Regeringskansliet
Faktapromemoria 2005/06:FPM116

En strategi för ett säkert informationssamhälle

Näringsdepartementet

2006-09-06

Dokumentbeteckning

KOM(2006) 251 slutlig
Meddelande från kommissionen till rådet, Europaparlamentet, europeiska ekonomiska och sociala kommittén samt regionkommittén – En strategi för ett säkert informationssamhälle – ”Dialog, partnerskap och användarinflytande”

Sammanfattning

Europeiska kommissionen presenterar en strategi för ett säkert informationssamhälle. Målet är att vidareutveckla en dynamisk och omfattande strategi för EU, grundad på en säkerhetskultur och på dialog, partnerskap och användarinflytande. I EU har arbetet med att bekämpa säkerhetsproblem följt tre linjer: specifika åtgärder för informationssäkerhet, de rättsliga ramarna för elektronisk kommunikation och kampen mot IT-relaterad brottslighet.

I meddelandet redogör kommissionen för vad de anser vara de viktigaste frågorna på området t.ex. att ekonomiska motiv ligger bakom attacker mot IT-system och att ny teknik skapar nya risker. IT-användningen har stor betydelse för EU:s ekonomi och störningar kan får stora konsekvenser samtidigt som man i EU tenderar att underskatta riskerna. Kunskapen om informationssäkerhet behöver enligt kommissionen öka. Kommissionen avser att komma med ytterligare förslag enligt de tre huvudlinjerna.

Kopplingar till andra områden inom EU-politiken görs enligt regeringens bedömning i för liten utsträckning. Regeringen menar att fortsatt EU-arbete inom området behövs, men att kommissionens fokusering på IT-relaterade brottslighet och attacker är för smalt. Då framstår en del av förslagen som otillräckliga. Regeringen förordar en bred definition av informationssäkerhet, inklusive förebyggande åtgärder som leder till hög driftsäkerhet och som främjar en bred IT-användning i samhället.

1.1 Innehåll

1.1.1 Bakgrund

Europeiska kommissionen skrev i meddelandet i2010 – det europeiska informationssamhället för tillväxt och sysselsättning[1] om hur viktigt det är med nät- och informationssäkerhet om man vill skapa ett gemensamt informationsområde i EU. Kommissionen menade att vår ekonomi och vårt samhälles alla strukturer blir allt mer beroende av nätens och informationssystemens tillgänglighet, tillförlitlighet och säkerhet.

Syfte med detta meddelande, som presenterades den 31 maj 2006, är att blåsa nytt liv i kommissionens strategi så som den beskrivs i 2001 års meddelande Nät- och informationssäkerhet: förslag till en europeisk strategi.[2]

Målet är att vidareutveckla en dynamisk och omfattande strategi för EU, grundad på en säkerhetskultur och på dialog, partnerskap och användarinflytande.

Inom EU-samarbetet har tre huvudlinjer följts för att hantera informationssamhällets säkerhetsproblem, nämligen med specifika åtgärder för nät- och informationssäkerhet, de rättsliga ramarna för elektronisk kommunikation (som också innehåller integritetsskydd och skydd av personuppgifter) samt kampen mot IT-relaterad brottslighet.

I 2001 års meddelande beskrivs nät- och informationssäkerheten som ”förmågan hos ett nät att tåla, vid en viss tillförlitlighetsnivå, olyckshändelser eller illvilligt uppträdande som äventyrar tillgängligheten, äktheten (autentisering), integriteten och konfidentialiteten hos lagrade eller vidarebefordrade data och besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät.”

1.1.2 Tidigare insatser

Kommissionen lämnar en redogörelse för de viktigaste insatserna som har gjorts inom nät- och informationssäkerhetsområdet.

De rättsliga ramarna för elektronisk kommunikation, som bl.a. innehåller säkerhetsbestämmelser, är föremål för översyn.

Förtroende och säkerhet är också viktiga frågor i EU:s program för forskning och utveckling. Programmet Safer Internet Plus ger stöd till åtgärder som

[1] KOM(2005) 229 slutlig av den 1 juni 2005.

[2] KOM(2001) 298 slutlig av den 6 juni 2001.

syftar till att främja användningen av Internet genom att bekämpa olagligt och skadligt innehåll.

Europeiska nät- och informationssäkerhetsbyrån (Enisa) inrättades i början av 2004 och skall arbeta under fem år. Enisa arbetar för en hög nivå på nät- och informationssäkerheten inom EU.

EU spelar också en aktiv roll i de olika internationella forum som behandlar dessa frågor, till exempel OECD, Europarådet och FN.

1.1.3 Det viktigaste frågorna för säkerheten i informationssamhället

Trots de ansträngningar som har gjorts menar kommissionen att det fortfarande finns stora informationssäkerhetsproblem. Ekonomisk vinning ligger nu ofta bakom attacker mot IT-system. Attackerna görs bl.a. genom att uppgifter olagligt samlas in från användare genom spionprogram och med hjälp av skräppost. Ett annat problem är att datorer kapas och används utan att ägarna vet om det.

Nya kommunikationsplattformar, särskilt de med mobilitet (tredje generationens mobiltelefoner, datorspel m.fl.), skapar nya förutsättningar för attacker och störningar. Datorspridningen och sammankopplingen av utrustning (t.ex. genom RFID, IPv6 och sensorer) ger stora möjligheter men skapar enligt kommissionen också risker för säkerhet och integritet. Kommissionen menar också att stor spridning av standardprogram skapar vad som kallas monokulturer vilket leder till att riskerna blir större (ett datavirus som utnyttjar en viss sårbarhet kan t.ex. spridas snabbare).

Kommissionen framhåller mångfald (diversitet), öppenhet och interoperabilitet (driftskompatibilitet) som viktiga säkerhetsaspekter som bör främjas.

IT-sektorn har stor betydelse för Europas ekonomi, bl.a. genom produktivitetstillväxt, forskning och innovation. IT bidrar enligt kommissionen till ekonomisk tillväxt och sysselsättning. IT-användningen har blivit en grundläggande funktion i ekonomisk och social utveckling.

Bristande informationssäkerhet innebär inte bara risker för ekonomin. Oro kan minska IT-användningen. Tillgängligheten, tillförlitligheten och säkerheten i IT-användningen är förutsättningar för att grundläggande rättigheter skall kunna garanteras på nätet. Kommissionen preciserar inte rättigheterna närmare.

Ett annat viktigt förhållande är att många samhällsviktiga infrastrukturer (t.ex. transporter och energiförsörjning) blir beroende av säkra IT-system. Riskerna underskattas enligt kommissionen fortfarande av företag och allmänheten i EU. Kommissionen understryker också att informationssäkerhet är en fråga som berör alla – myndigheter, företag och enskilda användare.

Kommissionen anser att tillförlitliga uppgifter om utvecklingen och händelser ofta saknas och vill därför öka kunskapen om problemen.

Det är viktigt att presentera nät- och informationssäkerhet som en dygd och en möjlighet menar kommissionen. Om informationskampanjer är alltför negativa undergräver man användarnas förtroende för den nya tekniken.

1.1.4 En dynamisk strategi för ett säkert informationssamhälle

Ett säkert informationssamhälle måste utgå från ökad nät- och informationssäkerhet och en väletablerad säkerhetskultur. Därför föreslår kommissionen vad de kallar en dynamisk och samordnad strategi som omfattar alla berörda parter och grundas på dialog och användarinflytande. Den offentliga och den privata sektorn kompletterar varandra i skapandet av en säkerhetskultur, och därför måste strategiska initiativ på detta område utgå från en öppen dialog mellan alla berörda parter.

Inom ramen för strategin skall kommissionen under 2006 publicera två meddelanden. Ett skall ta upp utvecklingen av skräppost och sabotageprogram (skadlig kod), det andra skall vara ett särskilt meddelande om IT-relaterad brottslighet.

Dessa initiativ kopplas till målen i kommissionens grönbok[3] om ett europeiskt program för skydd av samhällsviktig (kritisk) infrastruktur (t.ex. energiförsörjning och transporter).

I 2006 års översyn av regelverket för elektronisk kommunikation ingår att undersöka hur nät- och informationssäkerheten kan förbättras, t.ex. tjänsteleverantörernas tekniska och organisatoriska åtgärder.

Det är i första hand den privata sektorn som skall förse slutanvändarna med lösningar, tjänster och säkerhetsprodukter skriver kommissionen. Därför är det strategiskt viktigt att den europeiska industrin både är en krävande användare och leverantör inom säkerhetsområdet.

Medlemsstaternas regeringar måste kunna identifiera och införa de bästa metoderna i sin politik, och samtidigt visa sitt engagemang för dessa mål genom att sköta sina egna informationssystem på ett säkert sätt. Myndigheter, både i medlemsstaterna och på EU-nivå, har en viktig uppgift i att informera användarna. En prioriterad uppgift bör vara att öka medvetenheten om nät- och informationssäkerhet och ge information i tid. Kommissionen anser därför att ett viktigt mål för Enisa skulle kunna vara att undersöka möjligheterna att skapa ett EU-omfattande, flerspråkigt system för informationsutbyte och alarmering, baserat på befintliga och planerade initiativ.

Informationssäkerhetens globala dimension innebär att kommissionen, både internationellt och i samordning med medlemsstaterna, måste öka sina ansträngningar att främja ett globalt samarbete, bl.a. genom att arbeta efter den dagordning som antogs vid världstoppmötet om informationssamhället (WSIS) i november 2005.

[3] KOM(2005) 576 slutlig, 17.11.2005.

Forskning och utveckling, inte minst på EU-nivå, bidrar till uppkomsten av nya samarbeten som kan driva på den europeiska IT-industrins tillväxt, inklusive säkerhetssektorn. Kommissionen kommer därför att försöka se till att det inom EU:s sjunde ramprogram för forskning avsätts tillräckliga ekonomiska resurser för forskning om nät- och informationssäkerhet.

1.1.5 Dialoger

Som ett första steg för att förbättra dialogen mellan myndigheter föreslår kommissionen att göra en jämförelse mellan medlemsstaternas nät- och informationssäkerhetsrelaterade strategier, inbegripet särskilda strategier för den offentliga sektorn.

Resultaten från en sådan jämförelse skulle göra det möjligt att hitta de bästa metoderna för att öka medvetenheten om informationssäkerhet hos små och medelstora företag och allmänheten.

Kommissionen anser att det behövs en strukturerad debatt mellan berörda parter om hur man bäst kan utnyttja befintliga instrument och rättsakter för att uppnå den balans som samhället behöver mellan säkerhet och skydd av grundläggande rättigheter som t.ex. personlig integritet.

1.1.6 Partnerskap

Kommissionen menar att det är viktigt att verkligen förstå problemens art och omfattning om man skall kunna föra en effektiv politik. Därför behövs det inte bara tillförlitliga uppgifter om informationssäkerhetstillbud och graden av förtroende för tekniken, utan också aktuella uppgifter om hur stor informationssäkerhetsbranschen är i EU och hur den utvecklas. Kommissionen har för avsikt att be Enisa att utveckla ett samarbete med medlemsstaterna och de berörda parterna för att utarbeta ramar för en sådan datainsamling.

Eftersom EU:s marknader är olika kommer kommissionen att uppmana medlemsstaterna, den privata sektorn och forskningssamfundet att utveckla ett strategiskt samarbete för att garantera tillgången till uppgifter om informationssäkerhetsbranschen i EU.

I syfte att förbättra EU:s möjligheter att bemöta nätsäkerhetshot kommer kommissionen att be Enisa att undersöka om det går att skapa ett system för informationsutbyte och varning. En förutsättning för ett sådant system vore en flerspråkig EU-portal som kan ge information om hot, risker och varningar.

1.1.7 Delaktighet

De olika berörda parternas delaktighet är en förutsättning för att man skall kunna öka medvetenheten om säkerhetsbehov och främja nät- och informationssäkerheten. Därför vill kommissionen uppmana medlemsstaterna att

- delta i den föreslagna jämförelsen av nationella strategier för nät- och informationssäkerhet
- främja informationskampanjer om fördelarna och vinsterna med informationssäkerhet
- driva på spridningen av e-förvaltningstjänster med säkerhetsinformation
- främja utvecklingen av nät- och informationssäkerhet som del av högskolornas läroplaner.

Kommissionen uppmanar också de berörda parterna inom den privata sektorn att ta initiativ för att

- utveckla en lämplig definition av det ansvar som vilar på programtillverkare och Internets tjänsteleverantörer i fråga om att tillhandahålla lämpliga och kontrollerbara säkerhetsnivåer
- främja mångfald (diversifiering), öppenhet, interoperabilitet (driftskompatiilitet), användarvänlighet och konkurrenskraft för att nå säkerhet, och uppmuntra till ett säkerhetsarbete som kan motverka identitetsstölder och integritetskränkningar
- sprida god säkerhetsmetodik för nätoperatörer, tjänsteleverantörer och små och medelstora företag
- främja utbildningsprogram inom affärssektorn så att de anställda får den kunskap som behövs för att ett effektivt säkerhetsarbete
- sträva efter säkerhetscertifiering för produkter, processer och tjänster till lägre kostnader
- engagera försäkringssektorn i utvecklingen av lämpliga metoder för att hantera IT-relaterade risker och främja en kultur för hantering av risker.

1.1.8 Kommissionens slutsatser

Avslutningsvis skriver kommissionen att alla berörda parter måste vara delaktiga om man skall kunna identifiera och lösa säkerhetsproblemen kring informationssystem och nät i EU. Kommissionens strategi skall uppnå detta genom att uppmuntra till insatser där flera parter samarbetar. Detta skulle bygga på gemensamt intresse, och de olika parternas respektive roll skulle framhävas. Därigenom skulle man utveckla en dynamisk ram för att främja en effektiv offentlig beslutsprocess och effektiva insatser från den privata sektorn.

1.2 Gällande svenska regler och förslagets effekt på dessa

Det finns ingen sammanhängande lagstiftning om informationssäkerhet i Sverige. Informationssäkerhetsfrågor behandlas bl.a. i personuppgiftslagen (1998:204) och lagen (2000:832) om kvalificerade elektroniska signaturer och säkerhetsskyddslagen (1996:627).

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).

Regeringen redogjorde för frågor om Internetsäkerhet i propositionen Från IT-politik för samhället till politik för IT-samhället (prop. 2004/05:175). En övergripande svensk strategi inom informationssäkerhetspolitiken redovisades 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 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) och ett europeiskt program för samhällsviktig infrastruktur. Kommissionen uppmanar även medlemsstaterna och den privata sektorn att vidta egna åtgärder.

2 Ståndpunkter

2.1 Svensk ståndpunkt

Regeringen menar att det behövs fortsatt EU-arbete inom informationssäkerhetspolitiken. Att bygga en strategi på **dialog, partnerskap och användarinflytande** (s. 3 i den svenska översättningen av meddelandet) kan vara en bra utgångspunkt för fortsatt arbete. Regeringen vill sätta det vardagliga, förebyggande informationssäkerhetsarbetet i fokus och se fler konkreta åtgärder inom fler områden för att skapa en verklig helhetssyn.

2.1.1 Definition, huvudlinjer och omfattning

Vad som är nät- och informationssäkerhet och politiken för området har länge varit föremål för diskussion. Regeringen noterar att den definition som kommissionen återger är snäv och inriktad på nät för elektronisk kommunikation, samtidigt som kommissionens resonemang senare rör ett bredare fält som datoranvändning, informationsteknikens ekonomiska betydelse, kunskapsuppbyggnad m.m.

De tre huvudlinjer som kommissionen redogör för (specifika åtgärder för nät- och informationssäkerhet, de rättsliga ramarna för elektronisk kommunikation samt kampen mot IT-relaterad brottslighet) är viktiga delar i arbetet. Regeringen menar att det fortsatt kommer att finnas behov av specifika åtgärder inom området och att området elektronisk kommunikation intar en särställning i arbetet med nät- och informationssäkerhet. Till exempel ändrade riksdagen 2005 lagen (2003:389) om elektronisk kommunikation för att öka Post- och telestyrelsens (PTS) möjligheter att arbeta med säkerhetsfrågor (bet. 2004/05:TU17, rskr. 2004/05:201).

Även om det finns kopplingar mellan informationssäkerhetspolitiken och kampen mot IT-relaterad brottslighet, som kommissionen påpekar, så framstår de två andra områdena (specifika åtgärder för informationssäkerhet och översynen av direktiven om elektronisk kommunikation) som mer relevanta i det här sammanhanget för att nå framgång inom informationssäkerhetspolitiken och få driftsäkra och pålitliga IT-system.

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.

En brist i kommissionens meddelande är att andra politikområden på EU-nivå är frånvarande. IT-användningen och IT-beroendet finns nu inom snart sagt alla politikområden och överallt i samhället. Det innebär att informationssäkerhetsfrågorna också måste behandlas inom dessa områden t.ex. finansiella tjänster, energi och transporter. Informationssäkerhet behövs också för en effektiv och säker användning av IT i det europeiska samarbetet. Bristen på helhetssyn tillsammans med kommissionens fokus på avsiktliga attacker och IT-relaterad brottslighet ger enligt regeringens mening en skev bild av informationssäkerhetsfrågorna och möjliga åtgärder.

Det vardagliga informationssäkerhetsarbetet måste enligt regeringen lyftas fram – inom alla politikområden – för att vi ska kunna ha förtroende för de IT-system som vi är beroende av i dagens samhälle.

2.1.2 Kommissionens förslag

Kommissionen framhåller **diversitet, öppenhet och driftskompatibilitet som viktiga säkerhetsaspekter som bör främjas** (s. 5). Regeringen konstaterar att informationssäkerhetsarbetet är komplext och starkt beroende av vilka IT-system som används, i vilken miljö de används etc. De uppräknade aspekterna är ofta, men inte alltid, relevanta och försiktighet bör iakttas när man slår fast principer på hög nivå inom ett tekniskt område i snabb utveckling.

Regeringen delar kommissionens syn att vi behöver **öka kunskapen om problemen** (s. 6), men anser att basera detta på uppgifter om IT-incidenter (tillbud) är otillräckligt och inte ändamålsenligt.

Att upprätthålla förtroende för den nya tekniken och **presentera informationssäkerheten som en dygd och en möjlighet** (s. 6) är enligt regeringen angeläget, men också ett ansvar som delas av många aktörer. Regeringen understryker behovet av hög informationssäkerhet till skydd för personlig integritet och personuppgifter.

Regeringen menar att en **dialog mellan de berörda parterna** (s. 7) behövs, men noterar att detta sedan tidigare har varit del av både kommissionen och Enisas uppdrag.

I arbetet med översynen av regelverket för elektronisk kommunikation har regeringen, liksom kommissionen, lyft fram säkerhetsfrågorna.

Regeringen delar också synen att det i första hand är den privata sektorn som skall förse användarna med lösningar tjänster och produkter inom området. Medlemsstaterna har ansvar för de egna systemen, som kommissionen framhåller, medan uppmaningen om vad och hur myndigheter skall informera framstår som för detaljerad.

Kommissionens förslag om att **skapa ett EU-omfattande, flerspråkigt system för informationsutbyte och alarmering** (s. 7) framstår enligt regeringen som oklart. Givet de invändningar mot kommissionens huvudlinjer (ovan) som regeringen har, framstår förslaget som missriktat. Ett omfattande internationellt arbete pågår inom CSIRT-området (t.ex. varningar om nyupptäckta säkerhetsbrister i program). Kommissionen har inte särskilt motiverat vad vare sig EU-nivån eller flerspråkigheten tillför. Vidare finns det en marknad 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 av uppgifter (t.ex. varningar) om IT-incidenter – det görs i Sveriges IT-incidentcentrum (Sitic).

Regeringen välkomnar ansatserna att **främja ett globalt samarbete om nät- och informationssäkerhet** (s. 7) och forskning på området.

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

I mitten av 2007 kommer kommissionen att rapportera till rådet och Europaparlamentet om vilka insatser som inletts och vad man hittills kommit fram till samt hur långt man kommit med de olika insatserna (inbegripet Enisas verksamhet och medlemsstaternas och den privata sektorns insatser). Vid behov kommer kommissionen att föreslå en rekommendation om nät- och informationssäkerhet.

3.2 Rättslig grund och beslutsförfarande

Strategin innehåller inga konkreta förslag för beslut.

3.3 Fackuttryck/termer

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)*.
Enisa	Engelsk förkortning Europeiska byrån för nät- och informationssäkerhet *(European Network and Information Security Agency)*.
IPv6	En ny version av datakommunikationsprotokollet *Internet Protocol (IP)* som används för att skicka data till datorer och andra apparater i olika nät (t.ex. på Internet). I dag är IPv4 den vanligaste versionen.
RFID	Engelsk förkortning för *Radio Frequency Identification* – radiofrekvensidentifiering. Det är teknik för lagring och trådlös överföring av små datamängder på korta avstånd mellan speciella kretsar och sändare/mottagare.
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.
WSIS	Engelsk för kortning 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.