RÅDETS AFGØRELSE

af 31. marts 1992

om informationssystemers sikkerhed

(92/242/EØF)

RÅDET FOR DE EUROPÆISKE FÆLLESSKABER HAR —

under henvisning til Traktaten om Oprettelse af Det Europæiske Økonomiske Fællesskab, særlig artikel 235,

under henvisning til forslag fra Kommissionen (1),

under henvisning til udtalelse fra Europa-Parlamentet (2),

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg (3), og

ud fra følgende betragtninger:

Fællesskabet har til opgave gennem oprettelsen af et fælles marked og gennem gradvis tilnærmelse af medlemsstaternes økonomiske politik at fremme en harmonisk udvikling af den økonomiske virksomhed i Fællesskabet som helhed, en varig og afbalanceret ekspansion, en øget stabilitet, en hurtigere højnelse af levestandarden og snævrere forbindelser mellem medlemsstaterne;

elektronisk lagring, behandling og formidling af information spiller en stadig større rolle for erhvervslivet og samfundet;

fremkomsten af en effektiv verdensomspændende kommunikation og den udstrakte brug af elektronisk behandling af information betyder, at behovet for en passende beskyttelse øges;

Europa-Parlamentet har i sine drøftelser og beslutninger ved flere lejligheder understreget vigtigheden af informationssystemers sikkerhed;

Det Økonomiske og Sociale Udvalg har fremhævet behovet for at behandle de aspekter, der vedrører informationssystemers sikkerhed i forbindelse med Fællesskabets foranstaltninger, blandt andet på baggrund af de virkninger, gennemførelsen af det indre marked må forventes at få;

foranstaltninger på nationalt, internationalt og EF-niveau udgør et godt udgangspunkt;

der er en nær forbindelse mellem telekommunikation, informationsteknologi, standardisering, informationsmarkedet og politikken vedrørende forskning og teknologisk udvikling (FTU) samt det arbejde, som Det Europæiske Fællesskab allerede har indledt på disse felter;

der bør ske en samordning af indsatsen på grundlag af allerede igangværende nationalt og internationalt arbejde og ved fremme af samarbejdet mellem hovedaktørerne; dette bør ske inden for rammerne af en sammenhængende handlingsplan;

informationssystemers sikkerhed omfatter mange forskellige aspekter, og der må derfor udarbejdes strategier, der dels sikrer fri bevægelighed for informationer i enhedsmarkedet, dels garanterer sikkerheden i anvendelsen af informationssystemer i hele Fællesskabet;

det er den enkelte medlemsstats ansvar at fastsætte de begrænsninger, der er nødvendige af hensyn til sikkerheden og den offentlige orden;

medlemsstaternes ansvar på dette område indebærer en samordnet indsats på grundlag af et snævert samarbejde med højtstående embedsmænd fra medlemsstaterne;

der er behov for en plan omfattende en handlingsplan for en indledende periode på 24 måneder og nedsættelse af et udvalg af højtstående embedsmænd med et langfristet mandat, der skal rådgive Kommissionen vedrørende foranstaltninger inden for informationssystemers sikkerhed;

et beløb på 12 mio. ECU skønnes nødvendigt til gennemførelsen af planen i en indledende periode på 24 måneder; de midler, der i 1992 skønnes nødvendige inden for de nuværende finansielle overslag, beløber sig til 2 mio. ECU;

de midler, der skal afsættes til finansiering af planen for tiden efter regnskabsåret 1992, skal ligge inden for Fællesskabets gældende finansieringsramme —

TRUFFET FØLGENDE AFGØRELSE:

Artikel 1

Der vedtages hermed en plan for informationssystemers sikkerhed, der omfatter:

— udvikling af overordnede strategier for informationssystemers sikkerhed (handlingsplan) for en indledende periode på 24 måneder, og

— nedsættelse af en gruppe af højtstående embedsmænd med et langfristet mandat, i det følgende benævnt »udvalget«, der skal rådgive Kommissionen vedrørende de foranstaltninger, der skal gennemføres inden for informationssystemers sikkerhed.

(1) EFT nr. C 277 af 5. 11. 1990, s. 18.
(2) EFT nr. C 94 af 13. 3. 1992.
(3) EFT nr. C 159 af 17. 6. 1991, s. 38.

Artikel 2

1. Kommissionen hører systematisk udvalget vedrørende spørgsmål om informationssystemers sikkerhed i forbindelse med de forskellige fællesskabsaktiviteter, navnlig vedrørende fastlæggelsen af arbejdsstrategier og -programmer.

2. Handlingsplanen omfatter som anført i bilag I forberedende arbejde på følgende områder:

I. Etablering af strategiske rammer for informationssystemers sikkerhed

II. Kortlægning af brugernes og tjenesteydernes behov med hensyn til informationssystemers sikkerhed

III. Løsninger for brugernes, leverandørernes og tjenesteydernes umiddelbare og midlertidige behov

IV. Udvikling af specifikationer, standardisering, evaluering og certificering i forbindelse med informationssystemers sikkerhed

V. Teknologisk og driftsmæssig udvikling inden for informationssystemers sikkerhed

VI. Tilvejebringelse af sikkerhed for informationssystemer.

Artikel 3

1. De fællesskabsmidler, der skønnes nødvendige til gennemførelse af planen i en indledende periode på 24 måneder, beløber sig til 12 mio. ECU, hvoraf 2 mio. ECU i 1992 inden for rammerne af de finansielle overslag for 1988 til 1992.

Midler til finansiering af den efterfølgende gennemførelse af planen skal ligge inden for Fællesskabets gældende finansieringsramme.

2. Budgetmyndigheden fastlægger de disponible bevillinger for hvert regnskabsår under hensyntagen til de i artikel 2 i finansforordningen vedrørende De Europæiske Fællesskabers almindelige budget omhandlede principper om forsvarlig økonomisk forvaltning.

Artikel 4

En gruppe uafhængige eksperter foretager på Kommissionens vegne en evaluering af de fremskridt, der er gjort i løbet af den indledende periode. Denne gruppes rapport samt eventuelle bemærkninger fra Kommissionen sendes til Europa-Parlamentet og Rådet.

Artikel 5

1. Kommissionen er ansvarlig for planens gennemførelse. Den bistås af et rådgivende udvalg, der består af repræsentanter for medlemsstaterne, og som har Kommissionens repræsentant som formand.

2. Handlingsplanen gennemføres i overensstemmelse med de mål, der er fastlagt i artikel 2, og ajourføres om nødvendigt. Den skal i detaljer beskrive, hvilke mål og foranstaltningstyper der skal gennemføres, og den skal indeholde en oversigt over, hvilke finansielle ordninger der skal gennemføres herfor. Kommissionen indkalder forslag på grundlag af handlingsplanen.

3. Handlingsplanen gennemføres i samarbejde med sektoraktørerne. Den tager hensyn til, fremmer og supplerer igangværende europæisk og internationalt standardiseringsarbejde på området.

Artikel 6

1. Fremgangsmåden i artikel 7 gælder for foranstaltninger vedrørende Fællesskabets politik inden for informationssystemers sikkerhed.

2. Fremgangsmåden i artikel 8 gælder for:

— udarbejdelse og ajourføring af handlingsplanen som omhandlet i artikel 5

— indholdet af indkaldelser af forslag, vurderingen af forslag og det anslåede beløb for Fællesskabets bidrag til foranstaltningerne, hvis dette beløb overstiger 200 000 ECU

— medvirken fra ikke-fællesskabsorganisationers side i aktiviteter, der er omfattet af denne afgørelse

— ordninger for spredning, beskyttelse og udnyttelse af resultaterne af foranstaltningerne

— de foranstaltninger, der skal træffes for at evaluere planen.

3. Hvis beløbet for Fællesskabets bidrag til foranstaltningerne er på 200 000 ECU eller derunder, hører Kommissionen udvalget om de foranstaltninger, der skal træffes, og underretter udvalget om resultatet af sin vurdering.

Artikel 7

Kommissionens repræsentant forelægger udvalget et udkast til de foranstaltninger, der skal træffes. Udvalget afgiver en udtalelse om dette udkast inden for en frist, som formanden kan fastsætte under hensyn til, hvor meget det pågældende spørgsmål haster, i givet fald ved afstemning.

Udtalelsen optages i mødeprotokollen; derudover har hver medlemsstat ret til at anmode om, at dens holdning indføres i mødeprotokollen.

Kommissionen tager størst muligt hensyn til udvalgets udtalelse. Den underretter udvalget om, hvorledes den har taget hensyn til dets udtalelse.

Artikel 8

Kommissionens repræsentant forelægger udvalget et udkast til de foranstaltninger, der skal træffes. Udvalget afgiver en udtalelse om dette udkast inden for en frist, som formanden kan fastsætte under hensyn til, hvor meget det pågældende spørgsmål haster. Det udtaler sig med det flertal, der er fastsat i Traktatens artikel 148,

stk. 2, for vedtagelse af de afgørelser, som Rådet skal træffe på forslag af Kommissionen. Ved afstemninger i udvalget tillægges de stemmer, der afgives af repræsentanterne for medlemsstaterne, den vægt, som er fastlagt i nævnte artikel. Formanden deltager ikke i afstemningen.

Kommissionen vedtager de påtænkte foranstaltninger, når de er i overensstemmelse med udvalgets udtalelse.

Er de påtænkte foranstaltninger ikke i overensstemmelse med udvalgets udtalelse, eller er der ikke afgivet nogen udtalelse, forelægger Kommissionen straks Rådet et forslag til de foranstaltninger, der skal træffes. Rådet træffer afgørelse med kvalificeret flertal.

Har Rådet ved udløbet af en frist på tre måneder regnet fra forslagets forelæggelse for Rådet ikke truffet nogen afgørelse, vedtages de foreslåede foranstaltninger af Kommissionen, medmindre Rådet med simpelt flertal har udtalt sig imod de nævnte foranstaltninger.

Udfærdiget i Bruxelles, den 31. marts 1992.

På Rådets vegne

Vitor MARTINS

Formand

BILAG

Resumé af aktionslinjerne

RETNINGSLINJER FOR EN HANDLINGSPLAN VEDRØRENDE INFORMATIONSSYSTEMERS SIKKERHED

INDLEDNING

Handlingsplanen har til formål at fastlægge overordnede strategier med henblikpå at yde brugere og producenter af elektronisk lagret, behandlet eller transmitteret information passende beskyttelse mod hændelige eller forsætlige trusler mod informationssystemer.

Handlingsplanen skal tage hensyn til og supplere det verdensomspændende standardiseringsarbejde, der er i gang på dette område.

Den skal omfatte følgende aktionslinjer:

— etablering af strategiske rammer for informationssystemers sikkerhed

— kortlægning af brugernes og tjenesteydernes behov med hensyn til informationssystemers sikkerhed

— løsninger for brugernes, leverandørernes og tjenesteydernes umiddelbare og midlertidige behov

— udvikling af specifikationer, standardisering, evaluering og certificering i forbindelse med informationssystemers sikkerhed

— teknologisk og driftsmæssig udvikling inden for informationssystemers sikkerhed

— tilvejebringelse af sikkerhed for informationssystemer.

Handlingsplanen gennemføres af Kommissionen i nær forbindelse med tilsvarende foranstaltninger i medlemsstaterne og sammen med tilsvarende fællesskabsforskning og udviklingsforanstaltninger.

1. Aktionslinje I — Etablering af strategiske rammer for informationssystemers sikkerhed

1.1. *Område*

Det erkendes, at informationssystemers sikkerhed er et grundlæggende behov i mange sammenhænge i det moderne samfund. Elektroniske informationstjenester gør sikre telekommunikationsinfrastrukturer, sikker hardware og software samt sikker brug og forvaltning påkrævet. Der bør etableres en overordnet strategi, der tager hensyn til alle aspekter af informationssystemers sikkerhed, således at en spredning mellem forskellige metoder undgås. Enhver strategi vedrørende sikkerhed i forbindelse med information, der behandles i elektronisk form, bør afspejle samfundets ønske om at fungere effektivt, samtidig med at det beskytter sig selv i en verden i hastig forandring.

1.2. *Mål*

Der bør fastlægges strategiske rammer, således at de samfundsmæssige, økonomiske og politiske mål kan forenes med de muligheder, der findes på teknisk, driftsmæssigt og lovgivningsmæssigt plan inden for Fællesskabet og i international sammenhæng. Der må findes en balance mellem de forskellige ønsker, målsætninger og begrænsninger. Dette bliver en opgave for sektoraktørerne gennem et samarbejde med sigte på fastlæggelse af et fælles synspunkt og en fælles strategisk ramme. Dette er en forudsætning for at kunne forene modstridende interesser og behov både inden for den politiske beslutningstagning og i forbindelse med industriens udvikling.

1.3. *Status og tendenser*

Situationen præges af en voksende erkendelse af, at der er behov for handling. Så længe der ikke foreligger foranstaltninger med sigte på at samordne indsatsen, er det sandsynligt, at der vil blive taget forskellige initiativer inden for de forskellige sektorer, og at dette konkret vil ytre sig i en situation med indbyrdes modsætninger, idet der efterhånden vil opstå alvorligere juridiske, samfundsmæssige og økonomiske problemer.

1.4. *Behov, muligheder og prioriteter*

Inden for sådanne fælles rammer må der tages stilling til risikoanalyse og risikostyring afhængigt af informationens og informationstjenesternes følsomhed, den indbyrdes tilnærmelse af lovgivninger og bestemmelser vedrørende forkert brug og misbrug af edb og telekommunikation, de administrative infrastrukturer, herunder sikkerhedspolitik, og hvorledes disse kan implementeres effektivt inden for de forskellige brancher/fagområder, samt samfundsmæssige aspekter og aspekter i forbindelse med kommunikationshemmeligheden (blandt andet spørgsmålet om identificerings-, autentificerings-, ikke-afvisnings- og eventuelt autorisationsordninger i et demokratisk miljø).

Der må opstilles klare bestemmelser for udarbejdelse af fysiske og logiske arkitekturer med sigte på sikre distribuerede informationstjenester, standarder, retningslinjer for og definitioner af garanteret sikre produkter og tjenester, pilotforsøg og prototyper til konstatering af gennemførligheden af de forskellige administrative strukturer, arkitekturer og standarder med henblik på specifikke sektorers behov.

Der må skabes opmærksomhed omkring sikkerhedsproblematikken med henblik på at gøre brugerne mere agtpågivende med hensyn til sikkerheden inden for informationsteknologi (IT).

2. Aktionslinje II — Kortlægning af brugernes og tjenesteydernes behov med hensyn til informationssystemers sikkerhed

2.1. *Område*

Informationssystemers sikkerhed er en klar forudsætning for integritet, applikationers pålidelighed inden for erhvervslivet, intellektuel ejendomsret og fortrolighed. Dette gør det vanskeligt at finde en balance i valget mellem ønsket om fri handel og ønsket om at sikre privatlivets fred og den intellektuelle ejendomsret. Disse valg og de dermed forbundne kompromisløsninger bør baseres på en fuldstændig vurdering af behovene og mulighederne for at udnytte forskellige løsninger for informationssystemers ikkerhed.

Brugerbehov indebærer, at infomationssystemernes sikkerhedsmæssige funktionaliteter afspejler de teknologiske, driftsmæssige og regulatoriske aspekter. Det vil sige, at en systematisk undersøgelse af de sikkerhedsmæssige behov i forbindelse med informationssystemer udgør en væsentlig del af arbejdet med at udvikle passende og effektive foranstaltninger.

2.2. *Mål*

Målet er at konstatere art og karakteristika for brugernes og tjenesteydernes behov samt disses forhold til informationssystemers sikkerhedsforanstaltninger.

2.2. *Status og tendenser*

Indtil nu er der ikke blevet gjort noget samordnet forsøg på at konstatere, hvilke behov hovedaktørerne har med hensyn til informationssystemers sikkerhed, idet disse behov udvikler og ændrer sig meget hurtigt. Fællesskabets medlemsstater har konstateret, at der er behov for harmonisering af de enkelte landes aktiviteter (specielt for så vidt angår sikkerhedskriterier for IT). Ensartede evalueringskriterier og regler for gensidig anerkendelse af evalueringscertifikater er af stor betydning.

2.2. *Behov, muligheder og prioriteter*

Som grundlag for en konsekvent og transparent behandling af sektoraktørernes behov bør der vedtages en klassificering af brugerbehovene og konsekvenserne af denne for etableringen af sikkerhed for informationssystemer.

Det betragtes også som vigtigt at få konstateret behovene for lovgivning, bestemmelser og kodekser på baggrund af en vurdering af tendenserne inden for tjenestekarakteristika og tjenesteteknologi, at få indkredset alternative strategier for, hvordan målsætningerne kan tilgodeses gennem administrative, tjenesterelaterede, driftsmæssige og tekniske bestemmelser, og at få vurderet, hvor effektive og brugervenlige samt hvor bekostelige eventuelle alternative løsninger med hensyn til informationssystemers sikkerhed og strategier for brugere, tjenesteleverandører og operatører vil være.

3. Aktionslinje III — Løsninger for brugernes, leverandørernes og tjenesteydernes umiddelbare og midlertidige behov

3.1. *Område*

Det er i dag muligt at beskytte datamater effektivt mod uvedkommendes indtrængen ved hjælp af »isolerende« foranstaltninger, dvs. ved hjælp af konventionelle organisatoriske og fysiske tiltag. Dette gælder også for elektronisk kommunikation inden for en lukket brugergruppe på et dedikeret net. Forholdene er meget anderledes, dersom informationen er fælles mellem brugergrupper, eller hvis den udveksles via et offentligt net eller et net, hvortil flere har adgang. I dette tilfælde mangler både teknologi, terminaler og tjenester, for slet ikke at nævne standarder og procedurer, hvorfor der ikke er mulighed for at opnå en tilsvarende informationssystemsikkerhed.

3.2. *Mål*

Målet skal være med kort varsel at fremskaffe løsninger, der kan tilgodese brugeres, tjenesteyderes og fabrikanters mest presserende behov. Dette indebærer, at der anvendes fælles sikkerhedsevalueringskriterier for IT. Disse bør opfattes som åbne over for fremtidige behov og løsninger.

3.3. *Status og tendenser*

Visse brugergrupper har udviklet forskellige former for teknik og procedurer til deres egne specifikke behov, blandt andet behovet for autentificering, integritet og »ikke-afvisning« (non-repudiation). Normalt anvendes der magnetkort eller smart kort (chipkort). Nogle anvender mere eller mindre sofistikeret krypteringsteknik. Dette indebærer ofte, at der må etableres brugergruppespecifikke »myndigheder«. Det er imidlertid vanskeligt at generalisere denne teknik og disse metoder, således at behovene i et mere åbent miljø kan tilgodeses.

ISO arbejder med OSI-informationssystemsikkerhed (ISO DIS 7498-2), og CCITT er også beskæftiget hermed inden for rammerne af X400. Det er også muligt at indsætte informationssikkerhedssegmenter i meddelelser. Autentificering, integritet og ikke-afvisning behandles som led i meddelelser (EDIFACT) og som en del af X400 MHS.

De retlige rammer omkring elektronisk dataudveksling (EDI) er endnu ikke fuldt fastlagt. Det Internationale Handelskammer har fastlagt ensartede regler i en kodeks for udveksling af handelsdata via telenet.

Flere lande (f.eks. Frankrig, Tyskland, Det Forenede Kongerige og USA) er i færd med at fastlægge eller har allerede fastlagt kriterier for evaluering af IT- og telekommunikationsprodukters og -systemers troværdighed og procedurer for gennemførelse af evalueringer. Disse kriterier er blevet koordineret med landenes egne fabrikanter og vil resultere i et voksende antal pålidelige produkter og systemer, i første omgang simplere produkter. Oprettelsen af nationale organisationer til gennemførelse af evalueringer og udstedelse af certifikater vil støtte denne tendens.

Bestemmelser vedrørende fortrolighedsaspektet betragtes af de fleste brugere som knap så vigtige i første omgang. Det må imidlertid forventes, at dette vil ændre sig i fremtiden, efterhånden som avancerede kommunikationstjenester, herunder specielt mobiltjenester, bliver mere almindelige.

3.4. *Behov, muligheder og prioriteter*

Det er vigtigt, at der snarest muligt etableres procedurer, standarder, produkter og værktøjer til beskyttelse af sikkerheden dels i selve informationssystemerne (datamater, periferiudstyr), dels i offentlige kommunikationsnet. Autentificering, integritet og ikke-afvisning bør prioriteres højt. Der bør udføres pilotprojekter til konstatering af, om de foreslåede løsninger er de bedste. Løsninger på prioriteringsbehov vedrørende EDI er genstand for undersøgelse inden for TEDIS-programmet som led i denne handlingsplans mere generelle indhold.

4. Aktionslinje IV — Udvikling af specifikationer, standardisering, evaluering og certificering i forbindelse med informationssystemers sikkerhed

4.1. *Område*

Behovet for sikkerhed for informationssystemer er alment, og ensartede specifikationer og standarder er derfor af afgørende betydning. Mangelen på standarder og specifikationer for IT-sikkerhed kan være en stor hindring for indførelsen af informationsbaserede processer og tjenester i erhvervslivet og i samfundet som helhed. Der må også tages skridt til en hurtigere udvikling og brug af teknologi og standarder inden for flere indbyrdes beslægtede kommunikations- og datamatnetsområder, der er af kritisk betydning for brugerne, industrien og det offentlige.

4.2. *Mål*

Der bør gøres en indsats for at understøtte og varetage specifikke sikkerhedsfunktioner inden for generelle områder, såsom OSI, ONP, ISDN/IBC og netstyring. Verifikationsteknik og -metoder er tæt knyttede til standardisering og specificering, herunder certificering med henblik på gensidig anerkendelse. Hvor det er muligt, skal internationalt vedtagne løsninger støttes. Man bør ligeledes fremme udviklingen og anvendelsen af edb-systemer med sikkerhedsfunktioner.

4.3. *Status og tendenser*

Navnlig i USA har man taget væsentlige initiativer med henblik på informationssystemers sikkerhed. I Europa behandles spørgsmålet inden for standardiseringen på IT- og telekommunikationsområdet af blandt andre ETSI og CEN/Cenelec som forberedelse af CCITT's og ISO's arbejde på området.

På baggrund af de tiltagende betænkeligheder på dette felt sker der for øjeblikket en hastig udbygning af arbejdet i USA, og både handlende og tjenesteydere er i færd med at intensivere deres indsats på området. I Europa har Frankrig, Tyskland og Det Forenede Kongerige uafhængigt af hinanden indledt tilsvarende aktiviteter. En samlet indsats på linje med den amerikanske er dog kun langsomt ved at komme i stand.

4.4. *Behov, muligheder og prioriteter*

Inden for informationssystemers sikkerhed er der en naturlig tæt sammenhæng mellem regulerende, driftsmæssige, administrative og tekniske aspekter. Regulativer må udmøntes i standarder, og bestemmelser vedrørende informationssystemsikkerheden må på kontrollerbar måde være i overensstemmelse med standarder og regulativer. I flere henseender kræver regulativerne specifikationer, der går ud over standardiseringens konventionelle sigte, idet de f.eks. kan indeholde adfærdskodekser. Behovet for standarder og adfærdskodekser er til stede inden for alle områder af informationssystemers sikkerhed, og der må skelnes mellem de beskyttelseskrav, der beror på sikkerhedsmålsætningen, og de tekniske krav, der kan varetages af de europæiske standardiseringsorganer med beføjelser på området (CEN/Cenelec/ETSI).

Specifikationer og standarder må omfatte sikkerhedstjenester for informationssystemer (autentificering af personer og virksomheder, protokoller for ikke-afvisning, juridisk bindende elektronisk bevis, autorisationskontrol), disses kommunikationstjenester (kommunikationshemmelighed for billeder og for mobilkommunikation af tale og data, beskyttelse af data/billedbaser, beskyttelse af integrerede tjenester), disses kommunikations- og sikkerhedsstyring (systemer baseret på offentlig/privat nøgle inden for åbne net, beskyttelse af netstyring, beskyttelse af tjenesteydere) samt certificering heraf (kriterier og niveauer for beskyttelse af informationssikkerheden, procedurer for sikkerhedsbeskyttelse af sikrede informationssystemer).

4. Aktionslinje V — Teknologisk og driftsmæssig udvikling inden for informationssystemers sikkerhed

5.1. *Formål*

Systematisk udforskning og udvikling af teknologien med henblik på økonomisk rentable og driftsmæssigt tilfredsstillende løsninger på en række nutidige og fremtidige behov for informationssystemers sikkerhed er en forudsætning for at kunne udvide tjenestemarkedet og forbedre konkurrenceevnen inden for den europæiske industri som helhed betragtet.

Enhver form for teknologisk udvikling af informationssystemernes sikkerhed på nødvendigvis indbefatte såvel datamatsikkerhed som kommunikationssikkerhed, idet de fleste moderne systemer er distribuerede systemer, hvortil man får adgang via kommunikationstjenesterne.

5.2. *Mål*

Målet er en systematisk udforskning og udvikling af teknologien med henblik på økonomisk rentable og driftsmæssigt tilfredsstillende løsninger på en række nutidige og fremtidige behov med hensyn til informationssystemers sikkerhed.

5.3. *Behov, muligheder og prioriteter*

Arbejdet inden for informationssystemers sikkerhed må omfatte udviklings- og implementeringsstrategi, teknologi, integration og verificering.

Det strategiske FU-arbejde må indbefatte konceptuelle modeller til sikre systemer (sikre mod kompromiser, ubeføjede ændringer og afvisning af adgang til tjenesten), modeller for funktionsbehov, risikomodeller og sikkerhedsorienterede arkitekturer.

Det teknologiske FU-arbejde bør omfatte bruger- og meddelelsesautentificering (f.eks. ved hjælp af stemmeanalyse og elektronisk underskrift), tekniske grænseflader og protokoller for kryptering, adgangskontrolordninger og metoder til implementering af efterprøveligt sikre systemer.

Verificering og validering af tekniske systemers sikkerhed og anvendeligheden heraf skal udforskes inden for integrations- og verificeringsprojekter.

Ud over konsolidering og udvikling af sikkerhedsteknologi er det påkrævet med en række ledsageforanstaltninger af hensyn til udarbejdelse, vedligeholdelse og korrekt anvendelse af standarder, samt validering og certificering af IT- og telekommunikationsprodukter med hensyn til deres sikkerhedsegenskaber, herunder validering og certificering af metoder til udformning og implementering af systemer.

Fællesskabets tredje rammeprogramm for FTU kan eventuelt finde anvendelse med henblik på at fremme samarbejdsbaserede projekter på prækompetitivt og prænormativt niveau.

6. Aktionslinje VI — Tilvejebringelse af sikkerhed for informationssystemer

6.1. *Område*

Afhængigt af den nøjagtige karakter af informationssystemernes sikkerhedssystemer er der behov for inkorporering af sikkerhedsfunktioner i forskellige dele af informationssystemet, blandt andet terminaler og datamater, tjenester, netstyring, krypteringsanordninger, smart kort, offentlige og private nøgler osv. Nogle af disse funktioner kan forventes indbygget i hardware og software af producenterne, mens andre kan indgå som en del af distribuerede systemer (f.eks. netstyring), være i den enkelte brugers besiddelse (f.eks. smart kort) eller stilles til rådighed af særlige organisationer (f.eks. offentlige/private nøgler).

Det kan forventes, at de fleste sikkerhedsprodukter vil blive stillet til rådighed af producenter, tjenesteleverandører og operatører. Med hensyn til specifikke funktioner (f.eks. etablering af offentlige/private nøgler, revision og autorisation) kan det blive nødvendigt at udpege og bemyndige særlige organisationer.

Det samme gælder med hensyn til certificering, evaluering og verificering af tjenestens kvalitet, dvs. funktioner, der må kontrolleres af organisationer, der er uafhængige af producenternes, tjenesteleverandørernes og operatørernes interesser. Disse organisationer kan være private, statslige eller være koncessioneret af det offentlige med henblik på varetagelse af bestemte uddelegerede funktioner.

6.2. *Mål*

For at sørge for, at informationssystemers sikkerhed stilles til rådighed i Fællesskabet på harmonisk måde, således at offentlighedens og erhvervslivets interesser tilgodeses, må der fastlægges en kohærent fremgangsmåde for, hvorledes dette skal ske. I de tilfælde, hvor der må udpeges uafhængige organisationer, må deres funktioner og vilkår fastlægges og vedtages og i givet fald indføjes i en forskriftsmæssig ramme. Målet bør være at nå frem til en klart defineret og alment accepteret fordeling af ansvaret mellem de forskellige aktører på fællesskabsniveau som en forudsætning for gensidig anerkendelse.

6.3. *Status og tendenser*

I dag er informationssystemernes sikkerhed kun tilgodeset på specifikke områder, og normalt kun med sigte på tilfredsstillelse af specifikke behov. Tilrettelæggelsen heraf på europæisk niveau er for det meste af uformel art, og man har endnu ikke etableret gensidig anerkendelse af verifikation og certificering uden for visse lukkede grupper. Med informationssystemssikkerhedens voksende betydning begynder der at opstå et presserende behov for at få fastlagt en kohærent fremgangsmåde med hensyn til, hvorledes informationssystemssikkerheden skal tilgodeses i Europa og på internationalt plan.

6.4. *Behov, muligheder og prioriteter*

Da der er mange forskellige aktører involveret, og der er en nær tilknytning til spørgsmål af forskriftsmæssig og lovgivningsmæssig art, er det meget vigtigt på forhånd at nå til enighed om, hvilke principper der bør lægges til grund for informationssystemers sikkerhed.

For at kunne behandle dette spørgsmål er det nødvendigt at tage stilling til forskellige aspekter, herunder indkredsning og specificering af, hvilke funktioner der på grund af deres karakter gør det påkrævet, at der står uafhængige organisationer (eller samarbejdende organisationer) til rådighed. Herunder hører eventuelt funktioner som administration af et system for offentlige/private nøgler.

Endvidere er det nødvendigt i en tidlig fase at undersøge og fastslå, hvilke funktioner der i almenhedens interesse bør overlades til uafhængige organisationer (eller samarbejdende organisationer). Dette kan blandt andet omfatte revision, kvalitetsstyring, verificering, certificering og lignende funktioner.