392D0242

RÅDETS BESLUT

av den 31 mars 1992

om informationssystemens säkerhet

(92/242/EEG)

EUROPEISKA GEMENSKAPERNAS RÅD HAR BESLUTAT FÖLJANDE

med beaktande av Fördraget om upprättandet av Europeiska ekonomiska gemenskapen, särskilt artikel 235 i detta,

med beaktande av kommissionens förslag([1]),

med beaktande av Europaparlamentets yttrande([2]),

med beaktande av Ekonomiska och sociala kommitténs yttrande([3]), och

med beaktande av följande:

Gemenskapen har som sin uppgift att genom upprättandet av en gemensam marknad och genom en gradvis tillnärmning av medlemsstaternas ekonomiska politik främja en harmonisk utveckling av den ekonomiska verksamheten i hela gemenskapen, en kontinuerlig och väl avvägd expansion, en ökning av stabiliteten, en snabbare höjning av levnadsstandarden samt närmare relationer mellan medlemsstaterna.

Information som lagras, bearbetas och sänds elektroniskt spelar i allt större utsträckning en viktig roll för de ekonomiska och sociala aktiviteterna.

Tillkomsten av effektiva, världsomspännande kommunikationer och den ökade användningen av elektronisk informationshantering understryker behovet av adekvat skydd.

Europaparlamentet har i sina debatter och resolutioner upprepade gånger understrukit betydelsen av informationssystemens säkerhet.

Ekonomiska och sociala kommittén har betonat behovet av att inom gemenskapen behandla frågor om informationssystemens säkerhet, särskilt med hänsyn till de effekter som genomförandet av den inre marknaden kommer att få.

Åtgärder på nationell, internationell och gemenskapsnivå utgör en god grund.

Det finns ett nära samband mellan telekommunikation, informationsteknologi, standardisering, informationsmarknaden, forsknings-, utvecklings- och teknikpolitiken samt det arbete som gemenskapen redan tagit sig an inom dessa områden.

Det är lämpligt att samordna insatserna genom att vidareutveckla pågående nationellt och internationellt arbete och genom att främja samarbete mellan de viktigaste berörda parterna. Detta bör ske inom ramen för en samordnad handlingsplan.

Informationssystemens säkerhet är en så komplicerad fråga, att särskilda strategier behöver utvecklas som möjliggör fri rörlighet för information inom den inre marknaden samtidigt som säkerheten vid användning av informationssystem säkerställs i hela gemenskapen.

Det är varje medlemsstats ansvar att fastställa de begränsningar som säkerheten och den allmänna ordningen kräver.

Medlemsstaternas ansvar inom detta område kräver en samordnad insats, grundad på nära samarbete med chefstjänstemän i medlemsstaterna.

Beslut bör fattas om en handlingsplan för en inledande period på tjugofyra månader och om inrättandet av en kommitté av chefstjänstemän med ett långsiktigt uppdrag att råda kommissionen beträffande åtgärder inom området informationssystemens säkerhet.

Ett belopp på 12 miljoner ecu anses nödvändigt för att genomföra verksamheten under en inledande period av tjugofyra månader. I nuvarande finansiella perspektiv uppskattas det belopp som behövs för 1992 till 2 miljoner ecu.

De belopp som avsätts för att finansiera programmet under den period som följer efter budgetåret 1992 skall inrymmas i gemenskapens gällande ekonomiska ram.

HÄRIGENOM BESLUTAS FÖLJANDE.

Artikel 1

Inom området informationssystemens säkerhet vidtas härmed följande åtgärder:

— Utveckling av övergripande strategier för informationssystemens säkerhet (handlingsplan) för en inledande period på 24 månader.

— Inrättande av en grupp chefstjänstemän med långsiktigt uppdrag att råda kommissionen om vilka åtgärder som bör vidtas inom området informationssystemens säkerhet, i det följande kallad "kommittén".

([1]) EGT nr C 277, 5.11.1990, s. 18.
([2]) EGT nr C 94, 13.3.1992
([3]) EGT nr C 159, 17.6.1991, s. 38.

Artikel 2

1. Kommissionen skall fortlöpande samråda med kommittén i frågor som rör informationssystemens säkerhet i samband med de olika verksamheter som utförs av gemenskapen, särskilt vid utformningen av arbetsstrategier och arbetsprogram.

2. Handlingsplanen skall, som anges i bilagan, innefatta förberedande arbete enligt följande riktlinjer:

I. Utveckling av en strategisk ram för informationssystemens säkerhet.

II. Kartläggning av användares och tjänsteproducenters krav på informationssystemens säkerhet.

III. Lösningar på omedelbara och interimistiska behov hos användare, leverantörer och tjänsteproducenter.

IV. Utveckling av specifikationer, standardisering, evaluering och certifiering i fråga om informationssystemens säkerhet.

V. Teknisk och driftmässig utveckling av informationssystemens säkerhet.

VI. Tillhandahållande av tjänster för informationssystemens säkerhet.

Artikel 3

1. De gemenskapsmedel som beräknas vara nödvändiga för verksamhetens genomförande uppgår till 12 miljoner ecu för den inledande perioden, inklusive 2 miljoner ecu för 1992 inom budgetperioden 1988-1992.

För den därpå följande tillämpningsperioden för programmet skall beloppet inrymmas i den gällande ekonomiska ramen för gemenskapen.

2. Den budgetansvariga myndigheten skall bestämma vilka anslag som finns tillgängliga för varje budgetår med beaktande av de principer för sund förvaltning av finanserna som anges i artikel 2 av den budgetförordning som är tillämplig för de europeiska gemenskapernas allmänna budget.

Artikel 4

En utvärdering av de framsteg som uppnåtts under den inledande perioden skall för kommissionens räkning utföras av en grupp oberoende experter. Denna grupps rapport skall, tillsammans med eventuella kommentarer från kommissionen, överlämnas till Europaparlamentet och rådet.

Artikel 5

1. Kommissionen skall vara ansvarig för handlingsplanens genomförande. Den skall biträdas av en rådgivande kommitté, sammansatt av företrädare för medlemsstaterna och med en företrädare för kommissionen som ordförande.

2. Handlingsplanen skall genomföras i enlighet med de mål som fastställts i artikel 2 och uppdateras om så är nödvändigt. Planen skall ange de detaljerade målen och finansiella och andra typer av åtgärder som skall vidtas. Kommissionen skall infordra anbud på grundval av handlingsplanen.

3. Handlingsplanen skall genomföras i nära samarbete med dem som är verksamma inom denna sektor. Den skall ta hänsyn till, främja och komplettera det pågående europeiska och internationella standardiseringsarbetet inom detta område.

Artikel 6

1. Det förfarande som fastställs i artikel 7 skall gälla åtgärder som berör gemenskapspolitiken inom området informationssystemens säkerhet.

2. Det förfarande som fastställs i artikel 8 skall gälla

— utarbetande och uppdatering av den handlingsplan som anges i artikel 5,

— innehåll i anbudsinfordran, bedömningar av anbuden och uppskattat belopp för gemenskapens bidrag till åtgärder, om detta belopp överskrider 200 000 ecu,

— samarbete i verksamheter enligt detta beslut med organisationer som inte tillhör gemenskapen,

— åtgärder för spridning, skydd och utnyttjande av uppnådda resultat,

— åtgärder som skall vidtas för att utvärdera insatserna.

3. Om beloppet för gemenskapens bidrag till åtgärderna är mindre än eller lika med 200 000 ecu skall kommissionen samråda med kommittén om vilka åtgärder som skall vidtas och underrätta kommittén om resultatet av sin bedömning.

Artikel 7

Kommissionens företrädare skall till kommittén överlämna ett förslag till åtgärder. Kommittén skall yttra sig över förslaget inom den tid som ordföranden bestämmer med hänsyn till hur brådskande frågan är, om så erfordras genom röstning.

Yttrandet skall protokollföras och dessutom har varje medlemsstat rätt att begära att få sin uppfattning tagen till protokollet.

Kommissionen skall ta största hänsyn till det yttrande som kommittén avgett. Den skall underrätta kommittén om det sätt på vilket dess yttrande har beaktats.

Artikel 8

Kommissionens företrädare skall till kommittén framlägga förslag till åtgärder. Kommittén skall yttra sig över förslaget inom den tid som ordföranden bestämmer med hänsyn till hur brådskande frågan är. Yttrandet skall avges med den majoritet som enligt artikel 148.2 i fördraget skall

tillämpas vid beslut som rådet skall fatta på förslag av kommissionen. De röster som avges av företrädarna för medlemsstaterna inom kommittén skall vägas enligt nämnda artikel. Ordföranden får inte rösta.

Kommissionen skall själv anta förslaget om det har tillstyrkts av kommittén.

Om förslaget inte är förenligt med kommitténs yttrande eller om inget yttrande avges, skall kommissionen utan dröjsmål föreslå rådet vilka åtgärder som skall vidtas. Rådet skall fatta sitt beslut med kvalificerad majoritet.

Om rådet inte har fattat något beslut inom tre månader från det att förslaget mottagits, skall kommissionen själv besluta att de föreslagna åtgärderna skall vidtas såvida inte rådet med enkel majoritet har avvisat förslaget.

Utfärdat i Bryssel den 31 mars 1992.

På rådets vägnar

Vitor MARTINS

Ordförande

BILAGA

Sammanfattning av handlingslinjer

RIKTLINJER FÖR EN HANDLINGSPLAN INOM OMRÅDET INFORMATIONSSYSTEMENS SÄKERHET (IT-SÄKERHET)

INLEDNING

Målet för handlingsplanen skall vara att utveckla övergripande strategier i syfte att ge alla berörda användare och producenter av elektroniskt lagrad, bearbetad eller överförd information tillräckligt skydd av informationssystemen mot oavsiktliga och avsiktliga hot.

Handlingsplanen skall ta hänsyn till och komplettera den världsomspännande standardiseringsverksamhet som pågår inom området.

Den skall innefatta följande handlingslinjer:

— Utveckling av en strategisk ram för IT-säkerhet.

— Kartläggning av användares och tjänsteproducenters krav på IT-säkerhet.

— Lösningar på omedelbara och interimistiska behov hos användare, leverantörer och tjänsteproducenter.

— Utveckling av specifikationer, standardisering, evaluering och certifiering i fråga om IT-säkerhet.

— Teknisk och driftmässig utveckling av IT-säkerhet.

— Tillhandahållande av tjänster för IT-säkerhet.

Handlingsplanen skall genomföras av kommissionen i nära anslutning till motsvarande åtgärder i medlemsstaterna och i samband med liknande forsknings- och utvecklingsarbete i gemenskapen.

1. Handlingslinje I – utveckling av en strategisk ram för IT-säkerhet

1.1 *Uppgift*

IT-säkerhet är ett grundläggande behov i det moderna samhället. Elektroniska informationstjänster behöver en säker infrastruktur för telekommunikation, säker maskin- och programvara liksom säker användning och förvaltning. En övergripande strategi, som tar hänsyn till alla aspekter på IT-säkerheten behöver upprättas, för att en splittrad insats skall kunna undvikas. Varje strategi som gäller säkerhet för information, bearbetad i elektronisk form måste återspegla varje samhälles önskan att fungera effektivt men ändå skydda sig i en snabbt föränderlig värld.

1.2 *Mål*

En strategiskt uppbyggd ram måste upprättas för att bringa sociala, ekonomiska och politiska mål i överensstämmelse med tekniska, driftmässiga och juridiska intressen för gemenskapen i ett internationellt sammanhang. Den känsliga jämvikten mellan olika intressen, mål och begränsningar måste uppnås genom att aktörerna inom sektorn tillsammans utvecklar en gemensam uppfattning och kommer överens om en strategisk ram. Detta är en förutsättning för att olika intressen och behov skall kunna sammanjämkas både politiskt och industriellt.

1.3 *Status och tendenser*

Situationen kännetecknas av en allt större medvetenhet om behovet av handling. I avsaknad av ett initiativ för att samordna ansträngningarna förefaller det emellertid mycket troligt att skilda åtgärder inom olika sektorer kommer att skapa en situation, som i själva verket kommer att vara motsägelsefull och leda till ökande allvarliga juridiska, sociala och ekonomiska problem.

1.4 *Krav, möjligheter och prioriteringar*

En sådan gemensam ram bör omfatta riskanalyser och riskhantering då det gäller sårbarheten hos informationstjänster och andra berörda tjänster, samordningen av lagar och förordningar med avseende på missbruk och felaktig användning av dator/telekommunikation, administrativa infrastrukturer inklusive säkerhetspolicy och fastställande av hur dessa bestämmelser effektivt skall kunna genomföras inom olika industrisektorer/fackområden, sociala hänsyn och sekretessfrågor (t.ex. användning av identifiering, autentiecering, mottagningsbevis och möjligen auktorisationsplaner i en demokratisk miljö).

Tydliga anvisningar skall ges för utvecklingen av fysiska och logiska arkitekturer för säkra distribuerade informationstjänster, standarder, riktlinjer och definitioner avseende kvalitetsgranskade säkerhetsprodukter och säkerhetstjänster, samt för pilotförsök och prototyper för att upprätta olika funktionsdugliga administrativa strukturer, arkitekturer och standard i förhållande till behoven inom särskilda sektorer.

Ett säkerhetsmedvetande måste skapas för att påverka användarna till en större omsorg om IT-säkerhet.

2. Handlingslinje II – kartläggning av användares och tjänsteproducenters krav på IT-säkerhet

2.1 *Uppgift*

IT-säkerhet är en oundgänglig förutsättning för tillförlitlighet och pålitlighet av tillämpningar i affärslivet, för immateriella rättigheter och för sekretess. Det leder oundvikligen till en svår avvägning och ibland till val mellan ett ställningstagande för fri handel och ett ställningstagande för personlig integritet och immateriella rättigheter. Dessa val och kompromisser måste bygga på en fullständig bedömning av behoven och den inverkan som olika möjliga åtgärder har på de berörda informationssystemens säkerhet.

Användarkraven medför att säkerhetsfunktionerna för informationssystem påverkas av tekniska, driftmässiga och reglerande villkor. En systematisk undersökning av säkerhetskraven på informationssystem utgör därför ett viktigt led i utvecklingen av lämpliga och effektiva åtgärder.

2.2 *Mål*

Att fastställa art och kännetecken för användares och tjänsteproducenters krav på säkerhet och deras förhållande till säkerhetsåtgärder för informationssystem.

2.3 *Status och tendenser*

Hittills har inga samordnade ansträngningar gjorts för att fastställa de snabbt framväxande och föränderliga krav som de viktigaste aktörerna har i fråga om IT-säkerhet. Gemenskapens medlemsstater har identifierat kraven på harmonisering av nationella verksamheter (särskilt i fråga om evalueringskriterier för IT-säkerhet). Enhetliga evalueringskriterier och regler för ömsesidigt erkännande av evalueringscertifikat är av stor betydelse.

2.4 *Behov, möjligheter och prioriteringar*

Som grundval för en enhetlig och öppen behandling inom sektorn av aktörernas berättigade behov, anses det nödvändigt att utveckla en överenskommen klassificering av användarkraven och konsekvenserna av denna för att tillhandahålla IT-säkerhet.

Det anses också viktigt att identifiera behoven av lagstiftning, förordningar och praxis mot bakgrund av en bedömning av tendenserna i fråga om tjänsternas egenskaper och den teknik som används, att identifiera alternativa strategier för att uppfylla målen genom administrativa åtgärder och åtgärder som gäller service, drift eller teknik samt att bedöma effektivitet, användarvänlighet och kostnader för alternativa säkerhetslösningar och strategier för informationssystem för användare, tjänsteproducenter och operatörer.

3. Handlingslinje III – lösningar på omedelbara och interimistiska behov hos användare, leverantörer och tjänsteproducenter

3.1 *Uppgift*

För närvarande är det möjligt att på ett ändamålsenligt sätt skydda datorer från obehörigt intrång utifrån genom "isolering", dvs. genom att använda sig av konventionella organisatoriska och fysiska åtgärder. Detta gäller också för elektronisk kommunikation inom en sluten användargrupp som arbetar via ett nät, avsett för ett visst ändamål. Situationen är mycket annorlunda, om informationen delas mellan användargrupper eller utväxlas via ett offentligt eller allmänt tillgängligt nät. I dessa fall finns i allmänhet varken teknik, terminaler och tjänster eller därmed sammanhängande standarder och förfaranden tillgängliga för att ge jämförbar IT-säkerhet.

3.2 *Mål*

Målet måste vara att på kort tid finna lösningar som kan uppfylla de mest angelägna behoven hos användare, tjänsteproducenter och tillverkare. Detta inbegriper användning av gängse evalueringskriterier för IT-säkerhet. Dessa bör formuleras så att de är öppna för framtida behov och lösningar.

3.3 *Status och tendenser*

En del användargrupper har utvecklat tekniker och förfaranden för sin specifika användning, vilka framför allt uppfyller behovet av autenticering (äkthetsbevis), åtkomstskydd och mottagningsbevis. I allmänhet används magnetkort eller aktiva kort. En del använder mer eller mindre komplicerade kryptografiska tekniker. Detta har ofta inneburit att man har definierat speciella "gruppbehörigheter". Det är emellertid svårt att anpassa dessa tekniker och metoder till att allmänt tillfredsställa behoven i en öppen miljö.

ISO arbetar med OSI Information System Security (ISO DIS 7498-2) och CCITT i X.400-sammanhang. Det är också möjligt att sätta in säkerhetssegment i meddelandena. Autenticering, åtkomstskydd och mottagningsbevis behandlas som en del av meddelandena (EDIFACT) liksom som en del av X.400 MHS.

För närvarande är den juridiska ramen för elektroniskt datautbyte (EDI) fortfarande under utformning. Internationella handelskammaren har offentliggjort enhetliga regler för utbyte av kommersiella data via telenät.

Flera länder (t.ex. Tyskland, Frankrike, Storbritannien och Förenta staterna) har utvecklat eller håller på att utveckla kriterier för utvärdering av tillförlitligheten hos produkter och system för IT och telekommunikation och därtill hörande förfaranden för utvärderingar. Dessa kriterier har samordnats med de nationella tillverkarna och kommer att leda till ett växande antal tillförlitliga produkter och system med början av enkla produkter. Inrättandet av nationella organisationer som skall genomföra utvärderingar och utfärda certifikat kommer att stödja denna utveckling.

Sekretessbestämmelser anses av de flesta användare som mindre viktiga för ögonblicket. Det förhållandet kommer emellertid sannolikt att ändras i framtiden, när avancerade kommunikationstjänster och framför allt mobila tjänster blivit tillgängliga för alla.

3.4 *Behov, möjligheter och prioriteringar*

Det är väsentligt att så snart som möjligt utveckla förfaranden, standarder, produkter och verktyg som är lämpade för att trygga säkerheten, både för själva informationssystemen (datorer, kringutrustning) och för de allmänt tillgängliga telenäten. Hög prioritet bör ges åt autenticering, åtkomstskydd och mottagningsbevis. Pilotprojekt bör genomföras för att fastställa värdet av de föreslagna lösningarna. Lösningar på prioriterade behov i fråga om elektroniskt datautbyte (EDI) undersöks i TEDIS-programmet inom det mera allmänna innehållet i denna handlingsplan.

4. Handlingslinje IV – utveckling av specifikationer, standardisering, evaluering och certifiering i fråga om IT-säkerhet

4.1 *Uppgift*

Behovet av IT-säkerhet är omfattande och därför är gemensamma specifikationer och standarder av avgörande betydelse. Frånvaron av allmänt antagna standarder och specifikationer för IT-säkerhet kan utgöra ett viktigt hinder för framsteg i fråga om informationsbaserade processer och tjänster inom hela ekonomin och samhället. Åtgärder krävs också för att påskynda utvecklingen och användningen av teknik och standarder i flera besläktade områden för kommunikations- och datornät, som är av avgörande betydelse för användare, industri och förvaltningar.

4.2 *Mål*

Det krävs ansträngningar för att åstadkomma ett sätt att införa och stödja specifika säkerhetsfunktioner inom de allmänna områden som omfattas av OSI, ONP, ISDN/IBC och näthantering. De tekniker och metoder som krävs för verifiering, inklusive certifiering, och som skall leda till ömsesidigt godkännande är också förknippade med standardisering och specificering. Då så är möjligt skall internationellt antagna lösningar stödjas. Utvecklingen och användningen av datorsystem med säkerhetsfunktioner bör också uppmuntras.

4.3 *Status och tendenser*

Framför allt Förenta staterna har tagit viktiga initiativ med avseende på IT-säkerhetsfrågor. I Europa behandlas ämnet i samband med standardisering av informationsteknik och telekommunikation inom ETSI, och CEN/CENELEC, som förberedelse för CCITT- och ISO-arbete inom området.

Mot bakgrund av det växande intresset intensifieras verksamheten snabbt i Förenta staterna och både säljare och tjänsteproducenter ökar sina ansträngningar inom området. I Europa har Frankrike, Tyskland och Storbritannien oberoende av varandra påbörjat liknande verksamheter, men en gemensam insats som motsvarar arbetet i Förenta staterna utvecklas endast långsamt.

4.4 *Behov, möjligheter och prioriteringar*

När det gäller IT-säkerhet råder ett mycket nära samband mellan reglerande, driftmässiga, administrativa och tekniska aspekter. Föreskrifterna måste återspeglas i standarder, och bestämmelserna om IT-säkerhet måste på ett sätt som kan verifieras överensstämma med standarder och föreskrifter. I flera hänseenden kräver föreskrifterna specifikationer som går utanför den vanliga ramen för standardisering genom att innefatta branschspecifika överenskommelser. Behovet av standarder och branschregler föreligger inom alla områden då det gäller IT-säkerhet, och åtskillnad måste göras mellan sådana krav som motsvarar säkerhetsmålen och vissa tekniska följdkrav, som kan anförtros åt de behöriga europeiska standardiseringsorganen (CEN/CENELEC/ETSI).

Specifikationer och standarder måste omfatta objekten för säkerhetstjänsterna (personlig autenticering och företagsautenticering, registrering av mottagningsbevis, juridiskt godtagbara elektroniska bevis, behörighetskontroll), informationssystemens kommunikationstjänster (sekretess för bildkommunikation, sekretess för röst- och dataöverföring vid mobilkommunikation, skydd för databaser och bilddatabaser, tjänsteintegrerad säkerhet), administrationen av kommunikation och säkerhet (system med öppna och privata nycklar för drift av öppna nät, skydd för näthanteringen, skydd för tjänsteproducenter) och certifiering av dessa tjänster (säkerhetskriterier och säkerhetsnivåer, säkerhetsförfaranden för säkra informationssystem).

5. Handlingslinje V – teknisk och driftmässig utveckling av IT-säkerhet

5.1 *Uppgift*

En systematisk undersökning och utveckling av teknik för att möjliggöra ekonomiskt genomförbara och driftmässigt tillfredsställande lösningar för en rad nuvarande och framtida behov av IT-säkerhet är en förutsättning för tjänstemarknadens utveckling och för konkurrenskraften hos den europeiska ekonomin i sin helhet.

All teknisk utveckling i fråga om IT-säkerhet kommer att behöva innefatta både datorsäkerhet och kommunikationssäkerhet, eftersom de flesta nutida system är distribuerade och tillgång till sådana system erhålls genom kommunikationstjänster.

5.2 *Mål*

Systematisk undersökning och utveckling av tekniken för att möjliggöra ekonomiskt lönsamma och driftmässigt tillfredsställande lösningar i fråga om en rad nuvarande och framtida behov av IT-säkerhet.

5.3 *Behov, möjligheter och prioriteringar*

Arbetet med IT-säkerhet bör omfatta utvecklings- och genomförandestrategier, teknik samt integrering och verifiering.

Det strategiska forsknings- och utvecklingsarbetet bör omfatta begreppsmässiga modeller för säkra system (säkerhet mot skadegörelse och intrång, obehöriga modifieringar och förlust av tillgång till tjänsten), modeller för funktionskrav, riskmodeller och arkitekturer för säkerhet.

Det tekniskt orienterade forsknings- och utvecklingsarbetet bör innefatta användar- och meddelandeautenticering (t.ex. genom röstanalys och elektroniska signaturer), tekniska gränssnitt och protokoll för kryptering, mekanismer för accesskontroll och metoder för att implementera bevisligen säkra system.

Verifiering och validering av säkerheten i det tekniska systemet och dess användbarhet bör undersökas genom integrerings- och verifieringsprojekt.

Förutom konsolidering och utveckling av säkerhetstekniken, krävs ytterligare ett antal åtgärder som rör utvecklingen, underhållet och den konsekventa tillämpningen av standarder samt validering och certifiering av IT- och teleprodukter med avseende på deras säkerhetsegenskaper, inklusive validering och certifiering av metoderna för att utforma och införa system.

Gemenskapens tredje ramprogram för forskning, utveckling och teknik kan eventuellt användas för att främja samarbetsprojekt på nivåer som kommer före konkurrens och normering.

6. Handlingslinje VI – tillhandahållande av tjänster för IT-säkerhet

6.1 *Uppgift*

Beroende på den speciella karaktären hos säkerhetsfunktionerna i informationssystem kommer de erforderliga funktionerna att behöva införlivas i olika delar av informationssystemet såsom terminaler/datorer, tjänster, näthantering och dessutom krypteringsanordningar, aktiva kort, öppna och privata nycklar osv. En del av dessa funktioner kan förväntas vara inbyggda i den maskinvara eller programvara som tillhandahålls av leverantörerna medan andra kan vara en del av distribuerade system (t.ex. näthantering), vara i den enskilde användarens ägo (t.ex. aktiva kort) eller tillhandahållas av en specialiserad organisation (t.ex. öppna/privata nycklar).

Det kan förväntas att de flesta av säkerhetsprodukterna och säkerhetstjänsterna tillhandahålls av leverantörer, tjänsteproducenter eller operatörer. När det gäller speciella funktioner, t.ex. tillhandahållande av öppna/privata nycklar eller revisionsbehörighet kan det föreligga behov av att utse och bemyndiga lämpliga organisationer.

Detsamma gäller för certifiering, evaluering och verifikation av tjänstekvalitet, funktioner som måste skötas av organisationer vilka är neutrala i förhållande till leverantörers, tjänsteproducenters och operatörers intressen. Dessa organisationer kan vara privata eller statliga eller ha fått ett statligt tillstånd att fullgöra de uppgifter som delegerats till dem.

6.2 *Mål*

För att underlätta en harmonisk utveckling av hur IT-säkerhet tillhandahålls i gemenskapen till skydd för allmänhetens och affärslivets intressen, kommer det att bli nödvändigt att utveckla en enhetlig process för att uppnå denna säkerhet. Om uppdrag skall ges åt oberoende organisationer, skall deras funktioner och villkor definieras och antas genom överenskommelse och då så erfordras innefattas i ramen av föreskrifter. Målet bör vara att uppnå en klart definierad och överenskommen fördelning av ansvaret mellan de olika aktörerna på gemenskapsnivå som en förutsättning för ömsesidigt erkännande.

6.3 *Status och tendenser*

För närvarande är tillgången på IT-säkerhet väl organiserad endast inom vissa områden och begränsad till att endast tillfredsställa specifika behov. Den organisation som finns på europanivå är för det mesta informell och ömsesidigt erkännande av verifiering och certifiering är ännu inte etablerad utanför slutna grupper. Med den ökande betydelsen av IT-säkerhet blir behovet av att definiera en enhetlig process för att tillhandahålla IT-säkerhet i Europa och internationellt alltmer brådskande.

6.4 *Behov, möjligheter och prioriteringar*

På grund av antalet olika berörda aktörer och de nära sambanden mellan regelfrågor och lagstiftning är det särskilt viktigt att i förväg komma överens om vilka principer som bör styra hur IT-säkerhet tillhandahålls.

Vid utvecklingen av en enhetlig process för att behandla denna fråga, kommer man att behöva ta ställning till de aspekter som berör identifiering och specifikation av funktioner som genom sin karaktär kräver att det finns tillgång till vissa oberoende organisationer (eller samarbetande organisationer). Detta skulle kunna inbegripa funktioner såsom administrationen av ett öppet/privat nyckelsystem.

Dessutom är det nödvändigt att på ett tidigt stadium identifiera och specificera de funktioner som i allmänhetens intresse måste anförtros åt oberoende organisationer (eller samarbetande organisationer). Detta skulle t.ex. kunna inbegripa revision, kvalitetssäkring, verifikation, certifiering och liknande funktioner.