BESLUIT VAN DE RAAD

van 31 maart 1992

betreffende de beveiliging van informatiesystemen

(92/242/EEG)

DE RAAD VAN DE EUROPESE GEMEENSCHAPPEN,

Gelet op het Verdrag tot oprichting van de Europese Economische Gemeenschap, inzonderheid op artikel 235,

Gezien het voorstel van de Commissie (1),

Gezien het advies van het Europese Parlement (2),

Gezien het advies van het Economisch en Sociaal Comité (3),

Overwegende dat de Gemeenschap tot taak heeft door het instellen van een gemeenschappelijke markt en door het geleidelijk nader tot elkaar brengen van het economisch beleid van de Lid-Staten de harmonische ontwikkeling van de economische activiteit binnen de gehele Gemeenschap, een gestadige en evenwichtige expansie, een grotere stabiliteit, een toenemende verbetering van de levensstandaard en nauwere betrekkingen tussen de in de Gemeenschap verenigde Staten te bevorderen ;

Overwegende dat elektronisch opgeslagen, verwerkte en verzonden informatie bij economische en sociale activiteiten een steeds belangrijker rol vervult ;

Overwegende dat de komst van efficiënte, alomvattende communicatie en de wijdverbreide toepassing van elektronische informatieverwerking adequate bescherming dringend noodzakelijk maken ;

Overwegende dat het Europese Parlement in zijn beraadslagingen en resoluties herhaaldelijk het belang van de beveiliging van informatiesystemen heeft onderstreept ;

Overwegende dat het Economisch en Sociaal Comité beklemtoond heeft dat op het gebied van de beveiliging van informatiesystemen communautaire acties moeten worden ondernomen, met name met het oog op de gevolgen van de verwezenlijking van de interne markt ;

Overwegende dat acties op nationaal, internationaal en communautair niveau een goede basis vormen ;

Overwegende dat er een nauw verband is tussen telecommunicatie, informatietechnologie, normalisatie, de informatiemarkt en het onderzoek- en technologische ontwikkelingsbeleid, alsmede het werk dat de Europese Gemeenschap reeds op deze gebieden heeft ondernomen ;

Overwegende dat voor coördinatie van inspanningen dient te worden gezorgd door op bestaande nationale en internationale werkzaamheden voort te bouwen en door de samenwerking tussen de voornaamste betrokken partijen te bevorderen ; dat men derhalve in het kader van een coherent actieplan te werk dient te gaan ;

Overwegende dat de complexiteit van de beveiliging van informatiesystemen vereist dat strategieën worden ontwikkeld om het vrije verkeer van informatie in de ongedeelde markt mogelijk te maken en tegelijkertijd de veiligheid van het gebruik van informatiesystemen in de gehele Gemeenschap te verzekeren ;

Overwegende dat het aan elke Lid-Staat staat rekening te houden met de eisen in verband met veiligheid en openbare orde ;

Overwegende dat de verantwoordelijkheid van de Lid-Staten op dit terrein een gecoördineerde benadering gebaseerd op een nauwe samenwerking met hoge ambtenaren van de Lid-Staten nodig maakt ;

Overwegende dat er een actie nodig is die voorziet in een actieplan voor een eerste periode van vierentwintig maanden en in de oprichting van een comité van hoge ambtenaren met een langlopend mandaat dat de Commissie moet adviseren over maatregelen betreffende beveiliging van informatiesystemen ;

Overwegende dat voor de uitvoering van de actie voor een eerste periode van vierentwintig maanden een bedrag van 12 miljoen ecu noodzakelijk wordt geacht ; dat het noodzakelijk geachte bedrag voor 1992, in het kader van de huidige financiële vooruitzichten, 2 miljoen ecu bedraagt ;

Overwegende dat de bedragen die voor de financiering van het programma moeten worden vastgelegd voor de periode na het begrotingsjaar 1992, moeten worden ingepast in het dan geldende communautaire financiële kader,

BESLUIT :

Artikel 1

Hierbij wordt een actie betreffende de beveiliging van informatiesystemen aangenomen die het volgende behelst :

— de ontwikkeling van algemene strategieën ter beveiliging van informatiesystemen („actieplan") voor een eerste periode van vierentwintig maanden ;

— de oprichting van een groep van hoge ambtenaren met een langlopend mandaat die de Commissie moet adviseren over maatregelen betreffende de beveiliging van informatiesystemen, hierna te noemen „het Comité".

(1) PB nr. C 277 van 5. 11. 1990, blz. 18.
(2) PB nr. C 94 van 13. 3. 1992.
(3) PB nr. C 159 van 17. 6. 1991, blz. 38.

Artikel 2

1. De Commissie raadpleegt het Comité systematisch over de met de beveiliging van informatiesystemen verband houdende aspecten van de verschillende communautaire activiteiten, meer bepaald over de opstelling van werkstrategieën en -programma's.

2. Het in de bijlage uiteengezette actieplan omvat voorbereidende werkzaamheden op de volgende gebieden :

I. Ontwikkeling van een algemene strategie voor de beveiliging van informatiesystemen ;

II. Vaststelling van de behoeften van gebruikers en dienstverleners inzake de beveiliging van informatiesystemen ;

III. Oplossingen voor de behoeften op korte en middellange termijn van gebruikers, leveranciers en dienstverleners ;

IV. Ontwikkeling van specificaties, normen, evaluatie en certificatie op het gebied van de beveiliging van informatiesystemen ;

V. Technologische en operationele ontwikkelingen inzake de beveiliging van informatiesystemen ;

VI. Voorzieningen ter beveiliging van informatiesystemen.

Artikel 3

1. De voor de tenuitvoerlegging van de actie noodzakelijk geachte communautaire financiële middelen bedragen voor een eerste periode van vierentwintig maanden 12 miljoen ecu, waarvan 2 miljoen ecu voor 1992 in het kader van de financiële vooruitzichten 1988-1992.

Voor de verdere periode van uitvoering van het programma moet het bedrag in het dan geldende communautaire financiële kader worden ingepast.

2. De begrotingsautoriteit stelt de voor elke begrotingsjaar beschikbare kredieten vast, rekening houdend met de beginselen van goed beheer bedoeld in artikel 2 van het Financieel Reglement van toepassing op de algemene begroting van de Europese Gemeenschappen.

Artikel 4

Aan het eind van de eerste periode laat de Commissie de bereikte vooruitgang evalueren door een groep onafhankelijke deskundigen. Het verslag van deze groep wordt, samen met eventuele opmerkingen van de Commissie, aan het Europese Parlement en aan de Raad voorgelegd.

Artikel 5

1. De Commissie is voor de uitvoering van het actieplan verantwoordelijk. Zij wordt bijgestaan door een raadgevend comité bestaande uit vertegenwoordigers van de Lid-Staten en voorgezeten door de vertegenwoordiger van de Commissie.

2. Het actieplan wordt uitgevoerd overeenkomstig de doelstellingen van artikel 2 en zo nodig bijgewerkt. In dit actieplan worden de gedetailleerde doelstellingen, de te voeren typen acties en de daarvoor te treffen financiële voorzieningen aangegeven. De Commissie doet op grond van het actieplan uitnodigingen tot het indienen van voorstellen uitgaan.

3. Het actieplan wordt uitgevoerd in nauwe samenwerking met de betrokken partijen, waarbij de normalisatiewerkzaamheden zoals die zich op Europees en op internationaal vlak ontwikkelen, in aanmerking worden genomen, bevorderd en aangevuld.

Artikel 6

1. De procedure van artikel 7 is van toepassing op maatregelen met betrekking tot het communautaire beleid op het gebied van de beveiliging van informatiesystemen.

2. De procedure van artikel 8 is van toepassing op :

— de voorbereiding en bijwerking van het in artikel 5 bedoelde actieplan ;

— de inhoud van de uitnodigingen tot het indienen van voorstellen, de beoordeling van de voorstellen en de geraamde communautaire bijdrage aan maatregelen wanneer deze bijdrage meer bedraagt dan 200 000 ecu ;

— de inbreng van niet-communautaire organisaties in de onder het besluit vallende activiteiten ;

— regelingen voor het verspreiden, beschermen en gebruiken van de resultaten van de maatregelen ;

— de maatregelen die genomen moeten worden om de actie te evalueren.

3. Wanneer het bedrag van de communautaire bijdrage aan de maatregelen kleiner is dan of gelijk aan 200 000 ecu, raadpleegt de Commissie het Comité over de te nemen maatregelen en brengt zij het Comité op de hoogte van haar evaluatie.

Artikel 7

De vertegenwoordiger van de Commissie legt het Comité een ontwerp voor van de te nemen maatregelen. Het Comité brengt binnen een termijn die de voorzitter kan vaststellen naar gelang van de urgentie van de materie advies uit over dit ontwerp, zo nodig door middel van een stemming.

Het advies wordt in de notulen opgenomen ; voorts heeft iedere Lid-Staat het recht te verzoeken dat zijn standpunt in de notulen wordt opgenomen.

De Commissie houdt zoveel mogelijk rekening met het door het Comité uitgebrachte advies. Zij brengt het Comité op de hoogte van de wijze waarop zij rekening heeft gehouden met zijn advies.

Artikel 8

De vertegenwoordiger van de Commissie legt het Comité een ontwerp voor van de te nemen maatregelen. Het Comité brengt advies uit over dit ontwerp binnen een termijn die de voorzitter kan vaststellen naar gelang van de urgentie van de materie. Het Comité spreekt zich uit

met de meerderheid van stemmen die in artikel 148, lid 2, van het Verdrag is voorgeschreven voor de aanneming van de besluiten die de Raad op voorstel van de Commissie dient te nemen. Bij de stemming in het Comité worden de stemmen van de vertegenwoordigers van de Lid-Staten gewogen overeenkomstig genoemd artikel. De voorzitter neemt niet aan de stemming deel.

De Commissie stelt de beoogde maatregelen vast wanneer zij in overeenstemming zijn met het advies van het Comité.

Wanneer de beoogde maatregelen niet in overeenstemming zijn met het advies van het Comité of indien geen advies is uitgebracht, dient de Commissie onverwijld bij de Raad een voorstel in betreffende de te nemen maatregelen. De Raad besluit met gekwalificeerde meerderheid van stemmen.

Indien de Raad drie maanden na de indiening van het voorstel bij de Raad geen besluit heeft genomen, worden de voorgestelde maatregelen door de Commissie vastgesteld, behalve wanneer de Raad zich met gewone meerderheid van stemmen tegen genoemde maatregelen heeft uitgesproken.

Gedaan te Brussel, 31 maart 1992.

Voor de Raad

De Voorzitter

Vitor MARTINS

BIJLAGE

Overzicht van de actielijnen

RICHTLIJNEN VOOR EEN ACTIEPLAN INZAKE DE BEVEILIGING VAN INFORMATIE-SYSTEMEN

INLEIDING

Het actieplan heeft ten doel algemene strategieën te ontwikkelen die de gebruikers en producenten van elektronisch opgeslagen, verwerkte of verstuurde informatie passende bescherming van de informatiesystemen moeten bieden tegen toevallige of opzettelijke dreigingen.

Het actieplan houdt rekening met en vormt een aanvulling op de normalisatiewerkzaamheden die zich op dit gebied op wereldniveau ontwikkelen.

Het plan omvat de volgende actielijnen :

— ontwikkeling van een algemene strategie voor de beveiliging van informatie-systemen ;

— vaststelling van de behoeften van gebruikers en dienstverleners inzake de beveiliging van informatiesystemen ;

— oplossingen voor de behoeften op korte en middellange termijn van gebruikers, leveranciers en dienstverleners ;

— ontwikkeling van specificaties, normen, evaluatie en certificatie op het gebied van de beveiliging van informatiesystemen ;

— technologische en operationele ontwikkelingen inzake de beveiliging van informatiesystemen ;

— voorzieningen ter beveiliging van informatiesystemen.

Het actieplan wordt uitgevoerd door de Commissie in nauwe samenhang met aanverwante acties in de Lid-Staten en aanverwante communautaire acties betreffende onderzoek en ontwikkeling.

1. Actielijn I — Ontwikkeling van een algemene strategie voor de beveiliging van informatiesystemen

1.1. *Probleem*

In een moderne samenleving wordt de beveiliging van informatiesystemen als algemeen noodzakelijk beschouwd. Voor elektronische informatiediensten zijn een veilige telecommunicatie-infrastructuur, veilige hardware en software en een veilig gebruik en beheer vereist. Er moet een algemene, alle aspecten van de beveiliging van informatiesystemen omvattende strategie komen, terwijl een fragmentarische aanpak moet worden vermeden. Elke strategie voor de beveiliging van elektronisch verwerkte informatie moet rekening houden met het streven van elke samenleving naar zowel doelmatigheid als bescherming in een snel veranderende wereld.

1.2. *Doelstelling*

Er moet een strategisch kader worden opgebouwd, dat sociale, economische en politieke doelstellingen weet te verenigen met de technische, operationele en juridische opties waarover de Gemeenschap in een internationale context beschikt. Dit delicate evenwicht tussen uiteenlopende bekommernissen, doelstellingen en beperkingen moet worden gevonden door de betrokken partijen, die te zamen een gemeenschappelijke visie en een onderling overeengekomen strategisch kader zullen moeten ontwikkelen. Aan deze voorwaarden moet worden voldaan om de belangen en behoeften op het vlak van de uitstippeling van een beleid en van de industriële ontwikkelingen met elkaar te verzoenen.

1.3. *Stand van zaken en te verwachten ontwikkelingen*

Er is een groeiend besef dat er opgetreden moet worden. Indien echter geen poging wordt gedaan om de krachten te bundelen, ligt het voor de hand dat verschillende sectoren los van elkaar maatregelen gaan nemen, waardoor tegenstrijdige feitelijke ontwikkelingen op gang zullen komen die geleidelijk steeds ernstiger juridische, maatschappelijke en economische problemen zullen veroorzaken.

1.4. *Behoeften, opties en prioriteiten*

Binnen dit gemeenschappelijk strategisch kader zal moeten worden gekeken naar de risicoanalyse en het risicobeheer met betrekking tot de kwetsbaarheid van de informatie- en aanverwante diensten, de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen betreffende misbruik en verkeerd gebruik van computers en/of telecommunicatie, de administratieve infrastructuren, waaronder het beveiligingsbeleid en de vraag hoe dit op doeltreffende wijze kan worden ten uitvoer gelegd in de verschillende bedrijfstakken en/of takken van wetenschap, en de maatschappelijke en privacy-aspecten (b.v. de toepassing van identificatie-, authentisering-, niet-afwijzings- en eventueel autorisatieregelingen in een democratische omgeving).

Er moeten duidelijke lijnen worden aangegeven voor de ontwikkeling van fysieke en logische architecturen voor veilige gedistribueerde informatiediensten, normen, richtlijnen en definities voor gewaarborgde beveiligingsprodukten en -diensten, proefprojecten en prototypes ten einde de haalbaarheid te kunnen vaststellen van de verschillende administratieve structuren, architecturen en normen die bij de behoeften van specifieke sectoren aansluiten.

Er moet een grotere bewustwording op het gebied van beveiliging worden gekweekt waardoor gebruikers zich meer betrokken zullen voelen bij de beveiliging van informatietechnologie (IT).

2. Actielijn II — Vaststelling van de behoeften van gebruikers en dienstverleners inzake de beveiliging van informatiesystemen

2.1. *Probleem*

De veiligheid van informatiesystemen is een absoluut vereiste voor integriteit en betrouwbaarheid van zakelijke toepassingen, intellectuele eigendom en vertrouwelijkheid van gegevens. Een en ander heeft tot gevolg dat er een moeilijke afweging en soms keuzes moeten worden gemaakt tussen vrije handel en het streven naar bescherming van de persoonlijke levenssfeer en van intellectuele eigendom. Deze keuzes en compromissen moeten gebaseerd zijn op een volledige evaluatie van de behoeften en het effect van de mogelijke informatiebeveiligingsopties die daaraan moeten voldoen.

Gebruikersbehoeften impliceren functionaliteiten ter beveiliging van informatiesystemen die verweven zijn met technologische, operationele en regelgevingsaspecten. Derhalve vormt een systematisch onderzoek naar de behoeften met betrekking tot de beveiliging van informatiesystemen een essentieel onderdeel van de ontwikkeling van passende en doeltreffende maatregelen.

2.2. *Doelstelling*

Vaststelling van de aard en kenmerken van behoeften van gebruikers en dienstverleners en hun relatie tot maatregelen voor de beveiliging van informatiesystemen.

2.3. *Stand van zaken en verwachte ontwikkelingen*

Tot nu toe is niet getracht om in gezamenlijk overleg de zich snel ontwikkelende en veranderende behoeften van de voornaamste betrokkenen op het gebied van de beveiliging van informatiesystemen vast te stellen. De Lid-Staten van de Gemeenschap hebben de behoeften aan harmonisatie van nationale activiteiten (inzonderheid van de „evaluatiecriteria voor IT-beveiliging") bepaald. Uniforme evaluatiecriteria en regels voor de wederzijdse erkenning van evaluatiecertificaten zijn van groot belang.

2.4. *Behoeften, opties en prioriteiten*

Als basis voor een logische en doorzichtige behandeling van de rechtmatige behoeften van de betrokkenen moet een overeengekomen classificatie worden ontwikkeld van gebruikersbehoeften, alsmede de relatie daarvan met voorzieningen ter beveiliging van informatiesystemen.

Verder wordt het van belang geacht de behoeften inzake wettelijke en bestuursrechtelijke bepalingen en gedragscodes vast te stellen in het licht van een evaluatie van de trends op het gebied van kenmerken en technologie van de diensten, alternatieve strategieën uit te stippelen voor de realisering van de doelstellingen voor administratieve, dienst-, operationele en technische bepalingen, en de doeltreffendheid, gebruikersvriendelijkheid en kosten te beoordelen van alternatieve opties en strategieën ter beveiliging van informatiesystemen ten behoeve van gebruikers, dienstverleners en exploitanten.

3. Actielijn III — Oplossingen voor de behoeften op korte en middellange termijn van gebruikers, leveranciers en dienstverleners

3.1. *Probleem*

Momenteel is het mogelijk computers afdoende te beschermen tegen ongeautoriseerde toegang van buitenaf door „isolatie", dit wil zeggen door toepassing van conventionele, organisatorische en fysieke maatregelen. Dit geldt ook voor elektronische communicatie binnen een besloten gebruikersgroep die een specifiek netwerk gebruikt. De situatie ligt heel anders als de informatie wordt gedeeld door verschillende gebruikersgroepen of wordt uitgewisseld via een openbaar of algemeen toegankelijk netwerk. In het algemeen beschikt men niet over de technologie, terminals en diensten, noch over de bijbehorende normen en procedures om in deze gevallen voor een vergelijkbare beveiliging van de informatiesystemen te zorgen.

3.2. *Doelstelling*

Doelstelling is om op korte termijn oplossingen te bieden voor de meest dringende behoeften van de gebruikers, dienstverleners en fabrikanten ; dit impliceert het gebruik van gemeenschappelijke evaluatiecriteria voor ITbeveiliging. De opzet daarvan moet zoveel mogelijk aansluiting bieden voor toekomstige behoeften en oplossingen.

3.3. *Stand van zaken en te verwachten ontwikkelingen*

Sommige gebruikersgroepen hebben technieken en procedures ontwikkeld voor eigen gebruik die met name zijn afgestemd op de behoefte aan identificatie, integriteit en niet-afwijzing. Over het algemeen worden magneetkaarten of chipkaarten gebruikt. Sommigen gebruiken min of meer verfijnde cryptografische technieken. Vaak betekende dit dat er voor gebruikersgroepen specifieke „autorisaties" moesten worden gedefinieerd. Het is echter moeilijk om deze technieken en methoden te veralgemenen en geschikt te maken voor een open omgeving.

De ISO werkt aan OSI-informatieveiligheid (ISO DIS 7498-2) en de CCITT in het kader van het X 400. Het is ook mogelijk informatieveiligheidssegmenten in de berichten in te voegen. Het authentiseren, de integriteit en de niet-afwijzing worden bekeken als onderdeel van de berichten (Edifact) en als onderdeel van het X 400 MHS.

Het wettelijke kader voor de EDI (elektronische gegevensuitwisseling) verkeert momenteel nog in het ontwerpstadium. De Internationale Kamer van Koophandel heeft uniforme gedragsregels uitgevaardigd voor de uitwisseling van handelsgegevens via telecommunicatienetten.

Een aantal landen, waaronder Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten, hebben criteria ontwikkeld voor de evaluatie van de betrouwbaarheid van IT- en telecommunicatieprodukten en -systemen en de bijbehorende procedures voor de uitvoering van die evaluaties, of zijn daar mee bezig. Deze criteria zijn opgesteld in samenwerking met de nationale fabrikanten en zullen leiden tot een toenemend aantal betrouwbare produkten en systemen, te beginnen met eenvoudige produkten. De oprichting van nationale organisaties die evaluaties uitvoeren en certificaten afgeven, zullen deze ontwikkeling ondersteunen.

Vertrouwelijkheid wordt door de meeste gebruikers niet beschouwd als een eerste vereiste. Deze houding zal in de toekomst waarschijnlijk veranderen, wanneer het gebruik van geavanceerde communicatiediensten en met name mobiele diensten algemeen is geworden.

3.4. *Behoeften, opties en prioriteiten*

Het is van essentieel belang zo spoedig mogelijk de procedures, normen, produkten en gereedschappen te ontwikkelen die geschikt zijn om voor de beveiliging van zowel informatiesystemen als zodanig (computers, randapparatuur) als openbare communicatienetten te zorgen. Hoge prioriteit moet worden gegeven aan authentisering, integriteit en niet-afwijzing. Er moeten proefprojecten worden uitgevoerd om de bruikbaarheid van de voorgestelde oplossingen vast te stellen. Binnen de meer algemene opzet van dit actieplan wordt in het kader van het Tedis-programma gezocht naar oplossingen voor de prioritaire behoeften bij EDI.

4. Actielijn IV — Ontwikkeling van specificaties, normen, evaluatie en certificatie op het gebied van de beveiliging van informatiesystemen

4.1. *Probleem*

De behoefte aan beveiliging van informatiesystemen is algemeen en daarom zijn gemeenschappelijke specificaties en normen van essentieel belang. Het ontbreken van overeengekomen normen en spectificaties voor IT-beveiliging kan een ernstige belemmering vormen voor de vooruitgang op het gebied van op informatie gebaseerde processen en diensten in de hele economie en de hele samenleving. Acties zijn ook nodig om de ontwikkeling en toepassing van technologie en normen te versnellen op een aantal met communicatie- en computernetwerk verband houdende gebieden die van essentieel belang zijn voor gebruikers, industrie en administraties.

4.2. *Doelstelling*

Er zijn inspanningen nodig om middelen te vinden voor het ondersteunen en verrichten van specifieke beveiligingsfuncties op de algemene gebieden OSI, ONP, ISDN/IBC en netwerkbeheer. Nauw verbonden met normalisatie en specificatie zijn de voor verificatie vereiste technieken en benaderingen, met inbegrip van certificatie die leidt tot wederzijdse erkenning. Waar mogelijk moet steun worden gegeven aan internationaal overeengekomen oplossingen. De ontwikkeling en het gebruik van computersystemen met beveiligingsfuncties moet eveneens worden aangemoedigd.

4.3. *Stand van zaken en te verwachten ontwikkelingen*

Vooral in de Verenigde Staten is een belangrijke aanzet gegeven op het gebied van de beveiliging van informatiesystemen. In Europa wordt deze problematiek behandeld in het kader van IT- en telecommunicatienormalisatie door ETSI en CEN/Cenelec ter voorbereiding van CCITT en ISO-werkzaamheden op dit gebied.

Gezien de groeiende bezorgdheid worden de werkzaamheden in de Verenigde Staten snel opgevoerd en zowel fabrikanten als dienstverleners verhogen hun inspanningen op dit gebied. In Europa zijn los van elkaar soortgelijke activiteiten van start gegaan in Frankrijk, Duitsland en het Verenigd Koninkrijk, maar een gemeenschappelijke inspanning zoals die in de Verenigde Staten komt slechts langzaam op gang.

4.4. *Behoeften, opties en prioriteiten*

De regelgevende, operationele, administratieve en technische aspecten van de beveiliging van informatiesystemen zijn nauw met elkaar verweven. Voorschriften moeten tot uitdrukking komen in normen, en voorzieningen ter beveiliging van informatiesystemen moeten op een toetsbare wijze voldoen aan de normen en voorschriften. Onder een aantal aspecten vereist de regelgeving specificaties die verder gaan dan bij normalisatie gewoonlijk het geval is, en omvat zij gedragscodes. Op alle gebieden van de beveiliging van informatiesystemen bestaat behoefte aan normen en gedragscodes en er moet onderscheid worden gemaakt tussen de beschermingsbehoeften die overeenkomen met de beveiligingsdoelstellingen en bepaalde technische behoeften die aan de bevoegde Europese normalisatieorganisaties (CEN/Cenelec/ETSI) kunnen worden toevertrouwd.

De specificaties en normen moeten betrekking hebben op beveiligingsdiensten van informatiesystemen (persoons- en bedrijfsauthentisering, niet-afwijzingsprotocollen, wettelijk toegestaan elektronisch bewijs, autorisatiecontrole), hun communicatiediensten (privacy van beeldcommunicatie, privacy van stem en data bij mobiele communicatie, bescherming van data- en beelddatabase, beveiliging geïntegreerde diensten), hun communicatie en beveiligingsbeheer (openbaar/particulier centraal systeem voor opennetwerkbesturing, bescherming van netwerkbeheer, bescherming van dienstverleners) en hun certificatie (criteria en niveaus ter verzekering van de beveiliging van informatiesystemen, procedures ter verzekering van de beveiliging).

5. Actielijn V — Technologische en operationele ontwikkelingen inzake de beveiliging van informatiesystemen

5.1. *Probleem*

Systematisch O & O op technologisch gebied om economisch haalbare en operationeel bevredigende oplossingen te realiseren en daarmee te voldoen aan een reeks bestaande en toekomstige behoeften op het gebied van de beveiliging van informatiesystemen is een voorwaarde voor de ontwikkeling van de dienstenmarkt en de concurrentiekracht van de gehele Europese economie.

Alle technologische ontwikkelingen op het gebied van informatiesysteembeveiliging zullen zowel de computerbeveiliging als de communicatie-beveiliging moeten omvatten, aangezien de meeste systemen tegenwoordig gedistribueerde systemen zijn die toegankelijk zijn via communicatiediensten.

5.2. *Doelstelling*

Systematisch O & O op technologisch gebied om economisch haalbare en operationeel bevredigende oplossingen te vinden voor een reeks bestaande en toekomstige behoeften op het gebied van de beveiliging van informatiesystemen.

5.3. *Behoeften, opties en prioriteiten*

De werkzaamheden op het gebied van de beveiliging van informatiesystemen moeten betrekking hebben op ontwikkelings- en implementatiestrategieën, technologiën, alsmede integratie en verificatie.

De strategische O & O-werkzaamheden moeten betrekking hebben op ontwerpmodellen voor veilige systemen (beveiliging tegen compromis, ongeautoriseerde wijzigingen en onthouding van diensten), modellen van functionele eisen, risicomodellen en architecturen voor beveiliging.

De technologisch gerichte O & O-werkzaamheden moeten gebruikers- en berichtauthentisering omvatten (bij voorbeeld door stemanalyse en elektronische handtekeningen), technische interfaces en protocollen voor encryptie, toegangscontrolemechanismen en implementatiemethoden voor bewijsbaar veilige systemen.

In het kader van projecten op het gebied van integratie en verificatie moet onderzoek worden verricht naar verificatie en validering van de beveiliging van het technisch systeem en de toepasbaarheid ervan.

Naast consolidering en ontwikkeling van beveiligingstechnologie is een aantal begeleidende maatregelen nodig met betrekking tot de opstelling, het bijwerken en de consistente toepassing van normen, alsmede de validering en certificatie van IT- en telecommunicatieprodukten wat betreft hun veiligheidseigenschappen, met inbegrip van validering en certificatie van methoden voor het ontwerpen en implementeren van systemen.

Het derde kaderprogramma voor O & TO van de Gemeenschap kan misschien worden gebruikt voor het stimuleren van samenwerkingsprojecten op precommercieel en prenormatief vlak.

6. Actielijn VI — Voorzieningen ter beveiliging van informatiesystemen

6.1. *Probleem*

Afhankelijk van de precieze aard van de kenmerken van de beveiliging van informatiesystemen zullen de vereiste functies moeten worden ingebouwd in de verschillende delen van het informatiesysteem, dus in terminals/computers, diensten, netwerkbeheer, cryptografische apparatuur, chipkaarten, openbare en privé-sleutels, enz. Sommige functies zullen waarschijnlijk kunnen worden ingebed in de door leveranciers geleverde apparatuur of programmatuur, terwijl andere functies weer onderdeel zullen zijn van gedistribueerde systemen (bij voorbeeld netwerkbeheer), in het bezit zijn van individuele gebruikers (bij voorbeeld chipkaarten) of door een gespecialiseerde organisatie worden verschaft (bij voorbeeld openbare/privé-sleutels).

De meeste beveiligingsprodukten en -diensten zullen waarschijnlijk worden geleverd door fabrikanten, dienstverleners en exploitanten. Wat specifieke functies betreft, bij voorbeeld de verschaffing van openbare/privé-sleutels en auditing-autorisatie, zullen misschien bevoegde organisaties moeten worden aangewezen en van machtigingen voorzien.

Hetzelfde geldt voor certificatie, evaluatie en verificatie van de kwaliteit van diensten, zijnde functies die moeten vallen onder het beheer van organisaties die los staan van de belangen van fabrikanten, dienstverleners en exploitanten. Dit kunnen particuliere of overheidsorganisaties zijn dan wel organisaties die door de regering gemachtigd zijn gedelegeerde functies te verrichten.

6.2. *Doelstelling*

Met het oog op de bevordering van een harmonieuze ontwikkeling van de voorzieningen voor de beveiliging van informatiesystemen in de Gemeenschap ter bescherming van het publiek en van zakelijke belangen zal het nodig zijn een samenhangende aanpak op het betreffende gebied te ontwikkelen. Wanneer er machtiging van onafhankelijke organisaties nodig is, zullen functies en voorwaarden moeten worden omschreven en overeengekomen en indien nodig in een wettelijk kader worden ingebed. Men zou op communautair niveau moeten kunnen komen tot een duidelijk omschreven en overeengekomen verdeling van verantwoordelijkheden tussen de verschillende organisaties, hetgeen een vereiste is voor wederzijdse erkenning.

6.3. *Stand van zaken en te verwachten ontwikkelingen*

Momenteel zijn de voorzieningen ter beveiliging van informatiesystemen alleen goed georganiseerd voor specifieke gebieden en toegesneden op de specifieke behoeften daarvan. De organisatie op Europees niveau is meestal niet officieel en buiten besloten groepen is het nog niet gekomen tot wederzijdse erkenning van verificatie en certificatie. Gezien het steeds groter wordend belang van de beveiliging van informatiesystemen wordt de behoefte aan de bepaling van een samenhangende aanpak van de voorzieningen ter beveiliging van informatiesystemen op Europees en op internationaal vlak steeds dringender.

6.4. *Behoeften, opties en prioriteiten*

In verband met het grote aantal betrokkenen en de nauwe verwevenheid met wettelijke en bestuursrechtelijke vraagstukken is het van groot belang eerst tot overeenstemming te komen over de beginselen die ten grondslag moeten liggen aan de voorzieningen ter beveiliging van informatiesystemen.

Voor een samenhangende aanpak van deze kwestie moet worden nagegaan en aangegeven welke functies op grond van hun geaardheid zijn aangewezen op het voorhanden zijn van een onafhankelijke organisatie (of samenwerkende organisaties). Men zou hierbij kunnen denken aan functies als het beheer van een openbaar/privé-sleutelsysteem.

Daarnaast is het nodig om in een vroeg stadium na te gaan en aan te geven welke functies in het algemeen belang aan een onafhankelijke organisatie (of samenwerkende organisaties) moeten worden toevertrouwd. Men zou hierbij bij voorbeeld kunnen denken aan auditing, kwaliteitsborging, verificatie, certificatie en soortgelijke functies.