31992D0242

DECIZIA CONSILIULUI din 31 martie 1992 privind securitatea sistemelor de informare

(92/242/CEE)

CONSILIUL COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul de instituire a Comunității Economice Europene și, în special, articolul 235 al acestuia,

având în vedere propunerea Comisiei [1],

având în vedere avizul Parlamentului European [2],

având în vedere avizul Comitetului Economic și Social [3],

întrucât misiunea Comunității constă în promovarea unei dezvoltări armonioase a activităților economice în cadrul Comunității, a unei extinderi continue și echilibrate, a unei stabilități mărite, a unei creșteri accelerate a nivelului de trai și a unor relații mai strânse între statele membre, prin constituirea unei piețe comune și prin apropierea treptată a politicilor economice ale statelor membre;

întrucât informația păstrată, prelucrată și transmisă prin intermediul mijloacelor electronice dobândește o importanță tot mai mare în cadrul activității economice și sociale;

întrucât instituirea unor comunicații globale eficiente și utilizarea tot mai mare a prelucrării electronice a informației au pus un accent tot mai mare pe necesitatea oferirii unei protecții adecvate;

întrucât, în cadrul dezbaterilor și rezoluțiilor sale, Parlamentul European a pus accentul în repetate rânduri pe importanța securității sistemelor de informare;

întrucât Comitetul Economic și Social a subliniat necesitatea abordării problemelor privind securitatea sistemelor de informare în acțiunile Comunității, îndeosebi în vederea impactului realizării pieței interne;

întrucât acțiunile la nivel național, internațional și comunitar oferă o bază adecvată;

întrucât există o relație strânsă între telecomunicații, tehnologiile informației, standardizare, piața informației și politicile de cercetare și dezvoltare tehnologică (C-DT), precum și între lucrările întreprinse deja în aceste domenii de către Comunitate;

întrucât eforturile trebuie concertate prin valorificarea lucrărilor existente la nivel național și internațional și prin promovarea cooperării între principalele părți interesate; întrucât este oportun, prin urmare, să se acționeze în cadrul unui plan de acțiune coerent;

întrucât complexitatea securității sistemelor de informare necesită elaborarea unor strategii care să permită libera circulație a informației în interiorul pieței unice, asigurând totodată securitatea utilizării sistemelor de informare în cadrul Comunității;

întrucât este de datoria fiecărui stat membru să țină seama de constrângerile impuse de securitatea și ordinea publică;

întrucât responsabilitățile statelor membre în acest domeniu presupun o abordare concertată bazată pe o colaborare strânsă cu înalții funcționari ai statelor membre;

întrucât trebuie prevăzută o acțiune care să includă un plan de acțiune pentru o perioadă inițială de douăzeci și patru de luni și crearea unui comitet al înalților funcționari investiți cu un mandat pe termen lung, pentru a consilia Comisia asupra acțiunilor în domeniul securității sistemelor de informare;

întrucât o sumă de 12 milioane ECU este estimată ca fiind necesară pentru punerea în aplicare a acțiunii pentru o perioadă inițială de douăzeci și patru de luni; întrucât, în 1992, în cadrul perspectivelor financiare actuale, suma estimată ca fiind necesară este de 2 milioane ECU;

întrucât sumele care urmează să fie contractate în vederea finanțării programului pentru perioada următoare anului bugetar 1992 trebuie să se înscrie în cadrul financiar comunitar în vigoare,

DECIDE:

Articolul 1

Prin prezenta decizie se adoptă o acțiune în domeniul securității sistemelor de informare. Aceasta cuprinde:

— dezvoltarea de strategii globale în vederea asigurării securității sistemelor de informare (plan de acțiune) pentru o perioadă inițială de douăzeci și patru de luni;

— constituirea unui grup de înalți funcționari învestiți cu un mandat pe termen lung, numit în continuare „comitet”, în vederea consilierii Comisiei asupra acțiunilor care trebuie întreprinse în domeniul securității sistemelor de informare.

[1] JO C 277, 5.11.1990, p. 18.
[2] JO C 94, 13.3.1992.
[3] JO C 159, 17.6.1991, p. 38.

Articolul 2

(1) Comisia consultă în mod sistematic comitetul asupra problemelor referitoare la securitatea sistemelor de informare pentru diferite activități desfășurate de Comunitate, în special în privința definirii strategiilor și programelor de lucru.

(2) Așa cum se prevede în anexă, planul de acțiune cuprinde lucrări de pregătire privind următoarele teme:

I. dezvoltarea unui cadru strategic pentru securitatea sistemelor de informare;

II. identificarea necesităților utilizatorilor și prestatorilor de servicii în ceea ce privește securitatea sistemelor de informare;

III. elaborarea de soluții pentru unele necesități pe termen scurt și mediu ale utilizatorilor, furnizorilor și prestatorilor de servicii;

IV. elaborarea de specificații, standardizarea, evaluarea și certificarea în ceea ce privește securitatea sistemelor de informare;

V. dezvoltări tehnologice și operaționale în ceea ce privește securitatea sistemelor de informații;

VI. punerea în aplicare a securității sistemelor de informare.

Articolul 3

(1) Suma estimată ca fiind necesară, din mijloacele financiare comunitare, pentru punerea în aplicare a acțiunii pe perioada inițială este de 12 milioane ECU, din care 2 milioane ECU pentru 1992, în cadrul perspectivelor financiare 1988-1992.

Pentru perioada ulterioară de aplicare a programului, suma va trebui să se înscrie în cadrul financiar comunitar în vigoare.

(2) Autoritatea bugetară stabilește creditele disponibile pentru fiecare exercițiu financiar, ținând seama de principiile bunei gestiuni prevăzute la articolul 2 din regulamentul financiar care se aplică bugetului general al Comunităților Europene.

Articolul 4

Un grup de experți independenți efectuează, pentru Comisie, o evaluare a progreselor realizate în cursul perioadei inițiale. Raportul acestui grup, însoțit de eventuale observații ale Comisiei, este prezentat Parlamentului European și Consiliului.

Articolul 5

(1) Comisia este responsabilă pentru punerea în aplicare a acțiunii. Ea este asistată de un comitet consultativ compus din reprezentanții statelor membre și prezidat de reprezentantul Comisiei.

(2) Planul de acțiune este pus în aplicare în conformitate cu obiectivele prevăzute la articolul 2 și actualizat ori de câte ori este nevoie. Acesta prezintă obiectivele detaliat și tipurile de acțiuni care trebuie întreprinse, precum și aranjamentele financiare aferente. Comisia lansează cereri de oferte pe baza planului de acțiune.

(3) Planul de acțiune este pus în aplicare în strânsă colaborare cu operatorii din sector. El ține seama, promovează și completează activitățile de standardizare desfășurate la nivel european și internațional în acest domeniu.

Articolul 6

(1) Procedura prevăzută la articolul 7 se aplică

— măsurilor care au legătură cu politica comunitară în domeniul securității sistemelor de informare.

(2) Procedura prevăzută la articolul 8 se aplică:

— elaborării și actualizării planului de acțiune prevăzut la articolul 5;

— conținutului cererilor de oferte, evaluării ofertelor și valorii estimate a contribuției comunitare la măsuri, atunci când aceasta depășește 200 000 ECU;

— cooperării în orice activitate a organizațiilor necomunitare, în temeiul prezentei decizii;

— modalităților de difuzare, protecție și exploatare a rezultatelor măsurilor;

— măsurilor ce urmează să fie adoptate pentru evaluarea acțiunii.

(3) Atunci când valoarea contribuției comunitare pentru aceste măsuri este mai mică sau egală cu 200 000 ECU, Comisia consultă comitetul în privința măsurilor ce urmează să fie adoptate și îl informează de rezultatul evaluării sale.

Articolul 7

Reprezentantul Comisiei prezintă comitetului un proiect privind măsurile ce urmează să fie adoptate. Comitetul își dă avizul cu privire la acest proiect în termenul pe care președintele îl poate stabili în funcție de urgența subiectului în cauză, dacă este necesar prin vot.

Avizul este consemnat în procesul-verbal; în afară de aceasta, fiecare stat membru are dreptul să solicite ca poziția sa să fie consemnată în procesul-verbal.

Comisia ține seama în cea mai mare măsură de avizul emis de comitet. Aceasta informează comitetul despre modul în care avizul este luat în considerare.

Articolul 8

Reprezentantul Comisiei prezintă comitetului un proiect privind măsurile ce urmează să fie adoptate. Comitetul își dă avizul cu privire la acest proiect în termenul pe care președintele îl poate stabili în funcție de urgența subiectului în cauză. Avizul se adoptă cu majoritatea prevăzută la articolul 148 alineatul (2) din tratat

pentru adoptarea deciziilor pe care Consiliul trebuie să le ia la propunerea Comisiei. În cadrul comitetului, voturile reprezentanților statelor membre sunt ponderate în conformitate cu articolul menționat anterior. Președintele nu participă la vot.

Comisia adoptă măsurile preconizate în cazul în care acestea sunt conforme cu avizul comitetului.

Atunci când măsurile preconizate nu sunt conforme cu avizul comitetului sau în absența avizului, Comisia prezintă Consiliului, fără întârziere, o propunere cu privire la măsurile ce trebuie adoptate. Consiliul hotărăște cu majoritate calificată.

În cazul în care, la expirarea unui termen de trei luni de la data la care i-a fost prezentată propunerea, Consiliul nu adoptă nici o măsură, Comisia adoptă măsurile propuse și le pune în aplicare de îndată, cu excepția cazului în care Consiliul s-a pronunțat cu majoritate simplă împotriva măsurilor în cauză.

Adoptată la Bruxelles, 31 martie 1992.

Pentru Consiliu

Președintele

Vitor MARTINS

ANEXĂ

Rezumatul liniilor de acțiune

ORIENTĂRI PENTRU UN PLAN DE ACȚIUNE ÎN DOMENIUL SECURITĂȚII SISTEMELOR DE INFORMARE

INTRODUCERE

Planul de acțiune are ca obiectiv dezvoltarea strategiilor globale prin care să li se ofere utilizatorilor și producătorilor de informații păstrate, prelucrate sau transmise în format electronic o protecție adecvată a sistemelor de informații împotriva amenințărilor accidentale sau voluntare.

Planul de acțiune ține cont de activitățile de standardizare desfășurate la nivel mondial în acest domeniu și le completează.

Planul cuprinde următoarele linii de acțiune:

— dezvoltarea unui cadru strategic pentru securitatea sistemelor de informare;

— identificarea necesităților utilizatorilor și prestatorilor de servicii în ceea ce privește securitatea sistemelor de informare;

— elaborarea de soluții pentru unele necesități pe termen scurt și mediu ale utilizatorilor, furnizorilor și prestatorilor de servicii;

— elaborarea de specificații, standardizarea, evaluarea și certificarea în ceea ce privește securitatea sistemelor de informare;

— dezvoltări tehnologice și operaționale în ceea ce privește securitatea sistemelor de informații;

— punerea în aplicare a securității sistemelor de informare.

Planul de acțiune este pus în aplicare de Comisie, în strânsă legătură cu acțiunile conexe din statele membre și coroborat cu acțiunile comunitare de cercetare și dezvoltare în domeniu.

1. **Linia de acțiune I: dezvoltarea unui cadru strategic pentru securitatea sistemelor de informare**

1.1. *Problemă*

Securitatea sistemelor de informare este recunoscută drept o calitate necesară pretutindeni într-o societate modernă. Sistemele computerizate de informații necesită infrastructuri de telecomunicații sigure, materiale și programe de calculator securizate, precum și condiții de utilizare și de gestionare sigure. Trebuie stabilită o strategie globală, ținând cont de toate aspectele securității sistemelor de informare, evitând orice abordare fragmentară. Orice strategie privind securitatea informației prelucrate electronic trebuie să țină cont de dorința fiecărei societăți de a acționa eficient, protejându-se totodată, într-o lume care se schimbă rapid.

1.2. *Obiectiv*

Trebuie stabilit un cadru strategic pentru corelarea obiectivelor sociale, economice și politice cu alegerile tehnice, operaționale și juridice ale Comunității într-un context internațional. Operatorilor din sector care lucrează împreună la dezvoltarea unei percepții comune și a unui cadru strategic convenit le revine sarcina să găsească echilibrul delicat între diverse preocupări, obiective și constrângeri. Este vorba de o cerință preliminară pentru a concilia interesele și necesitățile atât în ceea ce privește definirea unei politici, cât și dezvoltarea industrială.

1.3. *Situație și tendințe*

Situația este caracterizată prin conștientizarea crescândă a nevoii de a acționa. Cu toate acestea, în absența unei inițiative de coordonare a eforturilor, este foarte probabil că eforturile dispersate în diverse sectoare ar crea o situație *de facto* contradictorie, care în timp să creeze mai multe probleme juridice, sociale și economice.

1.4. *Necesități, opțiuni și priorități*

Un asemenea cadru ar trebui să trateze și să examineze analiza și gestiunea riscului din punctul de vedere al vulnerabilității sistemelor de informare și al serviciilor aferente, armonizarea actelor cu putere de lege privind utilizarea abuzivă și improprie a tehnologiei informației și a telecomunicațiilor, a infrastructurilor administrative, inclusiv a politicilor de securitate, precum și modul în care acestea pot fi efectiv puse în practică de către diverse industrii și discipline, preocupările sociale și de protecție a vieții private (de exemplu utilizarea sistemelor de identificare, autentificare, neinterzicere a accesului și eventual de autorizare într-un mediu democratic).

Trebuie furnizate orientări clare pentru elaborarea de arhitecturi fizice și logice pentru servicii de informare distribuite sigur, standarde, linii directoare și definiții pentru produse și servicii de securitate garantate, proiecte pilot și prototipuri, în scopul asigurării viabilității diverselor structuri administrative, precum și arhitecturi și norme privind necesitățile sectoarelor specifice.

Trebuie încurajată conștientizarea problemelor de securitate, astfel încât utilizatorii să fie încurajați să manifeste o grijă sporită pentru securitate în domeniul tehnologiei informației (IT).

2. Linia de acțiune II: identificarea necesităților utilizatorilor și prestatorilor de servicii în ceea ce privește securitatea sistemelor de informare

2.1. *Problemă*

Securitatea sistemelor de informare este condiția intrinsecă a integrității și credibilității aplicațiilor comerciale, a proprietății intelectuale și a confidențialității. Aceasta ridică problema echilibrului delicat – și uneori a alegerii – între susținerea libertății schimburilor pe de o parte și protecția vieții private și a proprietății intelectuale, pe de altă parte. Alegerea și compromisul trebuie să se facă pe baza aprecierii globale a necesităților și a impactului opțiunilor adoptate în domeniul securității sistemelor de informare cu scopul de a satisface aceste necesități.

Utilizatorii au nevoie de funcții de securitate a sistemelor de informație legate de aspectele tehnologice, operaționale și de reglementare. O muncă de cercetare sistematică privind necesitățile de securitate a sistemelor de informare este, în consecință, esențială pentru elaborarea de măsuri adecvate și eficiente.

2.2. *Obiectiv*

Trebuie stabilită natura și caracteristicile necesităților utilizatorilor și prestatorilor de servicii și relațiile acestora cu măsurile privind securitatea sistemelor de informare.

2.3. *Situație și tendințe*

Până în prezent nu a fost întreprins nici un efort concertat în vederea identificării necesităților, aflate într-o evoluție rapidă, ale principalilor operatori din domeniul securității sistemelor de informare. Anumite state membre ale Comunității au identificat necesitățile de armonizare a activităților naționale (în special „criterii de evaluare a securității IT"). Criteriile și regulile de evaluare uniforme pentru recunoașterea reciprocă a certificatelor de evaluare sunt de o importanță vitală.

2.4. *Necesități, opțiuni și priorități*

Pentru a aborda într-o formă coerentă și transparentă necesitățile justificate ale operatorilor din sector, este necesară elaborarea unei clasificări convenite a necesităților utilizatorilor și a relațiilor acestora cu punerea în practică a securității sistemelor de informare.

De asemenea, este importantă identificarea necesităților privind legislația, reglementările și codurile de conduită, în lumina evaluării tendințelor în ceea ce privește caracteristicile și tehnologia serviciilor, definirea altor strategii care să permită atingerea obiectivelor prin intermediul dispozițiilor administrative, de serviciu, operaționale și tehnice și evaluarea eficacității, a ușurinței de utilizare și a costurilor opțiunilor și strategiilor de înlocuire în domeniul securității sistemelor de re pentru utilizatori, prestatori de servicii și comercianți.

3. Linia de acțiune III: elaborarea de soluții pentru unele necesități pe termen scurt și mediu ale utilizatorilor, furnizorilor și prestatorilor de servicii

3.1. *Problemă*

Astăzi, accesul neautorizat, din exterior, la calculatoare poate fi împiedicat în mod eficient, folosind măsuri de „izolare", adică măsuri tradiționale pe plan organizațional și fizic. Același lucru este valabil pentru comunicațiile electronice în interiorul unui grup închis de utilizatori care operează într-o rețea dedicată. Situația este cu totul alta atunci când informația este împărțită de diferite grupuri de utilizatori sau circulă printr-o rețea publică sau cu acces general. În astfel de cazuri, tehnologia, echipamentele terminale și serviciile, pe de o parte, și normele și procedurile asociate, pe de altă parte, nu sunt de obicei în măsură să asigure o securitate de un nivel comparabil sistemelor de informare.

3.2. *Obiectiv*

Obiectivul trebuie să fie furnizarea, într-un timp scurt, a unor soluții care pot să răspundă necesităților imediate ale utilizatorilor, prestatorilor de servicii și producătorilor. Aceasta implică utilizarea unor criterii comune de evaluare a securității IT. Aceste criterii trebuie concepute astfel încât să rămână deschise necesităților și soluțiilor viitoare.

3.3. *Situație și tendințe*

Unele grupuri de utilizatori au elaborat, pentru uzul propriu, tehnici și proceduri care răspund în special necesităților de autentificare, integritate și neinterzicere a accesului. În general sunt folosite carduri magnetice sau cu memorie. Unii folosesc tehnici mai mult sau mai puțin sofisticate de criptografie. Acestea implică deseori definirea „autorităților" specifice grupurilor de utilizatori. Cu toate acestea, este dificilă generalizarea acestor tehnici și metode pentru a răspunde necesităților unui mediu deschis.

ISO lucrează la o securitate a sistemelor de informare OSI (ISO DIS 7498-2), precum și la CCITT în contextul lui X 400. De asemenea, se pot insera segmente de securitate în mesaje. Autentificarea, integritatea și neinterzicerea accesului sunt tratate ca părți ale mesajelor (EDI – FACT) și ale X 400 MHS.

La ora actuală, cadrul juridic EDI (Electronic Data Interchange) este încă în stadiu de concept. Camera Internațională de Comerț a publicat reguli de conduită uniforme pentru schimburile de date comerciale prin rețelele de comunicații.

Mai multe țări (de exemplu Germania, Franța, Regatul Unit și Statele Unite ale Americii) au pus la punct sau elaborează criterii pentru evaluarea credibilității produselor și sistemelor IT, precum și procedurile corespondente pe baza cărora să se efectueze evaluări. Aceste criterii au fost coordonate cu producătorii naționali și vor da naștere unei game lărgite de produse și sisteme fiabile, începând cu produsele simple. Această tendință va fi susținută de înființarea de organizații naționale responsabile cu efectuarea evaluărilor și acordarea de certificări.

Cea mai mare parte a utilizatorilor consideră că dispozițiile referitoare la confidențialitate sunt de o importanță mai redusă. Cu toate acestea, este probabil ca această opinie să se schimbe în viitor din cauza unei foarte largi răspândiri a serviciilor de comunicație avansate, în special a serviciilor mobile.

3.4. *Necesități, opțiuni și priorități*

Este esențială dezvoltarea, cât mai curând cu putință, procedurilor, standardelor, produselor și instrumentelor capabile să asigure securitatea sistemelor de informare ca atare (computere, periferice) și a rețelelor publice de comunicații. Trebuie acordată prioritate autentificării, integrității și neinterzicerii accesului. Ar trebui puse în aplicare proiecte pilot pentru stabilirea validității soluțiilor propuse. Soluțiile care se adresează unor necesități prioritare în domeniul EDI sunt cercetate în cadrul programului Tedis și coordonate în cadrul mai vast al prezentului plan de acțiune.

4. Linia de acțiune IV: elaborare de specificații, standardizare, evaluare și certificare în ceea ce privește securitatea sistemelor de informare

4.1. *Problemă*

Necesitățile referitoare la securitatea sistemelor de informare se fac simțite peste tot, iar din acest motiv existența unor specificații și standarde comune este crucială. Absența standardelor și specificațiilor convenite pentru securitatea IT ar putea constitui un obstacol major în calea evoluției proceselor și serviciilor bazate pe informație în ansamblul economiei și al societății. Trebuie, de asemenea, luate măsuri pentru accelerarea elaborării și utilizării unei tehnologii și a standardelor în mai multe domenii conexe comunicațiilor și rețelelor informatizate de importanță capitală pentru utilizatori, industrie și administrații.

4.2. *Obiectiv*

Sunt necesare eforturi pentru susținerea și realizarea funcțiilor de securitate specifice în domeniile generale ale OSI, ONP, RNIS/IBC și al administrării rețelelor. Tehnicile și abordările referitoare la verificare, inclusiv certificarea ce conduce la o recunoaștere reciprocă, sunt în mod intrinsec legate de standardizare și specificație. Ori de câte ori este posibil, trebuie susținute soluții adoptate la nivel internațional. De asemenea, trebuie încurajate punerea la punct și utilizarea de sisteme informatice dotate cu funcții de securitate.

4.3. *Situație și tendințe*

Statele Unite ale Americii, în special, au lansat inițiative importante pentru soluționarea problemei securității sistemelor de informare. În Europa, acest subiect este tratat în contextul standardizării TIT în cadrul ETSI și CEN/Cenelec, în pregătirea lucrărilor CCITT și ISO în acest domeniu.

În vederea preocupărilor tot mai susținute, munca Statelor Unite ale Americii se intensifică rapid și atât distribuitorii, cât și prestatorii de servicii își sporesc eforturile în acest domeniu. În Europa, Franța, Germania și Regatul Unit au inițiat activități similare în mod independent, dar un efort comun asemănător celui din Statele Unite se dezvoltă lent.

4.4. *Necesități, opțiuni și priorități*

În domeniul securității sistemelor de informare, aspectele de reglementare, operaționale, administrative și tehnice se află, în mod inerent, într-o strânsă legătură. Standardele trebuie să reflecte reglementările și să poată demonstra că dispozițiile privind securitatea sistemelor de informare respectă standardele și reglementările. Din mai multe aspecte, reglementările trebuie să includă specificații care să depășească obiectivul tradițional al standardizării, respectiv includerea de coduri de conduită. Exigențe referitoare la standarde și coduri de conduită există în toate sectoarele securității sistemelor de informare și trebuie să se facă deosebirea între cerințele de protecție corespunzătoare obiectivelor de securitate și anumite cerințe tehnice care pot fi încredințate organismelor europene de standardizare competente (CEN/Cenelec/ETSI).

Specificațiile și standardele trebuie să acopere domeniile serviciilor de securitate a sistemelor de informare (autentificarea persoanelor și întreprinderilor, protocoale de nerespingere, dovadă electronică valabilă din punct de vedere juridic, controlul de autorizare), serviciile lor de comunicație (respectarea vieții private în ceea ce privește comunicarea de imagini, voce și date, protecția băncilor de imagini și de date, securitatea serviciilor integrate), gestionarea comunicării și a securității acestora (sisteme de parole publice/private pentru funcționarea rețelelor deschise, protecția administrării rețelelor, protecția prestatorilor de servicii) și certificarea lor (criterii și niveluri de asigurare, proceduri de asigurare a securității sistemelor de informare).

5. Linia de acțiune V: dezvoltarea tehnologică și operațională în ceea ce privește securitatea sistemelor de informare

5.1. *Problemă*

O condiție necesară pentru dezvoltarea pieței serviciilor și competitivității economiei europene în ansamblu este desfășurarea unei munci de cercetare și dezvoltare tehnologică sistematică care să permită găsirea de răspunsuri viabile din punct de vedere economic și satisfăcătoare din punct de vedere operațional pentru o serie de necesități prezente și viitoare în ceea ce privește securitatea sistemelor de informare.

Orice dezvoltare tehnologică în ceea ce privește securitatea sistemelor de informare va trebui să aibă în vedere concomitent securitatea informatică și securitatea comunicațiilor, în măsura în care cea mai mare parte a sistemelor actuale sunt sisteme distribuite la care accesul este asigurat prin servicii de comunicații.

5.2. *Obiectiv*

O muncă de cercetare și dezvoltare tehnologică sistematică care să permită găsirea de răspunsuri viabile din punct de vedere economic și satisfăcătoare din punct de vedere operațional pentru o serie de necesități prezente și viitoare în ceea ce privește securitatea sistemelor de informare.

5.3. *Necesități, opțiuni și priorități*

Lucrările în ceea ce privește securitatea sistemelor de informare ar trebui să se refere la strategiile de dezvoltare și de punere în aplicare, la tehnologii, precum și la integrare și verificare.

Munca strategică de C-DT ar trebui să includă studiul modelelor conceptuale ale sistemelor sigure (sigure din punctul de vedere al modificărilor neautorizate și al interdicției de serviciu), al modelelor de exigențe funcționale, al modelelor de risc și al arhitecturilor pentru securitate.

Munca de C-DT ar trebui să includă autentificarea utilizatorului și a mesajului (de exemplu prin analiza vocii sau a semnături electronice), interfețele tehnice și protocoale de codificare, mecanisme de control al accesului și metode de punere în aplicare în vederea obținerii de sisteme sigure garantate.

Verificarea și validarea securității sistemului tehnic și aplicabilitatea acestuia sunt studiate prin intermediul proiectelor de integrare și de verificare.

Pe lângă consolidarea și dezvoltarea tehnologiei securității, sunt necesare anumite măsuri de sprijin privind crearea, actualizarea și aplicare coerentă a standardelor, precum și validarea și certificarea produselor de IT din punctul de vedere al proprietăților acestora în ceea ce privește securitatea, inclusiv verificarea și certificarea metodelor de proiectare și punere în aplicare a sistemelor.

Al treilea program cadru comunitar de C-DT ar putea fi utilizat pentru promovarea proiectelor de cooperare la nivelele preconcurențial și prestandardizare.

6. **Linia de acțiune VI: punerea în aplicare a securității sistemelor de informare**

6.1. *Problemă*

În funcție de natura exactă a elementelor de securitate ale sistemelor de informare, trebuie integrate funcțiile necesare în diferite puncte ale sistemelor de informații, mergând de la terminale, servicii, administrarea rețelelor, până la dispozitive criptografice, carduri cu memorie, parole de acces public și privat etc. Unele dintre aceste funcții vor fi probabil încorporate în materialul sau în programele de calculator oferite de distribuitori, în timp ce altele vor putea face parte din sistemele distribuite (de exemplu administrarea rețelelor) sau vor putea fi în posesia utilizatorilor individuali (de exemplu cardurile cu memorie) sau vor putea fi furnizate de un organism specializat (de exemplu parolele de acces public și privat).

Majoritatea produselor și serviciilor de securitate sunt probabil furnizate de distribuitori, de prestatori de servicii sau de operatori. Pentru anumite funcții specifice, cum ar fi de exemplu furnizarea de parole de acces public și privat și autorizația de control, ar putea fi necesară identificarea și mandatarea unor organisme corespunzătoare.

Același lucru este valabil și pentru certificarea produselor, evaluarea și verificarea calității serviciului, orice funcție care trebuie încredințată organismelor independente de interesele distribuitorilor, prestatorilor de servicii sau operatorilor. Asemenea organisme pot fi private, publice sau mandatate de stat pentru a îndeplini aceste funcții.

6.2. *Obiectiv*

Pentru a facilita punerea în aplicare în mod armonios a securității sistemelor de informare în Comunitate, în cadrul preocupării pentru protejarea publicului și a intereselor comerciale, va fi necesară adoptarea unei atitudini consecvente în ceea ce privește punerea în aplicare a securității sistemelor de informare. Atunci când sunt mandatate organisme independente, funcțiile și condițiile de funcționare ale acestora trebuie vor trebui definite și acceptate și, în cazul în care este necesar, înscrise într-un cadru de reglementare. Obiectivul este de a ajunge la recunoașterea reciprocă, la o împărțire a responsabilităților clar definită și convenită între diverși operatori la nivel comunitar.

6.3. *Situație și tendințe*

La ora actuală, punerea în aplicare a securității sistemelor de informații nu este bine organizată decât pentru anumite domenii și nu răspunde decât necesităților specifice ale acestora. Organizarea la nivel european este de cele mai multe ori neoficială, iar recunoașterea reciprocă a verificării și certificării nu are loc în afara anumitor grupuri închise. Din cauza importanței în creștere a securității sistemelor de informare, trebuie definită urgent o abordare coerentă în acest domeniu, atât în Europa, cât și la nivel internațional.

6.4. *Necesități, opțiuni și priorități*

Din cauza numărului operatorilor interesați și a legăturilor strânse cu problemele de reglementare și cele legislative, este important să se ajungă la un consens privind principiile care vor reglementa punerea în aplicare a securității sistemelor de informare.

În definirea unei atitudini coerente în acest domeniu, trebuie analizate aspectele legate de identificarea și specificarea funcțiilor care implică, prin natura lor, intervenția organismelor independente (sau a organismelor care lucrează în colaborare). Aceasta poate cuprinde funcții precum administrarea unui sistem de parole de acces public/privat.

De altfel, trebuie identificate și precizate rapid funcțiile care, în interesul publicului, trebuie încredințate unor organisme independente (sau unor organisme care lucrează în colaborare). Aceste funcții ar putea să includă, de exemplu, controlul, garantarea calității, verificarea, certificarea și funcții similare.