31992D0242

8.5.1992 URADNI LIST EVROPSKIH SKUPNOSTI L 123/19

SKLEP SVETA
z dne 31. marca 1992
o varnosti informacijskih sistemov

(92/242/EGS)

SVET EVROPSKIH SKUPNOSTI JE

ob upoštevanju Pogodbe o ustanovitvi Evropske gospodarske skupnosti, zlasti člena 235,

ob upoštevanju predloga Komisije ([1]),

ob upoštevanju mnenja Evropskega parlamenta ([2]),

ob upoštevanju mnenja Ekonomsko-socialnega odbora ([3]),

ker je naloga Komisije, da z vzpostavitvijo skupnega trga in s postopnim približevanjem ekonomskih politik držav članic spodbudi skladen razvoj gospodarskih dejavnosti v celotni Skupnosti, trajen in uravnovešen razmah, večjo stabilnost, pospešen dvig življenjskega standarda in tesnejše stike med državami članicami;

ker postajajo informacije, ki se shranjujejo, obdelujejo in prenašajo elektronsko, v gospodarskih in socialnih dejavnostih čedalje pomembnejše;

ker se zaradi uvedbe učinkovitih globalnih komunikacij in vedno bolj razširjene uporabe elektronske obdelave podatkov posveča večja pozornost potrebi po ustreznem varstvu;

ker je Evropski parlament v svojih razpravah in sklepih večkrat poudaril pomen varnosti informacijskih sistemov;

ker je Ekonomsko-socialni odbor poudaril, da je treba obravnavati vprašanja varnosti informacijskih sistemov v okviru ukrepanja Skupnosti, predvsem glede vpliva dokončne vzpostavitve notranjega trga;

ker ukrepanje na nacionalni in mednarodni ravni ter na ravni Skupnosti zagotavlja dobro podlago;

ker obstaja tesna povezava med telekomunikacijami, informacijskimi tehnologijami, standardizacijo, informacijskim trgom, politiko raziskav in tehnološkega razvoja (RTR) ter že opravljenim delom Skupnosti na tem področju;

ker je treba uskladiti prizadevanje z opiranjem na tekoče delo na nacionalni in mednarodni ravni ter s spodbujanjem sodelovanja med glavnimi udeleženci; ker je zato primerno ravnanje po usklajenem delovnem načrtu;

ker je zaradi celovite varnosti informacijskih sistemov treba uvesti strategije, ki bodo omogočale prost pretok informacij na notranjem trgu in zagotavljale varno uporabo informacijskih sistemov po vsej Skupnosti;

ker mora vsaka država članica upoštevati obveznosti, ki jih nalagata varnost in javni red;

ker vključuje odgovornost držav članic na tem področju usklajeno ravnanje, ki temelji na tesnem sodelovanju z visokimi uradniki držav članic;

ker je treba predvideti ukrep, ki bo vključeval delovni načrt za začetno obdobje 24 mesecev in oblikovanje odbora visokih uradnikov z dolgoročnim pooblastilom za svetovanje Komisiji o ukrepih glede varnosti informacijskih sistemov,

ker je znesek, ki je potreben za izvajanje ukrepa za začetno obdobje 24 mesecev, ocenjen na 12 milijonov ekujev; ker znaša za leto 1992 ocenjeni potrebni znesek v okviru sedanjih finančnih perspektiv 2 milijona ekujev;

ker se morajo zneski, ki jih je treba nameniti za financiranje programa v obdobju po proračunskem letu 1992, vključiti v veljavni finančni okvir Skupnosti,

SKLENIL:

Člen 1

S tem sklepom se sprejme ukrep za varnost informacijskih sistemov. Ukrep vsebuje:

— razvijanje globalnih strategij, ki bi zagotovile varnost informacijskih sistemov (delovni načrt) za začetno obdobje 24 mesecev, in

— ustanovitev odbora visokih uradnikov z dolgoročnim pooblastilom — v nadaljevanju „odbor“ – za svetovanje Komisiji o ukrepih, ki jih je treba uvesti glede varnosti informacijskih sistemov.

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

Člen 2

1. Komisija se redno posvetuje z odborom o vprašanjih varnosti informacijskih sistemov v različnih dejavnostih, ki jih vodi Skupnost, predvsem pri določanju delovnih strategij in programov.

2. Kot je določeno v prilogi, vsebuje delovni načrt pripravljalna dela v zvezi z naslednjimi tematskimi področji:

I. razvijanje okvirne strategije za varnost informacijskih sistemov;

II. ugotavljanje potreb uporabnikov in ponudnikov storitev za varnost informacijskih sistemov;

III. izdelava rešitev za nekatere kratkoročne in srednjeročne potrebe uporabnikov, dobaviteljev in ponudnikov storitev;

IV. razvijanje specifikacij, standardiziranje, ocenjevanje in certificiranje varnosti informacijskih sistemov;

V. tehnološki in funkcionalni razvoj varnosti informacijskih sistemov;

VI. zagotovitev varnosti informacijskih sistemov.

Člen 3

1. Finančna sredstva Skupnosti, ki so potrebna za izvajanje ukrepa, se za začetno obdobje ocenjujejo na 12 milijonov ekujev, od tega v okviru finančnih perspektiv 1988-1992 za leto 1992 dva milijona ekujev.

Za naslednje obdobje izvajanja programa bo treba znesek vključiti v veljavni finančni okvir Skupnosti.

2. Proračunski organ določi razpoložljiva sredstva za posamezno proračunsko obdobje ob upoštevanju načel gospodarnosti, opredeljenih v členu 2 Finančne uredbe za splošni proračun Evropskih skupnosti.

Člen 4

Skupina neodvisnih strokovnjakov opravi za Komisijo oceno doseženega napredka v začetnem obdobju. Poročilo te skupine se dopolnjeno z morebitnimi pripombami Komisije predloži Evropskemu parlamentu in Svetu.

Člen 5

1. Komisija je pristojna za izvajanje delovnega načrta. Pomaga ji odbor, ki ga sestavljajo predstavniki držav članic in mu predseduje predstavnik Komisije.

2. Delovni načrt se izvaja skladno s cilji iz člena 2 in se po potrebi prilagaja. V njem so določeni natančni cilji in vrste ukrepov, ki jih je treba uvesti, pa tudi finančne določbe, ki se nanje nanašajo. Komisija izvaja razpise na podlagi delovnega načrta.

3. Delovni načrt se izvaja v tesnem sodelovanju z udeleženci iz sektorja. V njem se upoštevajo, spodbujajo in dopolnjujejo tekoče evropske in mednarodne dejavnosti standardiziranja na tem področju.

Člen 6

1. Postopek iz člena 7 se uporablja za:

— ukrepe v zvezi s politiko Skupnosti glede varnosti informacijskih sistemov.

2. Postopek iz člena 8 se uporablja za:

— izdelavo in sprotno prilagajanje delovnega načrta iz člena 5,

— vsebino razpisov, ocenjevanje ponudb in ocenjeni znesek prispevka Skupnosti za ukrepe, če je višji od 200 000 ekujev,

— sodelovanje organizacij zunaj Skupnosti pri dejavnostih iz tega sklepa,

— podrobnosti glede razširjanja, varovanja in uporabe rezultatov, doseženih z ukrepi,

— ukrepe, ki jih je treba sprejeti za oceno programa.

3. Če je znesek prispevka Skupnosti za ukrepe nižji ali enak 200 000 ekujem, Komisija obvesti odbor o ukrepih, ki jih je treba uvesti, in o rezultatu njene ocene.

Člen 7

Predstavnik Komisije predloži odboru osnutek za ukrepe, ki jih je treba sprejeti. Odbor izda — po potrebi z glasovanjem — mnenje o osnutku v roku, ki ga lahko določi predsednik glede na nujnost zadeve.

Mnenje se zapiše v zapisnik; poleg tega lahko vsaka država članica zahteva, da se njeno stališče zabeleži v zapisniku.

Komisija, kolikor je možno, upošteva mnenje odbora in ga obvesti, kako je upoštevala to mnenje.

Člen 8

Predstavnik Komisije predloži odboru osnutek za ukrepe, ki jih je treba sprejeti. Odbor izda mnenje v roku, ki ga lahko določi predsednik glede na nujnost zadeve. Mnenje se sprejme z večino,

določeno v členu 148(2) Pogodbe, ki je potrebna za sprejemanje sklepov Sveta na predlog Komisije. Na glasovanju v odboru se glasovi predstavnikov držav članic ponderirajo v skladu z omenjenim členom. Predsednik ne glasuje.

Komisija sprejme predvidene ukrepe, če so ti v skladu z mnenjem odbora.

Če predvideni ukrepi niso skladni z mnenjem odbora ali če se mnenje ne sprejme, Komisija nemudoma predloži Svetu predlog ukrepov, ki jih je treba sprejeti. Svet odloči s kvalificirano večino.

Če Svet v treh mesecih po predložitvi zadeve ne sprejme sklepa, Komisija uvede predlagane ukrepe, razen če se je Svet s preprosto večino izrekel proti njim.

V Bruslju, 31. marca 1992

Za Svet

Predsednik

Vitor MARTINS

PRILOGA

Povzetek področij ukrepov

SMERNICE ZA DELOVNI NAČRT O VARNOSTI INFORMACIJSKIH SISTEMOV

UVOD

Cilj delovnega načrta je razvijati globalne strategije, da bi se uporabnikom in proizvajalcem elektronsko shranjenih, obdelanih ali prenesenih informacij zagotovilo ustrezno varstvo informacijskih sistemov pred nenamernim ali namernim ogrožanjem.

V delovnem načrtu se upoštevajo in dopolnjujejo tekoče dejavnosti standardiziranja s tega področja po svetu.

Delovni načrt vsebuje naslednja področja ukrepov:

— razvijanje okvirne strategije za varnost informacijskih sistemov,

— ugotavljanje potreb uporabnikov in ponudnikov storitev na področju varnosti informacijskih sistemov,

— izdelava rešitev za nekatere kratkoročne in srednjeročne potrebe uporabnikov, dobaviteljev in ponudnikov storitev,

— razvijanje specifikacij, standardiziranje, ocenjevanje in certificiranje varnosti informacijskih sistemov,

— tehnološki in funkcionalni razvoj varnosti informacijskih sistemov,

— zagotovitev varnosti informacijskih sistemov.

Delovni načrt izvaja Komisija v tesni povezavi s podobnimi ukrepi v državah članicah in skupaj z ukrepi Skupnosti za raziskave in razvoj.

1. **Področje ukrepov I: Razvijanje okvirne strategije za varnost informacijskih sistemov**

1.1 *Problematika*

Varnost informacijskih sistemov je lastnost, ki se mora zagotoviti na vseh področjih sodobne družbe. Elektronske informacijske storitve zahtevajo varno telekomunikacijsko infrastrukturo, varno strojno in programsko opremo ter varno uporabo in upravljanje. Treba je vzpostaviti globalno strategijo in upoštevati vse vidike varnosti informacijskih sistemov ter se izogniti razdrobljenim pristopom. Vsaka strategija za varnost elektronsko obdelane informacije mora upoštevati željo družbe, da deluje uspešno in da se v hitro spreminjajočem svetu zaščiti.

1.2 *Cilj*

Izdelati je treba okvirno strategijo za uskladitev socialnih, gospodarskih in političnih ciljev s tehničnimi, operativnimi in zakonodajnimi možnostmi Skupnosti na mednarodni ravni. Udeleženci v sektorjih, ki sodelujejo pri razvijanju skupne vizije in usklajene okvirne strategije, morajo najti občutljivo ravnovesje med različnimi potrebami, cilji in obveznostmi. To je pogoj za usklajevanje interesov in potreb pri določanju politike, pa tudi pri industrijskem razvoju.

1.3 *Sedanje stanje in prizadevanje*

Za sedanje stanje je značilna rastoča zavest, da je ukrepanje nujno. Vendar je zelo verjetno, da bodo brez pobude za usklajenost ukrepi, razpršeni po sektorjih, povzročili dejansko sporni položaj in tako postopoma še več pravnih, socialnih in gospodarskih problemov.

1.4 *Zahteve, možnosti in prednosti*

Znotraj tega okvira bi se morala obravnavati in preučiti analiza in obvladovanje tveganja v zvezi z ogroženostjo informacijskih in sorodnih storitev, uskladitvijo zakonov in drugih predpisov o zlorabi in napačni uporabi informatike in telekomunikacij, upravnimi infrastrukturami, skupaj z varnostnimi politikami in načinom njihovega uspešnega uvajanja v razne industrije in discipline ter v zvezi z družbenim življenjem in varstvom informacijske zasebnosti (na primer uporaba sistemov za ugotavljanje identičnosti, avtentifikacijo, nezatajljivost in morebitno dovoljenje v demokratičnem okolju).

Da bi izdelali fizične in logične arhitekture za varne porazdeljene informacijske storitve, standarde, smernice in definicije za zagotovljene varnostne izdelke in storitve, pilotne projekte in prototipe, so potrebne jasne usmeritve, ki zagotavljajo ustreznost raznih upravnih struktur ter drugih arhitektur in standardov glede potreb specifičnih sektorjev.

Treba je ustvariti zavest o varnosti, da bi uporabnike spodbudili k večji skrbi za varnost informacijskih tehnologij (IT).

2. **Področje ukrepov II: Ugotavljanje potreb uporabnikov in ponudnikov storitev za varnost informacijskih sistemov**

2.1 *Problematika*

Varnost informacijskih sistemov je nujni pogoj za neokrnjenost in verodostojnost poslovnih aplikacij, varstvo intelektualne lastnine in zaupnosti. To povzroča problem občutljivega ravnovesja — in včasih možnost izbire med spodbujanjem proste trgovine in varstvom informacijske zasebnosti in intelektualne lastnine. Izbira in kompromisi morajo temeljiti na globalni presoji potreb in posledic možne izbire glede varnosti informacijskih sistemov, zato da bi zadovoljili te potrebe.

Zahteve uporabnikov se nanašajo na varnostne funkcije informacijskih sistemov v zvezi s tehnološkimi, delovnimi in zakonodajnimi vidiki. Za razvijanje ustreznih in učinkovitih ukrepov je zato potrebna sistematična raziskava zahtev za varnost informacijskih sistemov.

2.2 *Cilj*

Treba je določiti vrsto in značilnosti zahtev uporabnikov in ponudnikov storitev ter njihov odnos do ukrepov za varnost informacijskih sistemov.

2.3 *Sedanje stanje in prizadevanje*

Doslej še ni bil uveden noben skupni ukrep za ugotavljanje hitro spreminjajočih se zahtev glavnih udeležencev pri varnosti informacijskih sistemov. Nekatere države članice Skupnosti so določile potrebo po usklajevanju svojih dejavnosti (posebno „meril za ocenjevanje varnosti informacijskih tehnologij“). Zelo pomembna so enotna ocenjevalna merila in pravila za medsebojno priznavanje potrdil o oceni.

2.4 *Zahteve, možnosti in prednosti*

Za usklajeno in pregledno obravnavanje upravičenih zahtev udeležencev v sektorju je treba izdelati usklajeno razvrstitev zahtev uporabnikov in njihovega odnosa do zagotavljanja varnosti informacijskih sistemov.

Prav tako je treba ugotoviti potrebe za zakone, predpise in kodekse ravnanja, pri čemer je treba oceniti usmeritve glede značilnosti storitev in tehnologije, določiti druge možne strategije, ki bodo omogočile dosego ciljev z uporabo upravnih, storitvenih, operativnih in tehničnih določb, ter oceniti učinkovitost, prijaznost do uporabnika, stroške alternativnih možnosti in strategij varnosti informacijskih sistemov za uporabnike, ponudnike storitev in operaterje.

3. **Področje ukrepov III: Izdelava rešitev za nekatere kratkoročne in srednjeročne potrebe uporabnikov, dobaviteljev in ponudnikov storitev**

3.1 *Problematika*

Danes je z ukrepi „izolacije“, t. j. tradicionalnimi organizacijskimi in tehničnimi ukrepi, možno uspešno preprečevati nedovoljeni dostop do računalnikov od zunaj. Enako velja za elektronsko komunikacijo znotraj zaprte skupine uporabnikov v namenskem omrežju. Čisto drugače pa je, če so informacije na voljo več skupinam uporabnikov ali se izmenjujejo po javnem oz. vsem dostopnem omrežju. Niti tehnologija, terminali in storitve niti ustrezni standardi in postopki v tem primeru praviloma ne morejo primerljivo zagotoviti varnosti informacijskih sistemov.

3.2 *Cilj*

Cilj je kratkoročna izdelava rešitev, ki bi ustrezale najnujnejšim potrebam uporabnikov, ponudnikov storitev in proizvajalcev. To vključuje uporabo skupnih meril za ocenjevanje varnosti informacijskih tehnologij. Ta merila morajo biti odprta za prihodnje potrebe in rešitve.

3.3 *Sedanje stanje in prizadevanje*

Nekatere skupine uporabnikov so za svojo lastno uporabo razvile tehnike in postopke, ki posebej upoštevajo potrebe po avtentifikaciji, neokrnjenosti in nezatajljivosti. Praviloma se uporabljajo magnetne ali pametne kartice. Nekateri uporabljajo bolj ali manj visoko razvite kriptografske tehnike. V ta namen je treba pogosto določiti „organe“ za posebne skupine uporabnikov. Vendar je težko posploševati te tehnike in postopke ter tako zadovoljiti potrebe v odprtem okolju.

ISO razvija varnost informacijskih sistemov OSI (ISO DIS 7498-2) in CCITT v okviru X400. V sporočila je možno vdelati tudi varnostne segmente. Avtentifikacija, neokrnjenost in nezatajljivost se obravnavajo kot deli sporočil (EDIFACT) in deli X400 MHS.

Pravni okvir RIP (računalniška izmenjava podatkov) se zdaj šele razvija. Mednarodna trgovinska zbornica je objavila enotne kodekse ravnanja za izmenjavo poslovnih podatkov po telekomunikacijskih omrežjih.

Več držav (na primer Nemčija, Francija, Združeno kraljestvo in Združene države Amerike) so razvile ali razvijajo merila za ocenjevanje verodostojnosti informacijsko-telekomunikacijskih izdelkov in sistemov ter ustrezne postopke za ocenjevanje. Ta merila so bila

usklajena s proizvajalci v posameznih državah in bodo omogočila razvoj vedno več zanesljivih izdelkov in sistemov, najprej preprostih izdelkov. Ustanovitev organizacij po državah, pristojnih za vodenje ocenjevanja in izdajanja potrdil, bo to prizadevanje še okrepila.

Večina uporabnikov meni, da so predpisi o zaupnosti v tem trenutku manj pomembni. Vendar se bo to v prihodnosti zaradi splošnega razširjanja sodobnih komunikacijskih in predvsem storitev mobilne telefonije verjetno spremenilo.

3.4 *Zahteve, možnosti in prednosti*

Čim prej je treba razviti postopke, standarde, izdelke in orodje, ki bodo sposobni zagotavljati varnost informacijskih sistemov kot takih (računalniki, zunanje naprave) in javnih komunikacijskih omrežij. Prednost bi morale imeti avtentifikacija, neokrnjenost in nezatajljivost. Za ugotavljanje primernosti predlaganih rešitev bi morali izdelati pilotne projekte. Rešitve za nekatere prednostne potrebe glede RIP se preučujejo po programu TEDIS in se usklajujejo v širšem okviru tega delovnega načrta.

4. Področje ukrepov IV: Razvijanje specifikacij, standardiziranje, ocenjevanje in certificiranje varnosti informacijskih sistemov

4.1 *Problematika*

Potrebe po varnosti informacijskih sistemov je zaznati povsod, zato je obstoj skupnih specifikacij in standardov ključnega pomena. Pomanjkanje usklajenih standardov in specifikacij za varnost informacijskih tehnologij bi bilo lahko velika ovira za napredek pri informacijsko podprtih postopkih in storitvah v celotnem gospodarstvu in družbi. Prav tako je treba uvesti ukrepe za pospeševanje razvijanja ter uporabe tehnologije in standardov na raznih sorodnih področjih komunikacijskih in računalniških omrežij, ki so za uporabnike, industrijo in uprave odločilnega pomena.

4.2 *Cilj*

Potrebni so ukrepi za podpiranje in izvajanje posebnih varnostnih funkcij na splošnih področjih OSI, ONP, ISDN/IBC in pri upravljanju omrežja. Tehnike in načini preverjanja, s certificiranjem za medsebojno priznavanje vred, so tesno povezani s standardiziranjem in specifikacijo. Vedno ko je to možno, je treba podpirati rešitve, sprejete na mednarodni ravni. Prav tako bi bilo treba spodbuditi razvijanje in uporabo informacijskih sistemov z varnostnimi funkcijami.

4.3 *Sedanje stanje in prizadevanje*

Predvsem Združene države Amerike so prevzele glavne pobude glede vprašanja varnosti informacijskih sistemov. V Evropi se to vprašanje obravnava v zvezi s standardizacijo informacijske tehnologije in telekomunikacij v okviru ETSI in CEN/CENELEC kot priprava dela CCITT in ISO na tem področju.

Ker je za to področje vedno več zanimanja, delo v Združenih državah Amerike hitro napreduje; oboji, prodajalci in ponudniki storitev, krepijo svoje prizadevanje na tem področju. V Evropi so Francija, Nemčija in Združeno kraljestvo vsaka zase začele izvajati podobne dejavnosti, medtem ko se skupno prizadevanje, primerljivo s tistim v Združenih državah Amerike, razvija le počasi.

4.4 *Zahteve, možnosti in prednosti*

Glede varnosti informacijskih sistemov so zakonodajni, operativni, upravni in tehnični vidiki med seboj tesno povezani. Pri standardih je treba upoštevati pravne predpise, treba je tudi dokazati, da se določbe o varnosti informacijskih sistemov skladajo s standardi in predpisi. Predpisi morajo v več ozirih vsebovati specifikacije, ki se ne omejujejo na tradicionalni cilj standardizacije, to pomeni, da vključujejo kodekse ravnanja. Zahteve v zvezi s standardi in kodeksi ravnanja se izražajo na vseh varnostnih področjih informacijskih sistemov. Pri tem je treba razlikovati med varnostnimi zahtevami, ki ustrezajo varnostnim ciljem, in nekaterimi tehničnimi zahtevami, ki bi se lahko zaupale pristojnim evropskim organom za standardizacijo (CEN/CENELEC/ETSI).

Specifikacije in standardi morajo zajemati varnostne storitve informacijskih sistemov (avtentifikacija oseb in podjetij, protokoli nezatajljivosti, pravno veljavni elektronski dokaz, preverjanje upravičenosti), njihove komunikacijske storitve (varstvo informacijske zasebnosti pri slikovni, glasovni in podatkovni komunikaciji, varstvo slikovnih in podatkovnih zbirk, varnost sestavljenih storitev), njihovo upravljanje komunikacij in varnosti (sistem javnih/zasebnih ključev za delovanje odprtih omrežij, varstvo upravljanja omrežja, varstvo ponudnikov storitev) in njihovo certificiranje (merila in stopnje varnosti, postopki za zagotavljanje varnosti informacijskih sistemov).

5. Področje ukrepov V: Tehnološki in funkcionalni razvoj varnosti informacijskih sistemov

5.1 *Problematika*

Sistematično raziskovalno delo in tehnološki razvoj, ki bi spodbudila iskanje gospodarsko rentabilnih in uporabnih rešitev za vrsto sedanjih in prihodnjih potreb po varnosti informacijskih storitev, sta pogoj za razvoj trga storitev in konkurenčnosti celotnega evropskega gospodarstva.

Pri vsakem tehnološkem razvoju varnosti informacijskih sistemov bo treba upoštevati varnost računalnikov, pa tudi komunikacij, saj gre pri večini sedanjih sistemov za porazdeljene sisteme, dostop do katerih je mogoč s komunikacijskimi storitvami.

5.2 *Cilj*

Sistematično raziskovalno delo in tehnološki razvoj za iskanje gospodarsko rentabilnih in uporabnih rešitev za vrsto sedanjih in prihodnjih potreb po varnosti informacijskih storitev.

5.3 *Zahteve, možnosti in prednosti*

Delo za varnost informacijskih sistemov bi moralo zajemati strategije za razvijanje in izvajanje, tehnologije, pa tudi združevanje in preverjanje.

Strateške naloge RTR bi morale vključevati študijo teoretičnih modelov za varne sisteme (varne pred kompromitiranjem, nedovoljenimi spremembami in odpovedjo storitve), modele v zvezi s funkcionalnimi zahtevami, modele tveganja in varnostne arhitekture.

Tehnološko orientirane raziskave in razvoj bi morali vključevati avtentifikacijo uporabnika in sporočila (na primer z analizo glasu ali elektronskimi podpisi), tehnične vmesnike in protokole za šifriranje, mehanizme za nadzirani dostop in metode za izdelavo dokazljivo varnih sistemov.

Preverjanje in veljavnost varnosti tehničnega sistema in njegove uporabnosti se preučuje s projekti za združevanje in preverjanje.

Poleg ureditve in razvijanja varnostne tehnologije so potrebni spremljevalni ukrepi pri oblikovanju, sprotnem dopolnjevanju in dosledni uporabi standardov ter validacije in certificiranja izdelkov informacijske tehnologije in telekomunikacijskih izdelkov glede njihovih varnostnih značilnosti, skupaj z validacijo in certificiranjem metod za razvijanje in izvajanje sistemov.

Tretji okvirni program Skupnosti za RTR bi lahko uporabili za pospeševanje skupnih projektov na predkonkurenčni in prednormativni ravni.

6. **Področje ukrepov VI: Zagotovitev varnosti informacijskih sistemov**

6.1 *Problematika*

Glede na vrsto varnostnih značilnosti informacijskih sistemov je treba zahtevane funkcije vdelati v razna mesta informacijskega sistema, skupaj s terminali/računalniki, storitvami, upravljanjem omrežij, napravami za šifriranje, pametnimi karticami, javnimi in zasebnimi ključi itd. Nekatere od teh funkcij bodo verjetno vdelane v strojno ali programsko opremo, ki jo zagotovijo prodajalci, druge pa bodo del porazdeljenih sistemov (na primer upravljanje omrežij), v lasti posameznih uporabnikov (na primer pametne kartice) ali pa jih bo zagotavljala posebna organizacija (na primer javni in zasebni ključi).

Večino varnostnih izdelkov in storitev bodo pretežno zagotavljali prodajalci, ponudniki storitev ali operaterji. Za nekatere posebne naloge, npr. zagotavljanje javnih in zasebnih ključev in dovoljenje za nadzor, se bodo morale po potrebi določiti in pooblastiti ustrezne organizacije.

Enako velja za certificiranje izdelkov, ocenjevanje in preverjanje kakovosti storitev; to so naloge, ki se morajo zaupati organizacijam, delujočim neodvisno od interesov prodajalcev, ponudnikov storitev ali operaterjev. Takšne organizacije so lahko zasebne ali javne oz. jih za izpolnjevanje teh nalog pooblasti država.

6.2 *Cilj*

Da bi pospešili skladno izvajanje varnosti informacijskih sistemov v Skupnosti glede varovanja javnih in poslovnih interesov, bo nujna izdelava usklajenega načina izvajanja varnosti informacijskih sistemov. Ko bodo neodvisne organizacije prejele pooblastilo, bo treba določiti in sprejeti njihove naloge in pogoje za delovanje ter jih po potrebi zakonsko opredeliti. Cilj je doseči jasno določeno in usklajeno razdelitev pristojnosti med raznimi udeleženci na ravni Skupnosti, kar je prvi pogoj za medsebojno priznavanje.

6.3 *Sedanje stanje in prizadevanje*

Za zdaj je izvajanje varnosti informacijskih sistemov dobro organizirano samo na posameznih področjih in se omejuje le na njihove posebne potrebe. Organizacija na evropski ravni je večinoma neformalna, medsebojno priznavanje preverjanja in certificiranja še ni bilo uvedeno zunaj nekaterih zaprtih skupin. Zaradi čedalje večjega pomena varnosti informacijskih sistemov bo postala nujna določitev usklajenega ravnanja na tem področju na evropski in tudi mednarodni ravni.

6.4 *Zahteve, možnosti in prednosti*

Zaradi števila zadevnih udeležencev in tesne povezave z vprašanji ureditve in zakonodaje je pomembno, da se doseže soglasje glede načel, ki bi morala urejati izvajanje varnosti informacijskih sistemov.

Pri določitvi usklajenega načina ravnanja na tem področju bo treba obravnavati vidike določanja in specifikacije nalog, ki bodo že zaradi narave same zahtevale sodelovanje neodvisnih organov (ali sodelujočih organov). To bi lahko zajemalo naloge, kakršna je upravljanje sistema javnih/zasebnih ključev.

Poleg tega je treba dovolj zgodaj določiti in podrobno opredeliti naloge, ki se morajo zaradi javnega interesa zaupati neodvisnim organom (ali sodelujočim organom). Te naloge bi lahko na primer vključevale nadzor, zagotavljanje kakovosti, preverjanje, certificiranje in podobno.