som kan spridas vidare till andra datorer.

Enisa
Förkortning för Europeiska byrån för nät- och informationssäkerhet *(European Network and Information Security Agency)*.

LAP
London Action Plan är ett samarbete som startade 2004 i syfte att för att främja internationellt samarbete för att bekämpa skräppost och relaterade problem som bedrägeri, nätfiske och datavirus. Deltagarna utser t.ex. kontaktpunkter och ska främja privat-offentlig samverkan.

Nätfiske
Nätfiske (en. phishing) är en sorts skräppost som syftar till att samla in information från Internetanvändare. E-brevet ger sken av att komma från en legitim organisation. Tanken är att lura mottagaren att lämna ifrån sig personlig eller ekonomisk information, t.ex. användarnamn och lösenord, personnummer, kreditkortsnummer eller bankkontonummer, som sedan kan användas för bedrägerier. E-postmeddelandet kan också innehålla ett erbjudande och en länk till en webbsida med mer information. När man går till webbsidan laddas ett program ner till datorn utan att man märker det. Programmet samlar sedan automatiskt in känslig information, och skickar den vidare.

Phishing
Se nätfiske.

Sabotageprogram
Översättning av den engelska förkortningen *malware (malicious software)*. En överordnad term för de flesta typer av oönskade program, framför allt datavirus, datamaskar och trojaner. Ibland kallat skadlig kod.

Skadlig kod
Se sabotageprogram.

Spionprogram
Spionprogram samlar in personliga uppgifter såsom lösenord och kreditkortsnummer, kan också visa användningsmönster för en dator.

Trojaner
Ett slags sabotageprogram som döljs i ett annat program. Till skillnad från datavirus sprider sig inte trojaner.

WSIS
Engelsk förkortning för FN:s toppmöte om informationssamhället *(World Summit on Information Society)* som avslutades i Tunisien 2005 vars slutdokument *(Tunis Agenda on the Information Society)* behandlar bl.a. informationssäkerhet.