

31992D0242

8.5.1992.

EIROPAS KOPIENU OFICIĀLAIS VĒSTNESIS

L 123/19

**PADOMES LĒMUMS
(1992. gada 31. marts)
informācijas sistēmu drošības jomā**

(92/242/EEK)

EIROPAS KOPIENU PADOME,

ņemot vērā Eiropas Ekonomikas kopienas dibināšanas līgumu un jo īpaši tā 235. pantu,

ņemot vērā Komisijas priekšlikumu ⁽¹⁾,

ņemot vērā Eiropas Parlamenta atzinumu ⁽²⁾,

ņemot vērā Ekonomikas un sociālo lietu komitejas atzinumu ⁽³⁾,

tā kā Kopienas uzdevums, veidojot kopēju tirgu un pakāpeniski tuvinot dalībvalstu ekonomikas politikas, ir visā Kopienā veicināt saskaņotu saimnieciskās darbības attīstību, pastāvīgu un līdzsvarotu izaugsmi, lielāku stabilitāti, straujāku dzīves līmeņa paaugstināšanos un ciešākas attiecības starp dalībvalstīm;

tā kā elektroniski uzglabātas, apstrādātas un pārraidītas informācijas loma saimnieciskās un sociālās darbībās kļūst aizvien nozīmīgāka;

tā kā efektīvas globālas komunikācijas sākšanās un visaptveroša elektroniskās informācijas apstrādes izmantošana palielina vajadzību pēc adekvātas aizsardzības;

tā kā Eiropas Parlaments debatēs un rezolūcijās ir atkārtoti uzsvēris informācijas sistēmu drošības nozīmīgumu;

tā kā Ekonomikas un sociālo lietu komiteja ir uzsvērusi vajadzību ar Kopienas rīcību risināt jautājumus, kas saistīti ar informācijas sistēmu drošību, īpaši ņemot vērā iekšējā tirgus izveides ietekmi;

tā kā rīcība valstu, reģionālā un Kopienas līmenī nodrošina labu pamatu;

tā kā pastāv cieša saikne starp telekomunikāciju, informācijas tehnoloģiju, standartizācijas, informācijas tirgus un pētniecības un tehnoloģijas attīstības politiku, kā arī Kopienas jau uzsākto darbu šajās jomās;

tā kā ir lietderīgi nodrošināt, ka centienus saskaņo, balstoties uz esošo valstu un starptautisko darbu un veicinot sadarbību starp galvenajām iesaistītajām pusēm; tā kā tādējādi ir lietderīgi darboties pēc saskaņota rīcības plāna;

tā kā informācijas sistēmu drošības sarežģītība prasa izveidot stratēģijas, kas sekmē informācijas brīvu apriti vienotajā tirgū, vienlaikus nodrošinot informācijas sistēmu izmantošanas drošību visā Kopienā;

tā kā katras dalībvalsts pienākums ir ņemt vērā drošības un sabiedriskās kārtības radītos ierobežojumus;

tā kā dalībvalstu pienākumi šajā jomā saistās ar saskaņotu pieeju, kas balstīta uz ciešu sadarbību ar dalībvalstu augstākajiem ierēdņiem;

tā kā ir jāizstrādā rīcības plāns sākotnējam divdesmit četrus mēnešus posmam, un jāizveido Augstāko ierēdņu komiteja, kam piešķirtas ilglaicīgas pilnvaras konsultēt Komisiju par rīcību informācijas sistēmu drošības jomā;

tā kā ir vajadzīgi 12 miljoni ECU, lai īstenotu rīcību sākotnējā divdesmit četrus mēnešus posmā; tā kā ievērojot pašreizējo finanšu plānu, 1992. gadam vajadzīgā summa ir 2 miljoni ECU;

tā kā summas, kas paredzētas programmas finansējumam laika posmā pēc 1992. budžeta gada, ietilps esošajā Kopienas finanšu shēmā,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Ar šo lēmumu pieņem rīcību informācijas sistēmu drošības jomā. Tajā ietilpst:

- vispārējās stratēģijas izveide informācijas sistēmu drošībai (rīcības plāns) sākotnējam 24 mēnešu posmam,
- augstāko ierēdņu komitejas izveide, kam piešķirtas ilglaicīgas pilnvaras konsultēt Komisiju par informācijas sistēmu drošības jomā veicamo rīcību, šē turpmāk — "Komiteja".

⁽¹⁾ OV C 277, 5.11.1990., 18. lpp.

⁽²⁾ OV C 94, 13.3.1992.

⁽³⁾ OV C 159, 17.6.1991., 38. lpp.

2. pants

1. Komisija sistemātiski apspriežas ar Komiteju par jautājumiem, kas saistīti ar informācijas sistēmu drošību saistībā ar dažādām Kopienas darbībām, īpaši par darba stratēģiju un programmu noteikšanu.

2. Rīcības plānā, kā norādīts pielikumā, ietver sagatavošanas darbu saistībā ar šādām tēmām:

- I. Informācijas sistēmu drošības stratēģiskā pamata izveide.
- II. Lietotāju un pakalpojumu sniedzēju prasību identificēšana saistībā ar informācijas sistēmu drošību.
- III. Lietotāju, piegādātāju un pakalpojumu sniedzēju īstermiņa un vidēja termiņa vajadzību apmierināšana.
- IV. Specifikāciju, standartizācijas, novērtējuma un sertifikācijas izveide saistībā ar informācijas sistēmu drošību.
- V. Tehnoloģiski un darbības jauninājumi informācijas sistēmu drošības jomā.
- VI. Informācijas sistēmu drošības ieviešana.

3. pants

1. Paredzams, ka Kopienas līdzekļi, kas vajadzīgi šīs rīcības īstenošanai, ir 12 miljoni ECU sākotnējam periodam, ieskaitot 2 miljonus ECU 1992. gadam, atbilstoši 1988.- 1992. gada finanšu plānam.

Programmas piemērošanas turpmākajam posmam summa jāiekļauj spēkā esošajā Kopienas finanšu shēmā.

2. Budžeta lēmējinstāde nosaka apropriācijas, kas pieejamas katrā finanšu gadā, ņemot vērā pareizas finanšu vadības principus, kuri minēti 2. pantā Finanšu regulā attiecībā uz Eiropas Kopienu vispārējo budžetu.

4. pants

Neatkarīgu ekspertu grupa Komisijai novērtēs sākotnējā periodā panākto progresu. Grupas ziņojumu un Komisijas piezīmes iesniedz Eiropas Parlamentam un Padomei.

5. pants

1. Par rīcības īstenošanu atbild Komisija. Tai palīdz padomdevēja komiteja, ko veido dalībvalstu pārstāvji un vada Komisijas pārstāvis.

2. Rīcības plānu īsteno atbilstoši 2. pantā noteiktajiem mērķiem, un vajadzības gadījumā atjaunina. Tajā norāda precīzus mērķus

un veicamo darbību veidus, kā arī attiecīgos finanšu pasākumus. Komisija uzaicina iesniegt priekšlikumus, balstoties uz rīcības plānu.

3. Rīcības plānu īsteno ciešā sadarbībā ar nozares dalībniekiem. Tas ņem vērā, veicina un papildina esošos Eiropas un starptautiskos standartizācijas pasākumus šajā jomā.

6. pants

1. Procedūra, kas paredzēta 7. pantā, attiecas uz:

— pasākumiem saistībā ar Kopienas politiku informācijas sistēmu drošības jomā.

2. Procedūra, kas paredzēta 8. pantā, attiecas uz:

— 5. pantā minētā rīcības plāna sagatavošanu un atjaunināšanu,

— uz priekšlikumu iesniegšanas uzaicinājumu saturu, priekšlikumu novērtēšanu un paredzamo Kopienas ieguldījumu summu pasākumos, ja šī summa pārsniedz ECU 200 000,

— sadarbību ar organizācijām ārpus Kopienas jebkādos pasākumos saskaņā ar šo lēmumu,

— pasākumu rezultātu izplatīšanas, aizsardzības un izmantošanas noteikumiem,

— rīcības novērtēšanas pasākumiem.

3. Ja Kopienas ieguldījums pasākumos ir mazāks par vai vienāds ar ECU 200 000, tad Komisija apspriežas ar Komiteju par veicamajiem pasākumiem un informē Komiteju par tās novērtējuma rezultātiem.

7. pants

Komisijas pārstāvis iesniedz Komitejai veicamo pasākumu projektu. Komiteja sniedz atzinumu par šo projektu termiņā, ko nosaka priekšsēdētājs atkarībā no jautājuma steidzamības, vajadzības gadījumā par to balsojot.

Šo atzinumu ieraksta protokolā; turklāt katrai dalībvalstij ir tiesības pieprasīt, lai protokolā ieraksta tās nostāju.

Komisija īpaši ņem vērā Komitejas sniegto atzinumu. Komisija informē Komiteju par to, kā tās atzinums ir ņemts vērā.

8. pants

Komisijas pārstāvis iesniedz Komitejai veicamo pasākumu projektu. Komiteja sniedz atzinumu par šo projektu termiņā, ko nosaka priekšsēdētājs atkarībā no jautājuma steidzamības. Atzinumu sniedz ar balsu vairākumu, kas Eiropas Kopienas

dibināšanas līguma 148. panta 2. punktā noteikts attiecībā uz lēmumiem, kurus Padome pieņem pēc Komisijas priekšlikuma. Dalībvalstu pārstāvju balsis komitejā vērtē, kā noteikts minētajā pantā. Priekšsēdētājs nebalso.

Komisija pieņem paredzētos pasākumus, ja tie ir saskaņā ar Komitejas atzinumu.

Ja paredzētie pasākumi nav saskaņā ar Komitejas atzinumu vai ja Komiteja atzinumu nesniedz, tad Komisija tūlīt iesniedz Padomei priekšlikumu par veicamajiem pasākumiem. Padome pieņem lēmumu ar kvalificētu balsu vairākumu.

Ja trijos mēnešos pēc tam, kad šis jautājums nodots Padomei izskatīšanai, Padome lēmumu nav pieņēmusi, Komisija pieņem ierosinātos pasākumus, ja vien Padome ar vienkāršu balsu vairākumu nav pieņēmusi lēmumu pret minētajiem pasākumiem.

Briselē, 1992. gada 31. martā

Padomes vārdā —

priekšsēdētājs

Vitor MARTINS

PIELIKUMS

Rīcības virzienu kopsavilkums

ORIENTĒJOŠI NORĀDĪJUMI RĪCĪBAS PLĀNAM INFORMĀCIJAS SISTĒMU DROŠĪBAS JOMĀ

IEVADS

Rīcības plāna mērķis ir vispārēju stratēģiju veidošana, lai nodrošinātu elektroniski uzglabātas, apstrādātas vai pārraidītas informācijas lietotājus un veidotājus ar pienācīgu informācijas sistēmu aizsardzību pret nejašu vai apzinātu apdraudējumu.

Rīcības plāns ņem vērā un papildina vispasaules standartizācijas pasākumus šajā jomā.

Tas ietver šādus darbības virzienus:

- informācijas sistēmu drošības stratēģiskā pamata izveide,
- lietotāju un pakalpojumu sniedzēju prasību identificēšana saistībā ar informācijas sistēmu drošību,
- lietotāju, piegādātāju un pakalpojumu sniedzēju īstermiņa un vidēja termiņa vajadzību apmierināšana,
- specifikāciju, standartizācijas, novērtējuma un sertifikācijas izveide saistībā ar informācijas sistēmu drošību,
- tehnoloģiski un darbības jauninājumi informācijas sistēmu drošības jomā,
- informācijas sistēmu drošības ieviešana.

Rīcības plānu īsteno Komisija ciešā sasaistē ar attiecīgu dalībvalstu rīcību un saistībā ar attiecīgu Kopienas rīcību pētniecības un attīstības jomā.

1. I rīcības virziens — Informācijas sistēmu drošības stratēģiskā pamata izveide

atšķirīgiem apsvērumiem, mērķiem un ierobežojumiem. Tie ir priekšnoteikumi, lai saskaņotu intereses un vajadzības gan politikas veidošanā, gan rūpniecības attīstībā.

1.1. Problēma

Informācijas sistēmu drošība ir atzīta par vispārēji nepieciešamu elementu modernā sabiedrībā. Elektroniskās informācijas pakalpojumiem ir vajadzīga droša telekomunikāciju infrastruktūra, droša aparatūra un programmatūra, kā arī droša lietošana un pārvaldība. Ir jāievieš vispārēja stratēģija, apsverot visus informācijas sistēmu drošības aspektus un izvairoties no fragmentāras pieejas. Jebkurai stratēģijai, kas veltīta elektroniski apstrādātas informācijas drošībai, jāatspoguļo jebkuras sabiedrības vēlme efektīvi darboties, tomēr arī sevi aizsargāt pasaulē, kas strauji mainās.

1.2. Mērķis

Ir jāizveido stratēģiski orientēta sistēma, lai starptautiskā kontekstā saskaņotu Kopienas sociālos, ekonomiskos un politiskos mērķus ar tās tehniskajām, darbības un likumdošanas iespējām. Nozares dalībniekiem, kopā strādājot pie kopējas uztveres un saskaņotas stratēģijas sistēmas izveides, jārod trauslais līdzsvars starp

1.3. Stāvoklis un tendences

Situāciju raksturo augoša apziņa, ka jārikojas. Tomēr, tā kā trūkst iniciatīvas centienu koordinācijai, ir ļoti iespējams, ka izklaidētie centieni dažādās nozarēs *de facto* būs pretrunīgi, pamazām radot vairāk lielu juridisku, sociālu un ekonomisku problēmu.

1.4. Prasības, iespējas un prioritātes

Šādai kopējai sistēmai būtu jārisina un jāveic risku analīze un risku pārvaldība attiecībā uz informācijas un ar to saistīto pakalpojumu sensibilitāti, to tiesību aktu un noteikumu saskaņošana, kas saistīti ar datoru/telekomunikāciju ļaunprātīgu izmantošanu, administratīvo infrastruktūru, ieskaitot drošības politiku un tās efektīvu īstenošanu dažādās nozarēs un disciplīnās, un sabiedriskiem un privātās dzīves aizsardzības apsvērumiem (t.i. identificēšanas, autentificēšanas, nenoliedzamības un, iespējams, pilnvarošanas shēmu piemērošanu demokrātiskā vidē).

Ir jānodrošina skaidra ievirze, lai izveidotu droši izplatītas informācijas pakalpojumu fizisku un loģisku arhitektūru, garantētas drošības produktu un pakalpojumu standartus, vadlīnijas un definīcijas, modeļus un prototipus dažādu administratīvu struktūru dzīvotspējas nodrošināšanai, arhitektūras un standartus saistībā ar īpašu nozaru vajadzībām.

Ir jāveido izpratne par drošību, lai ietekmētu lietotāju attieksmi pret augošām bažām par drošību informācijas tehnoloģijās (IT).

2. II rīcības virziens — Lietotāju un pakalpojumu sniedzēju prasību identificēšana saistībā ar informācijas sistēmu drošību

2.1. Problēma

Informācijas sistēmu drošība ir uzņēmumiem paredzētu lietojumu programmu integritātes un drošuma, intelektuālā īpašuma un konfidencialitātes raksturīgs priekšnoteikums. Tas neizbēgami apgrūtina līdzsvara sasniegšanu un izvēli starp centieniem brīvās tirdzniecības jomā un centieniem privātuma nodrošināšanas un intelektuālā īpašuma aizsardzības jomā. Izvēlei un kompromisiem jābalstās uz pilnīgu prasību novērtējumu un to iespējamo izvēļu ietekmes novērtējumu, kas izdarītas, lai reaģētu uz šīm prasībām.

Lietotājiem ir vajadzīga tāda informācijas sistēmu drošības funkcionalitāte, kas būtu savstarpēji atkarīga ar tehnoloģiskiem, darbības un reglamentējošiem aspektiem. Tādējādi informācijas sistēmu drošības prasību sistematiska izpēte ir būtiska lietderīgu un efektīvu pasākumu izveides daļa.

2.2. Mērķis

Noteikt lietotāju un pakalpojumu sniedzēju prasību raksturu un iezīmes, un to saistību ar informācijas sistēmu drošības pasākumiem.

2.3. Stāvoklis un tendences

Līdz šim nav veikta saskaņota darbība, lai identificētu galveno dalībnieku prasības informācijas sistēmu drošības jomā, kas strauji attīstās un mainās. Kopienas dalībvalstis ir precizējušas prasības, lai saskaņotu valstu pasākumus (īpaši "IT drošības novērtēšanas kritērijus"). Ļoti būtiski ir vienoti novērtēšanas kritēriji un novērtēšanas sertifikātu savstarpējas atzīšanas noteikumi.

2.4. Prasības, iespējas un prioritātes

Lai vienotā un pārskatāmā veidā apmierinātu nozares dalībnieku pamatotas vajadzības, ir jāizveido saskaņota lietotāju prasību klasifikācija un tās saistība ar informācijas sistēmu drošības ieviešanu.

Ir svarīgi arī identificēt prasības tiesību aktiem un prakses kodeksiem, ņemot vērā pakalpojumu iezīmi un tehnoloģiju tendenču novērtējumu, identificēt alternatīvas mērķu īstenošanas stratēģijas, izmantojot administratīvus, pakalpojumu, darbības un tehniskus nosacījumus, un novērtēt alternatīvu drošības iespēju un stratēģiju efektivitāti, draudzīgumu lietotājiem un izmaksas informācijas sistēmu jomā saistībā ar lietotājiem, pakalpojumu sniedzējiem un operatoriem.

3. III rīcības virziens — Lietotāju, piegādātāju un pakalpojumu sniedzēju īstermiņa un vidēja termiņa vajadzību apmierināšana

3.1. Problēma

Pašlaik pienācīgi aizsargāt datorus pret nesankcionētu piekļuvi no ārpasaules ir iespējams, tos "izolējot", t.i., piemērojot standarta organizatoriskus un fiziskus pasākumus. Tas attiecas arī uz elektroniskām komunikācijām slēgtā lietotāju grupā, kas darbojas īpašā tīklā. Situācija ir pavisam atšķirīga, ja informāciju kopīgi lieto lietotāju grupas vai arī informācijas apmaiņa notiek, izmantojot publisku vai vispārpieejamu tīklu. Šajos gadījumos ne tehnoloģijas, termināļi un pakalpojumi, ne attiecīgie standarti un procedūras kopumā nespēj nodrošināt salīdzināmu informācijas sistēmu drošību.

3.2. Mērķis

Mērķis ir īsā laikā nodrošināt risinājumus, kas spēj apmierināt lietotāju, pakalpojumu sniedzēju un ražotāju steidzamākās vajadzības. Tas ietver arī kopēju IT drošības novērtēšanas kritēriju izmantošanu. Tie jāveido atvērta nākotnes prasībām un risinājumiem.

3.3. Stāvoklis un tendences

Dažas lietotāju grupas ir izveidojušas metodes un procedūras savai īpašai lietošanai, konkrēti, lai apmierinātu autentificēšanas, integritātes un nenoliedzamības vajadzības. Parasti izmanto magnētiskās kartes vai viedkartes. Citi izmanto sarežģītākas vai mazāk sarežģītas kriptogrāfiskas metodes. Bieži vien tas nozīmē, ka jādefinē lietotāju grupas īpašas "pilnvaras". Tomēr šos paņēmienus un metodes ir grūti vispārināt, lai tās atbilstu atvērtas vides prasībām.

ISO strādā pie OSI Informācijas sistēmu drošības (ISO DIS 7498-2) un CCITT darbojas saistībā ar standartu X400. Tāpat ir iespējams ziņojumos ievietot drošības segmentus. Autentificēšana, integritāte un nenoliedzamība jāuskata par ziņojumu (EDIFACT) daļu un X400 MHS daļu.

Pašlaik elektroniskās datu apmaiņas (EDI) tiesiskais regulējums vēl aizvien ir koncepcijas stadijā. Starptautiskā tirdzniecības palāta ir publicējusi vienus noteikumus darījumu datu apmaiņai, izmantojot sakaru tīklus.

Vairākas valstis (piem., Vācija, Francija, Apvienotā Karaliste un Amerikas Savienotās Valstis) ir izstrādājušas vai patlaban izstrādā kritērijus IT un telekomunikāciju produktu un sistēmu drošuma novērtēšanai, kā arī attiecīgas novērtēšanas procedūras. Šie kritēriji ir saskaņoti ar vietējiem ražotājiem un ļaus rasties aizvien lielākam skaitam uzticamu produktu un sistēmu, sākot ar vienkāršiem produktiem. Šo tendenci atbalstīs valstu organizāciju izveide, kas veiks novērtēšanu un piedāvās sertifikāciju.

Vairums lietotāju uzskata konfidencialitātes nodrošināšanu par tūlītēji mazāk svarīgu. Tomēr nākotnē šī situācija, visticamāk, mainīsies, attīstītiem sakaru, īpaši mobilo sakaru pakalpojumiem kļūstot vispārpieejamiem.

3.4. Prasības, iespējas un prioritātes

Ir būtiski cik drīz vien iespējams izveidot piemērotas procedūras, standartus, produktus un instrumentus, lai nodrošinātu drošību gan informācijas sistēmās vispār (datori, perifērās iekārtas), gan publiskos komunikāciju tīklos. Autentifikācijai, integritātei un nenoliedzamībai jāpiešķir īpaša prioritāte. Ir jāīsteno eksperimentāli projekti, lai pārliecinātos par ieteikto risinājumu derīgumu. Elektroniskās datu apmaiņas (EDI) prioritāro vajadzību risinājumus vispārīgākā šā rīcības plāna izpratnē pēta TEDIS programma.

4. IV rīcības virziens — Specifikāciju, standartizācijas, novērtējuma un sertifikācijas izveide saistībā ar informācijas sistēmu drošību

4.1. Problēma

Informācijas sistēmu drošības prasības ir visaptverošas, tādēļ ļoti būtiskas ir kopīgas specifikācijas un standarti. Saskaņotu standartu un specifikāciju trūkums IT drošības jomā var radīt nopietnus šķēršļus uz informāciju balstītu procesu un pakalpojumu attīstībai visā ekonomikā un sabiedrībā. Ir jāveic darbības, lai paātrinātu tehnoloģijas un standartu attīstību un izmantošanu vairākās saistītās sakaru un datortīklu jomās, kas ir sevišķi nozīmīgas lietotājiem, rūpniecībai un pārvaldes iestādēm.

4.2. Mērķis

Ir jācenšas nodrošināt līdzekļus īpašu drošības funkciju atbalstam un veikšanai OSI, ONP, ISDN/IBC un tīkla vadības galvenajās jomās. Ar standartizāciju un specifikāciju cieši saistītas ir verificēšanai vajadzīgās metodes un pieejas, ieskaitot sertifikāciju pirms savstarpējas atzišanas. Ja iespējams, ir jāatbalsta starptautiski saskaņoti risinājumi. Ir jārosina arī tādu datorsistēmu attīstība un lietošana, kam ir drošības funkcijas.

4.3. Stāvoklis un tendences

Īpaši Amerikas Savienotās Valstis ir uzņēmušās lielāko iniciatīvu informācijas sistēmu drošības jautājuma risināšanā. Eiropā šo jautājumu risina saistībā ar IT un telekomunikāciju standartizāciju, sasaistē ar Eiropas Telekomunikāciju Standartu institūtu (ETSI) un CEN/CENELEC, sagatavojot CCITT un ISO darbu šajā jomā.

Ņemot vērā augošās bažas, darbu Amerikas Savienotajās Valstīs strauji intensificē un gan pārdevēji, gan pakalpojumu sniedzēji pastiprina pūles šajā jomā. Eiropā Francija, Vācija un Apvienotā Karaliste ir neatkarīgi sākušas līdzīgas darbības, taču kopējie centieni, salīdzinot ar Amerikas Savienotajām Valstīm, attīstās lēni.

4.4. Prasības, iespējas un prioritātes

Informācijas sistēmu drošības jomai ir raksturīga ļoti cieša saikne starp reglamentējošiem, darbības, administratīviem un tehniskiem aspektiem. Regulējumi jāatspoguļo standartos, un informācijas sistēmu drošības noteikumiem jānodrošina veidā jāatbilst standartiem un regulējumiem. Vairākos aspektos regulējumiem vajadzīgas tādas specifikācijas, kas iziet ārpus standartizācijas robežām, t.i., tie ietver prakses kodeksus. Visās informācijas sistēmu drošības jomās ir standarti un prakses kodeksi, tādēļ ir jānoskaidro aizsardzības prasības, kas atbilst drošības mērķiem, no tehniskām prasībām, kuras var uzticēt kompetentām Eiropas standartu struktūrām (CEN/CENELEC/ETSI).

Specifikācijām un standartiem ir jāaptver šādas tēmas: informācijas sistēmu drošības pakalpojumi (personālā un uzņēmumu autentifikācija, nenoliedzamības protokoli, tiesiski pieļaujami elektroniski pierādījumi, pilnvarošanas kontrole), to komunikāciju pakalpojumi (attēlu pārraides privātums, mobilo sakaru balss un datu privātums, datu un attēlu datu bāzu aizsardzība, integrētu pakalpojumu drošība), to komunikāciju un drošības pārvaldība (publiskās/privātās atslēgas sistēma darbībai atvērtā tīklā, tīkla vadības aizsardzība, pakalpojumu sniedzēja aizsardzība) un to sertifikācija (nodrošinājuma kritēriji un līmeņi, drošības nodrošinājuma procedūras drošām informācijas sistēmām).

5. V rīcības virziens — Tehnoloģiski un darbības jauninājumi informācijas sistēmu drošības jomā

5.1. Problēma

Sistemātiska tehnoloģijas pētīšana un attīstīšana, lai radītu ekonomiski stabilus un darbībai apmierinošus risinājumus daudzām esošām un nākotnes prasībām saistībā ar informācijas sistēmu drošību, ir priekšnoteikums pakalpojumu tirgus attīstībai un Eiropas ekonomikas konkurētspējai kopumā.

Jebkādiem tehnoloģiskiem jauninājumiem informācijas sistēmu drošības jomā jāietver gan datoru drošība, gan komunikāciju drošība, jo vairums esošo sistēmu ir daļējas sistēmas, un šādām sistēmām piekļūst ar komunikāciju pakalpojumu starpniecību.

5.2. Mērķis

Sistemātiska tehnoloģijas pētīšana un attīstīšana, lai radītu ekonomiski stabilus un darbībai apmierinošus risinājumus daudzām esošām un nākotnes prasībām informācijas sistēmu drošībai.

5.3. Prasības, iespējas un prioritātes

Darbam pie informācijas sistēmu drošības vajadzētu būt vērstam uz stratēģiju attīstību un īstenošanu, tehnoloģijām, integrēšanu un verificēšanu.

Stratēģiskajam pētniecības un attīstības darbam būtu jāaptver drošu sistēmu konceptuālie modeļi (drošas pret negatīvu ietekmi, nesankcionētiem grozījumiem un pakalpojuma atteikumu), funkcionālo prasību modeļi, riska modeļi un drošības arhitektūras.

Uz tehnoloģiju orientētam pētniecības un attīstības darbam būtu jāietver lietotāja un ziņojuma autentificēšana (piemēram, izmantojot balss analīzi un elektroniskos parakstus), šifrēšanas tehniskās saskarnes un protokoli, piekļuves kontroles mehānismi un pārbaudāmi drošu sistēmu ieviešanas metodes.

Tehniskās sistēmas drošības un piemērojamības verificēšanu un validēšanu pētītu integrēšanas un verificēšanas projektos.

Līdztekus drošības tehnoloģijas konsolidēšanai un attīstībai, ir vajadzīgi vairāki papildu pasākumi attiecībā uz standartu radīšanu, uzturēšanu un vienotu piemērošanu, un uz IT un telekomunikāciju produktu validēšanu un sertifikāciju saistībā ar to drošības īpašībām, ieskaitot sistēmu izveides un ieviešanas metožu validēšanu un sertifikēšanu.

Trešo Kopienas pētniecības un tehnoloģijas attīstības pamatprogrammu var izmantot, lai stiprinātu sadarbības projektus pirmskonkurences un pirmsnormatīvos līmeņos.

6. VI rīcības virziens — Informācijas sistēmu drošības ieviešana

6.1. Problēma

Atkarībā no informācijas sistēmu drošības pazīmju konkrētajām īpašībām, vajadzīgās funkcijas jāiekļauj dažādās informācijas sistēmas daļās, ieskaitot termināļus/datorus, pakalpojumus, kriptogrāfisko ierīču tīkla vadību, viedkartes, publiskās un privātās atslēgas utt. Var sagaidīt, ka dažas no tām būs iestrādātas pārdevēju piedāvātajā aparātūrā vai programmatūrā, kamēr citas var ietilpt dalītās sistēmās (piem., tīklu vadība), būt individuālā lietotāja īpašumā (piem., viedkartes), vai tās var nodrošināt specializēta organizācija (piem., publiskās/privātās atslēgas).

Ir gaidāms, ka vairumu drošības produktu un pakalpojumu piedāvās pārdevēji, pakalpojumu sniedzēji vai operatori. Specifisku funkciju veikšanai, piemēram, nodrošināšanai ar publiskām/privātām atslēgām, pilnvarošanas auditam, var būt vajadzība noteikt un pilnvarot atbilstošas organizācijas.

Tas pats attiecas uz sertifikāciju, pakalpojumu kvalitātes novērtēšanu un pārbaudi, kas ir funkcijas, kuras jāveic no pārdevēju, pakalpojumu sniedzēju vai operatoru interesēm neatkarīgām organizācijām. Tās var būt privātas, valsts vai valsts licencētas organizācijas, kas veic deleģētās funkcijas.

6.2. Mērķis

Lai sekmētu saskaņotu informācijas sistēmu drošības ieviešanas attīstību Kopienā ar mērķi aizsargāt sabiedriskās un uzņēmējdarbības intereses, būs jāizveido vienota pieeja drošības ieviešanai. Ja jāpilnvaro neatkarīgas organizācijas, tad to funkcijas un nosacījumi jādefinē un jānosaka un vajadzības gadījumā jāietver reglamentējošos noteikumus. Mērķis būtu nonākt pie skaidri definēta un saskaņota dažādu dalībnieku atbildības sadalījuma Kopienas līmenī, kas ir savstarpējas atziņas priekšnoteikums.

6.3. Stāvoklis un tendences

Pašlaik informācijas sistēmu drošības ieviešana ir labi organizēta tikai specifiskās jomās un aprobežojas ar to specifisko vajadzību apmierināšanu. Organizācija Eiropas līmenī lielākoties ir neformāla, un ārpus slēgtām grupām vēl nav izveidota verificēšanas un sertifikācijas savstarpēja atzišana. Tā kā informācijas sistēmu drošība kļūst aizvien nozīmīgāka, tad arvien steidzamāka kļūst vajadzība definēt vienotu pieeju informācijas sistēmu drošības ieviešanai Eiropā un starptautiski.

6.4. Prasības, iespējas un prioritātes

Nemot vērā ieinteresēto dalībnieku skaitu un ciešās saiknes ar reglamentējošiem un likumdošanas jautājumiem, sevišķi svarīgi ir iepriekš vienoties par principiem, kas attiecas uz informācijas sistēmu drošības ieviešanu.

Attīstot vienotu pieeju šim jautājumam, būs jārisina jautājums par to funkciju identificēšanu un precizēšanu, kam, pēc būtības, vajadzīga neatkarīgu organizāciju (vai kopdarba organizāciju) līdzdalība. Tas varētu ietvert tādas funkcijas kā publisko/privāto atslēgu sistēmas pārvaldība.

Bez tam, jau pašā sākumā ir jāidentificē un jāprecizē tās funkcijas, kas sabiedrības interesēs uzticamas neatkarīgām organizācijām (vai kopdarba organizācijām). Tās varētu ietvert, piemēram, auditu, kvalitātes nodrošināšanu, verificēšanu, sertifikāciju un tamlīdzīgas funkcijas.