31992D0242

8.5.1992. *SLUŽBENI LIST EUROPSKIH ZAJEDNICA* L 123/19

ODLUKA VIJEĆA

od 31. ožujka 1992.

u području sigurnosti informacijskih sustava

(92/242/EEZ)

VIJEĆE EUROPSKIH ZAJEDNICA,

uzimajući u obzir Ugovor o osnivanju Europske ekonomske zajednice, a posebno njegov članak 235.,

uzimajući u obzir prijedlog Komisije [1],

uzimajući u obzir mišljenje Europskog parlamenta [2],

uzimajući u obzir mišljenje Gospodarskoga i socijalnoga odbora [3],

budući da je cilj Zajednice, kroz uspostavu zajedničkog tržišta i postupno usklađivanje gospodarskih politika država članica na području cijele Zajednice, promicati usklađen razvoj gospodarskih djelatnosti, kontinuirano i uravnoteženo širenje, veću stabilnost, brži rast životnog standarda i bliskije odnose između država članica;

budući da elektronički pohranjene, obrađene i prenesene informacije imaju sve važniju ulogu u gospodarskim i društvenim aktivnostima;

budući da s pojavom učinkovitih globalnih komunikacija i sve raširenijom upotrebom elektroničke obrade informacija raste i potreba za odgovarajućom zaštitom tih informacija;

budući da Europski parlament u svojim raspravama i rezolucijama stalno naglašava važnost sigurnosti informacijskih sustava;

budući da Gospodarski i socijalni odbor naglašava potrebu rješavanja pitanja koja se odnose na sigurnost informacijskih sustava kroz oblike djelovanja Zajednice, osobito u okviru nastanka unutarnjeg tržišta;

budući da oblici djelovanja na nacionalnoj i međunarodnoj razini i na razini Zajednice predstavljaju dobar temelj;

budući da postoji tijesna veza između telekomunikacija, informacijske tehnologije, normizacije, informacijskog tržišta i politike istraživanja i tehnološkog razvoja (RTD), kao i posla koji je u tim područjima Zajednica već obavila;

budući da je potrebno udružiti napore kroz nadogradnju postojećih rezultata na nacionalnoj i međunarodnoj razini i promicanje suradnje među glavnim strankama; budući da je stoga potrebno nastaviti aktivnosti u okviru jasno definiranog plana djelovanja;

budući da složenost sustava sigurnosti informacija zahtijeva razvoj strategija koje će istodobno omogućiti slobodan protok informacija unutar jedinstvenog tržišta i sigurno korištenje informacijskih sustava na području cijele Zajednice;

budući da je svaka država članica obvezna uzeti u obzir ograničenja koja nameću sigurnost i javni red;

budući da obveze država članica u ovom području podrazumijevaju zajednički pristup koji se temelji na uskoj suradnji s visokim dužnosnicima država članica;

budući da je potrebno usvojiti plan djelovanja za početno razdoblje od dvadeset i četiri mjeseca i osnovati odbor visokih dužnosnika s dugoročnim mandatom da Komisiju savjetuje o oblicima djelovanja u području sigurnosti informacijskih sustava;

budući da se smatra da je za provedbu plana djelovanja u početnom razdoblju od dvadeset i četiri mjeseca potreban iznos od 12 milijuna ECU; budući da je u kontekstu trenutačnog financijskog plana iznos za 1992. procijenjen na dva milijuna ECU;

budući da će iznosi potrebni za financiranje programa u razdoblju nakon proračunske godine 1992. biti dio postojećeg financijskog okvira Zajednice,

ODLUČILO JE:

Članak 1.

Ovom se Odlukom usvaja djelovanje u području sigurnosti informacijskih sustava. Djelovanje se sastoji od:

— razvoja općih strategija koje se odnose na sigurnost informacijskih sustava (plan djelovanja) za početno razdoblje od 24 mjeseca, i

— osnivanja skupine visokih dužnosnika s dugoročnim mandatom, dalje u tekstu „Odbor”, kako bi savjetovali Komisiju o djelovanju koje je potrebno poduzeti u području sigurnosti informacijskih sustava.

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

Članak 2.

1. Komisija se s Odborom sustavno savjetuje o pitanjima koja se odnose na sigurnost informacijskih sustava za različite aktivnosti Zajednice, a osobito o definiranju strategija i programa rada.

2. Plan djelovanja, kako je navedeno u Prilogu, uključuje pripremne radnje prema sljedećim temama:

I. razvoj strateškog okvira za sigurnost informacijskih sustava;

II. utvrđivanje zahtjeva korisnika i pružatelja usluga u pogledu sigurnosti informacijskih sustava;

III. rješenja za kratkoročne i srednjoročne potrebe korisnika, dobavljača i pružatelja usluga;

IV. razvoj specifikacija, normizacija, ocjenjivanja i certificiranje sigurnosti informacijskih sustava;

V. tehnološki i operativni trendovi u području sigurnosti informacijskih sustava;

VI. mjere u području sigurnosti informacijskih sustava.

Članak 3.

1. Sredstva Zajednice potrebna za provedbu ove mjere procijenjena su na 12 milijuna ECU za početno razdoblje, uključujući dva milijuna ECU za 1992. u financijskom razdoblju od 1988. do 1992.

Za razdoblje provedbe programa koje slijedi nakon navedenog razdoblja, iznos se mora uključiti u važeći financijski okvir Zajednice.

2. Proračunsko tijelo određuje proračunska sredstva za svaku proračunsku godinu, uzimajući u obzir načela dobroga upravljanja u smislu članka 2. Financijske uredbe koja se primjenjuje na opći proračun Europskih zajednica.

Članak 4.

Skupina nezavisnih stručnjaka za Komisiju obavlja procjenu napretka ostvarenog u početnom razdoblju. Izvješće te skupine, zajedno s eventualnim komentarima Komisije, podnosi se Europskom parlamentu i Vijeću.

Članak 5.

1. Komisija je odgovorna za provedbu plana djelovanja. U tome joj pomaže savjetodavni odbor koji čine predstavnici država članica i kojim predsjedava predstavnik Komisije.

2. Plan djelovanja provodi se u skladu s ciljevima određenima u članku 2. i ažurira se prema potrebi. Planom djelovanja precizno su određeni ciljevi i vrste mjera koje treba poduzeti, kao i za to potrebna financijska sredstva. Komisija na osnovu plana djelovanja objavljuje poziv na podnošenje prijedloga.

3. Plan djelovanja provodi se u uskoj suradnji sa sektorskim subjektima. Plan uzima u obzir, promiče i nadopunjava trenutačne europske i međunarodne aktivnosti normizacije u ovom području.

Članak 6.

1. Postupak utvrđen člankom 7. primjenjuje se na:

— mjere koje se odnose na politiku Zajednice u području sigurnosti informacijskih sustava;

2. Postupak utvrđen člankom 8. primjenjuje se na:

— pripremu i ažuriranje plana djelovanja iz članka 5.,

— sadržaj poziva na podnošenje prijedloga, procjenu prijedloga i procijenjeni iznos doprinosa Zajednice mjerama, u slučajevima kad taj iznos prelazi ECU 200 000,

— suradnju organizacija koje nisu dio Zajednice u bilo kojoj aktivnosti na koju se ova Odluka odnosi,

— dogovore oko distribucije, zaštite i korištenja rezultata tih mjera,

— mjere koje se poduzimaju radi ocjene plana djelovanja.

3. Kada je doprinos Zajednice ovim mjerama manji od ili jednak iznosu od ECU 200 000, Komisija se s Odborom savjetuje o mjerama koje treba poduzeti i obavješćuje Odbor o ishodu svoje procjene.

Članak 7.

Predstavnik Komisije Odboru podnosi nacrt mjera koje je potrebno poduzeti. Odbor usvaja mišljenje o nacrtu u roku koji određuje predsjedavajući ovisno o hitnosti pitanja, a prema potrebi, putem glasovanja.

Mišljenje se unosi u zapisnik; osim toga, svaka država članica ima pravo tražiti da se njezin stav unese u zapisnik.

Komisija u najvećoj mogućoj mjeri uzima u obzir mišljenje Odbora. Komisija obavješćuje Odbor o načinu na koji je njegovo mišljenje uzela u obzir.

Članak 8.

Predstavnik Komisije Odboru podnosi nacrt mjera koje treba poduzeti. Odbor usvaja mišljenje o nacrtu u roku koji određuje predsjedavajući ovisno o hitnosti pitanja. Mišljenje se usvaja većinom glasova utvrđenom člankom 148. stavkom 2. Ugovora, ako se radi o odlukama koje Vijeće mora usvojiti na prijedlog

Komisije. Glasovi predstavnika država članica u Odboru ponderiraju se na način utvrđen tim člankom. Predsjedavajući ne glasuje.

Komisija usvaja predviđene mjere ako su one u skladu s mišljenjem Odbora.

Ako predviđene mjere nisu u skladu s mišljenjem Odbora, ili ako nije usvojeno ni jedno mišljenje, Komisija Vijeću odmah podnosi prijedlog mjera koje treba poduzeti. Vijeće odluku donosi kvalificiranom većinom.

Ako Vijeće ne poduzme ni jednu mjeru u roku od tri mjeseca dana na koji mu je prijedlog podnesen, Komisija usvaja predložene mjere osim ako Vijeće glasuje protiv navedenih mjera običnom većinom.

Sastavljeno u Bruxellesu 31. ožujka 1992.

Za Vijeće

Predsjednik

Vitor MARTINS

PRILOG

Sažetak područja djelovanja

SMJERNICE ZA PLAN DJELOVANJA U PODRUČJU SIGURNOSTI INFORMACIJSKIH SUSTAVA

UVOD

Cilj je plana djelovanja razvoj općih strategija čija je svrha korisnicima i tvorcima elektronički pohranjenih, obrađenih ili prenesenih informacija pružiti odgovarajuću zaštitu za informacijske sustave od slučajnih ili namjernih prijetnji.

Plan djelovanja uzima u obzir i nadopunjuje trenutačne globalne aktivnosti normizacije u tom području.

Plan djelovanja uključuje sljedeća područja djelovanja:

— razvoj strateškog okvira za sigurnost informacijskih sustava,

— utvrđivanje zahtjeva korisnika i pružatelja usluga koji se odnose na sigurnost informacijskih sustava,

— rješenja za kratkoročne i srednjoročne potrebe korisnika, dobavljača i pružatelja usluga,

— razvoj specifikacija, normizacija, ocjena i certificiranje sigurnosti informacijskih sustava,

— tehnološki i operativni trendovi u području sigurnosti informacijskih sustava,

— mjere u području sigurnosti informacijskih sustava.

Komisija plan djelovanja provodi u koordinaciji sa srodnim aktivnostima u državama članicama i srodnim aktivnostima istraživanja i razvoja na razini Zajednice.

1. **Područje djelovanja I. – Razvoj strateškog okvira za sigurnost informacijskih sustava**

1.1. *Problematika*

Sigurnost informacijskih sustava prepoznata je kao sve prisutnija kvaliteta potrebna suvremenom društvu. Za usluge koje su povezane s elektroničkim informacijama potrebna je sigurna telekomunikacijska infrastruktura, siguran hardver i softver, kao i sigurno korištenje i upravljanje. S obzirom na sve aspekte sigurnosti informacijskih sustava, potrebno je usvojiti opću strategiju, izbjegavajući fragmentaran pristup. Bilo koja strategija koja se odnosi na sigurnost elektronički obrađenih informacija mora odražavati želju društva da djeluje učinkovito i da se istodobno zaštiti u svijetu koji se ubrzano mijenja.

1.2. *Cilj*

Potrebno je usvojiti strateški orijentiran okvir koji će pomiriti društvene, gospodarske i političke ciljeve s tehničkim, operativnim i zakonodavnim mogućnostima Zajednice u međunarodnom kontekstu. Osjetljivu ravnotežu između različitih interesa, ciljeva i ograničenja moraju uspostaviti sektorski subjekti kroz suradnju u usvajanju zajedničkog stava i strateškog okvira. To su uvjeti za usklađivanje interesa i potreba u kreiranju politike i u industrijskom razvoju.

1.3. *Trenutačno stanje i trendovi*

Trenutačno stanje obilježava sve veća svijest o potrebi djelovanja. Međutim, u nedostatku inicijative za koordinaciju napora, vrlo je vjerojatno da će neusklađeni napori u različitim sektorima dovesti do stanja koje će de facto biti kontradiktorno i postupno voditi prema ozbiljnijim pravnim, društvenim i gospodarskim problemima.

1.4. *Zahtjevi, opcije i prioriteti*

Takav zajednički okvir trebao bi izdvojiti i baviti se analizom rizika i upravljanjem rizikom u odnosu na osjetljivost informacija i srodnih usluga, usklađivanjem zakona i propisa koji se odnose na zloupotrebu i pogrešnu upotrebu računala/telekomunikacija, administrativnom infrastrukturom koja uključuje politiku sigurnosti i načine na koje se ta politika može učinkovito primijeniti u raznim granama industrije/disciplinama, kao i socijalnim pitanjima i pitanjima zaštite privatnosti (npr. kroz primjenu shema identifikacije, ustanovljenja vjerodostojnosti, neopozivosti, i po mogućnosti sustava autorizacije u demokratskom okruženju).

Potrebne su jasne smjernice za razvoj fizičkih i logičkih struktura za sigurne distribuirane informacijske usluge, norme, smjernice i definicije za provjerene proizvode i usluge koji se odnose na sigurnost i pilote i prototipe uz pomoć kojih se utvrđuje održivost raznih administrativnih struktura, sustava i normi koji se odnose na potrebe određenih sektora.

Potrebno je izgraditi svijest o potrebi sigurnosti kako bi se korisnici više brinuli za sigurnost u informacijskoj tehnologiji (IT).

2. **Područje djelovanja II. - Utvrđivanje zahtjeva korisnika i pružatelja usluga koji se odnose na sigurnost informacijskih sustava**

2.1. *Problematika*

Sigurnost informacijskih sustava neophodan je uvjet za cjelovitost i pouzdanost poslovnih aplikacija, intelektualnog vlasništva i povjerljivosti. To neizbježno dovodi do problema u održavanju ravnoteže, a ponekad i do potrebe odabira između slobodne trgovine i obveze zaštite privatnosti i intelektualnog vlasništva. Ti odabiri i kompromisi moraju se temeljiti na potpunom shvaćanju zahtjeva i utjecaju mogućih opcija na sigurnost informacijskih sustava u ispunjavanju tih zahtjeva.

Zahtjevi korisnika podrazumijevaju da su sigurnosne funkcije informacijskih sustava povezane s tehnološkim, operativnim i zakonodavnim aspektima. Zbog toga je sustavna analiza zahtjeva koji se odnose na sigurnost informacijskih sustava bitan dio razvoja odgovarajućih i učinkovitih mjera.

2.2. *Cilj*

Utvrditi prirodu i obilježja zahtjeva korisnika i pružatelja usluga i njihov odnos prema mjerama sigurnosti informacijskih sustava.

2.3. *Trenutačno stanje i trendovi*

Do sada nisu poduzimani zajednički napori kako bi se utvrdili brzo mijenjajući zahtjevi glavnih subjekata u pogledu sigurnosti informacijskih sustava. Države članice Zajednice utvrdile su zahtjeve za usklađivanje aktivnosti na nacionalnoj razini (posebno za usklađivanje „kriterija za ocjenu sigurnosti IT-a"). Jedinstveni kriteriji ocjenjivanja i pravila za međusobno priznavanje certifikata o ocjeni od velike su važnosti.

2.4. *Zahtjevi, mogućnosti i prioriteti*

Kao temelj dosljednog i transparentnog odnosa prema opravdanim potrebama sektorskih subjekata, potrebno je razviti sustav razvrstavanja zahtjeva korisnika i njegovu povezanost s mjerama sigurnosti informacijskih sustava.

Također se smatra važnim utvrditi zahtjeve u odnosu na zakonodavstvo, propise i načine postupanja, uzimajući u obzir procjenu trendova u obilježjima i tehnologiji usluga, kao i utvrditi alternativne strategije postizanja ciljeva kroz administrativne, stručne, operativne i tehničke dogovore, i procijeniti učinkovitost, lakoću korištenja i troškove alternativnih opcija i strategija za sigurnost informacijskih sustava za korisnike, pružatelje usluga i operatere.

3. **Područje djelovanja III. – Rješenja za kratkoročne i srednjoročne potrebe korisnika, dobavljača i pružatelja usluga**

3.1. *Problematika*

Računala je trenutačno moguće zaštititi na odgovarajući način od neovlaštenog pristupa izvana tako da ih se „izolira", to jest, primijeni konvencionalne organizacijske i fizičke mjere zaštite. Ovo se odnosi i na elektroničku komunikaciju unutar zatvorene skupine korisnika koja koristi namjensku mrežu. Stanje je bitno drukčije ako se informacije razmjenjuju između više korisničkih skupina ili putem javne ili javno dostupne mreže. Za pružanje slične razine sigurnosti takvim informacijskim sustavima ne postoji ni tehnologija, ni terminali ni usluge, kao ni srodni standardi ili postupci.

3.2. *Cilj*

Cilj je u kratkom roku ponuditi rješenja koja mogu zadovoljiti najhitnije potrebe korisnika, pružatelja usluga i proizvođača. To uključuje i korištenje zajedničkih kriterija za ocjenu sigurnosti IT-a. Ti bi kriteriji trebali biti prilagodljivi budućim zahtjevima i rješenjima.

3.3. *Trenutačno stanje i trendovi*

Neke skupine korisnika razvile su tehnike i postupke koji posebno zadovoljavaju potrebu identifikacije, cjelovitosti i neopozivosti. U tu se svrhu općenito koriste magnetne ili pametne kartice. Neke skupine korisnika koriste više ili manje sofisticirane tehnike šifriranja. To često podrazumijeva utvrđivanje „ovlasti" za određenu skupinu korisnika. Međutim, teško je postići opću primjenu ovih tehnika kako bi se zadovoljile potrebe otvorenog okruženja.

Međunarodna organizacija za normizaciju (ISO) radi na sigurnosti informacijskih sustava kod povezanih otvorenih sustava - OSI (ISO DIS 7498-2), a Savjetodavni odbor za međunarodnu telegrafiju i telefoniju (CCITT) na tome radi u kontekstu X400. U poruke je moguće ubaciti i sigurnosne segmente. Identifikacija, cjelovitost i neopozivost smatraju se dijelom poruka (EDIFACT), kao i dijelom X400 MHS.

Pravni okvir za elektroničku razmjenu podataka (EDI) trenutačno je još u fazi koncipiranja. Međunarodna gospodarska komora objavila je jedinstvena pravila postupanja za razmjenu poslovnih podataka putem telekomunikacijskih mreža.

Nekoliko zemalja (npr. Njemačka, Francuska, Ujedinjena Kraljevina i Sjedinjene Države) utvrdile su ili utvrđuju kriterije za ocjenjivanje pouzdanosti IT-a i telekomunikacijskih proizvoda i sustava i odgovarajućih postupaka ocjenjivanja. Ti se kriteriji usklađuju s nacionalnim proizvođačima i rezultirat će sve većim brojem pouzdanih proizvoda i sustava, počevši s jednostavnim proizvodima. Taj će se trend podržati osnivanjem organizacija na nacionalnoj razini koje će biti zadužene za ocjenjivanje i izdavanje certifikata.

Većina korisnika smatra mjere za zaštitu povjerljivosti trenutačno manje važnim. Međutim, to će se u budućnosti vjerojatno promijeniti jer će napredne komunikacijske usluge, a posebno mobilne usluge, postati sveprisutne.

3.4. *Zahtjevi, opcije i prioriteti*

Od presudne je važnosti što prije utvrditi postupke, norme, proizvode i alate koji jamče sigurnost i u informacijskim sustavima kao takvima (računalima, perifernim jedinicama) i u javnim komunikacijskim mrežama. Visok stupanj prioriteta mora se dati i identifikaciji, cjelovitosti i neopozivosti. Za provjeru učinkovitosti predloženih rješenja potrebno je provesti pilot projekte. Rješenja za prioritetne potrebe u vezi s razmjenom elektroničkih podataka traže se u programu TEDIS u širem okviru ovog plana djelovanja.

4. Područje djelovanja IV. - Razvoj specifikacija, normizacije, ocjenjivanja i certifikacije sigurnosti informacijskih sustava

4.1. *Problematika*

Zahtjevi koji se odnose na sigurnost informacijskih sustava prisutni su u svim područjima i stoga su zajedničke specifikacije i norme od presudne važnosti. Nepostojanje dogovorenih normi i specifikacija za sigurnost IT-a može predstavljati veliku prepreku napretku procesa i usluga koji se temelje na informacijama u čitavom gospodarstvu i društvu. Potrebno je poduzeti i mjere kako bi se ubrzao razvoj i korištenje tehnologija i normi nekoliko srodnih područja komunikacijskih i računalnih mreža, koja su od ključne važnosti za korisnike, gospodarstvo i upravu.

4.2. *Cilj*

Potrebno je uložiti napore kako bi se pronašlo sredstvo koje podržava i obavlja određene sigurnosne funkcije u općim područjima OSI-a, ONP-a, ISDN-a/IBC-a i upravljanje mrežom. Sastavni dio normizacije i specifikacije su tehnike provjere, koje uključuju certificiranje, koje vodi međusobnom priznavanju. Međunarodno dogovorena rješenja treba podržati kad je to moguće. Potrebno je poticati i razvoj i korištenje računalnih sustava sa sigurnosnim funkcijama.

4.3. *Trenutačno stanje i trendovi*

Sjedinjene Države pokrenule su važne inicijative kako bi riješile pitanje sigurnosti informacijskih sustava. U Europi se to pitanje rješava u kontekstu standardizacije IT-a i telekomunikacija u kontekstu ETSI-a i CEN-a/Cenelec-a kroz pripremu zadaća koje u tom području obavljaju CCITT i ISO.

S obzirom na sve veću zabrinutost, aktivnosti u Sjedinjenim Državama sve su intenzivnije, a proizvođači i pružatelji usluga podjednako pojačavaju napore u tom području. U Europi, Francuska, Njemačka i Ujedinjena Kraljevina zasebno su pokrenule slične aktivnosti, ali do zajedničkih aktivnosti sličnih onima u Sjedinjenim Državama dolazi sporo.

4.4. *Zahtjevi, opcije i prioriteti*

Kod sigurnosti informacijskih sustava postoji za te sustave svojstvena tijesna povezanost između zakonskih, operativnih, administrativnih i tehničkih aspekata. Pravila se moraju odražavati u normama, a odredbe koje se odnose na sigurnost informacijskih sustava moraju zadovoljavati norme i pravila tako da se to može provjeriti. U nekim aspektima pravila zahtijevaju specifikacije koje prelaze uobičajeni opseg normizacije, to jest uključuju pravila postupanja. Zahtjevi koji se odnose na norme i pravila postupanja postoje u svim područjima sigurnosti informacijskih sustava i potrebno je razlikovati između zahtjeva vezanih uz zaštitu koji se podudaraju s ciljevima sigurnosti i nekih tehničkih zahtjeva koji mogu biti povjereni europskim normizacijskim tijelima (CEN/Cenelec/ETSI).

Specifikacije i norme moraju obuhvaćati predmete usluga sigurnosti informacijskih sustava (identifikacija osoba i poduzeća, protokoli za neopozivost, pravno prihvatljiv elektronički dokaz, nadzor autorizacije), njihove komunikacijske usluge (zaštita privatnosti pri komunikaciji slikom, glasom i podacima u mobilnim komunikacijama, zaštita baza podataka i slika, sigurnost integriranih usluga), njihovo upravljanje komunikacijom i sigurnosti (sustav javnog/privatnog ključa za rad na otvorenoj mreži, zaštita upravljanja mrežom, zaštita pružatelja usluge) i njihovo certificiranje (kriteriji i razine sigurnosti, postupci potvrde sigurnosti za sigurne informacijske sustave).

5. Područje djelovanja V. - Tehnološki i operativni trendovi u području sigurnosti informacijskih sustava

5.1. *Problematika*

Sustavno istraživanje i razvoj tehnologije koja omogućava gospodarski održiva i operativno zadovoljavajuća rješenja za niz trenutačnih i budućih zahtjeva koji se odnose na sigurnost informacijskih sustava preduvjet je za razvoj tržišta usluga i konkurentnost europskoga gospodarstva u cjelini.

Tehnološke promjene u području sigurnosti informacijskih sustava morat će obuhvaćati i aspekte računalne sigurnosti i sigurnosti komunikacija jer su većina današnjih sustava distribuirani sustavi i pristup takvim sustavima ostvaruje se preko komunikacijskih usluga.

5.2. *Cilj*

Sustavno istraživanje i razvoj tehnologije koja omogućava gospodarski održiva i operativno zadovoljavajuća rješenja za niz trenutačnih i budućih zahtjeva koji se odnose na sigurnost informacijskih sustava.

5.3. *Zahtjevi, opcije i prioriteti*

Rad na sigurnosti informacijskih sustava treba obuhvaćati razvojne i provedbene strategije, tehnologije te integraciju i provjeru.

Strateški rad na istraživanju i razvoju morat će obuhvaćati teoretske modele sigurnih sustava (sigurnih od kompromitiranja, neovlaštenih izmjena i uskraćivanja usluge), modele koji se odnose na funkcionalne zahtjeve, modele rizika i arhitekturu sigurnosti.

Tehnološki orijentiran posao istraživanja i razvoja morao bi obuhvaćati identifikaciju korisnika i poruke (npr. putem analize glasa i elektroničkog potpisa), tehnička sučelja i protokole za šifriranje, mehanizme za nadzor pristupa i provedbene metode za dokazivo sigurne sustave.

Provjera i potvrda sigurnosti tehničkog sustava i njegova primjenjivost ispitivali bi se kroz projekte integracije i provjere.

Osim konsolidacije i razvoja tehnologije sigurnosti, potrebne su i popratne mjere koje se odnose na utvrđivanje, održavanje i dosljednu primjenu normi i potvrdu i certificiranje proizvoda IT-a i telekomunikacijskih proizvoda u odnosu na njihova sigurnosna obilježja, uključujući i potvrdu i certificiranje metoda za stvaranje i primjenu sustava.

Treći okvirni program Zajednice za RTD mogao bi se koristiti za poticanje projekata suradnje prije početka tržišne utakmice i donošenja propisa.

6. **Područje djelovanja VI. – Mjere za jamčenje sigurnosti informacijskih sustava**

6.1. *Problematika*

Ovisno o prirodi sigurnosnih obilježja informacijskih sustava, potrebne funkcije bit će neophodno integrirati u različite dijelove informacijskog sustava, od terminala/računala, usluga i mrežnog upravljanja do uređaja za šifriranje, pametnih kartica, javnih i privatnih ključeva itd. Za neke od ovih funkcija može se očekivati da će ih proizvođač ugraditi u hardver ili softver, dok ostale mogu biti dio distribuiranih sustava (npr. upravljanje mrežom), u posjedu korisnika (npr. pametne kartice) ili ih isporučuju specijalizirane organizacije (npr. javni/privatni ključevi).

Za većinu sigurnosnih proizvoda i usluga može se očekivati da će ih isporučivati proizvođači, pružatelji usluga ili operateri. Za posebne funkcije, npr. izdavanje javnih/privatnih ključeva ili nadzor autorizacije, može biti potrebno odrediti i ovlastiti odgovarajuće organizacije.

Isto vrijedi i za certificiranje, ocjenu i provjeru kvalitete usluge, što su funkcije kojima se trebaju baviti organizacije koje su neovisne o interesima proizvođača, pružatelja usluga ili operatera. Te organizacije mogu biti u privatnom ili državnom vlasništvu ili ih može ovlastiti država za obavljanje dodijeljenih zadaća.

6.2. *Cilj*

Kako bi se omogućio usklađen razvoj mjera sigurnosti informacijskih sustava u Zajednici, s ciljem zaštite javnih i poslovnih interesa, bit će potrebno razviti dosljedan pristup jamčenja sigurnosti. U slučaju kada će biti potrebno ovlastiti neovisne organizacije, funkcije i uvjeti tih organizacija morat će se odrediti i dogovoriti, a prema potrebi i ugraditi u regulatorni okvir. Cilj je postići jasno definiranu i sporazumnu podjelu odgovornosti između različitih subjekata na razini Zajednice kao preduvjet međusobnog priznavanja.

6.3. *Trenutačno stanje i trendovi*

Mjere sigurnosti za informacijske sustave trenutačno su dobro organizirane samo za određena područja i ograničene su na specifične potrebe u tim područjima. Organizacija mjera sigurnosti na europskoj razini uglavnom je neformalne prirode, a međusobno priznavanje provjere i certificiranja još ne postoji izvan zatvorenih skupina. S rastućom važnosti sigurnosti informacijskih sustava, sve važnija postaje i potreba definiranja dosljednog pristupa mjerama sigurnosti za informacijske sustave u Europi i šire.

6.4. *Zahtjevi, opcije i prioriteti*

Zbog velikog broja različitih sudionika i tijesne povezanosti s regulatornim i zakonodavnim pitanjima, osobito je važno postići dogovor o načelima za mjere sigurnosti informacijskih sustava.

U razvoju dosljednog pristupa ovom pitanju bit će potrebno utvrditi i odrediti funkcije koje zbog svoje prirode zahtijevaju sudjelovanje nekih neovisnih organizacija (ili organizacija koje međusobno surađuju). Ovo bi moglo uključivati funkcije poput upravljanja sustavom javnih/privatnih ključeva.

Osim toga, na samom početku potrebno je utvrditi i odrediti funkcije koje u interesu javnosti treba povjeriti neovisnim organizacijama (ili organizacijama koje međusobno surađuju). Ovo bi se, na primjer, moglo odnositi na nadzor, potvrdu kvalitete, provjeru, certificiranje i slične funkcije.