31992D0242

NÕUKOGU OTSUS, 31. märts 1992, infosüsteemide turvalisuse kohta

(92/242/EMÜ)

EUROOPA ÜHENDUSTE NÕUKOGU,

võttes arvesse Euroopa Majandusühenduse asutamislepingut, eriti selle artiklit 235,

võttes arvesse komisjoni ettepanekut, ([1])

võttes arvesse Euroopa Parlamendi arvamust, ([2])

võttes arvesse majandus- ja sotsiaalkomitee arvamust ([3])

ning arvestades, et:

ühenduse ülesanne on ühisturu rajamise ning liikmesriikide majanduspoliitika järkjärgulise ühtlustamise kaudu edendada ühenduse kõigis osades majandustegevuse arengut, pidevat ja tasakaalustatud laienemist, stabiilsuse kasvu, elatustaseme kiiret paranemist ning tihedamaid suhteid liikmesriikide vahel;

elektrooniliselt salvestataval, töödeldaval ja edastataval teabel on üha olulisem roll majandustegevuses ja ühiskondlikus elus;

tõhusa ülemaailmse kommunikatsioonivõrgu kasutuselevõtmine ja elektroonilise infotöötluse ulatuslik kasutamine rõhutavad piisava kaitse vajalikkust;

Euroopa Parlament on oma aruteludes ja resolutsioonides korduvalt rõhutanud infosüsteemide turvalisuse tähtsust;

majandus- ja sotsiaalkomitee on rõhutanud vajadust tegeleda infosüsteemide turvalisust käsitlevate küsimustega ühenduse tegevuse ja meetmete kaudu, pidades eelkõige silmas siseturu väljakujundamise mõju;

siseriiklikul, rahvusvahelisel ja ühenduse tasandil võetavad meetmed on sellisele tegevusele heaks aluseks;

telekommunikatsioon, infotehnoloogia, standardimine, infoturg ning uurimis- ja arendustegevuse ja tehnoloogia arendamise tegevuspõhimõtted on omavahel tihedalt seotud ning ühtlasi on need seotud ka ühenduse tasandil nendes valdkondades juba tehtud tööga;

on asjakohane teha ühiseid jõupingutusi, tuginedes olemasolevale siseriiklikule ja rahvusvahelisele tegevusele ning soodustades kõige tähtsamate osapoolte vahelist koostööd; seepärast on asjakohane jätkata tegevust kooskõlastatud tegevuskava raames;

infosüsteemide turvalisuse keerukus eeldab selliste strateegiate koostamist, mis võimaldavad teabe vaba liikumist ühtsel turul, tagades samal ajal infosüsteemide kasutamise turvalisuse kogu ühenduses;

iga liikmesriik on kohustatud arvesse võtma turvalisusest ja avalikust korrast tulenevaid piiranguid;

liikmesriikide kohustused selles valdkonnas eeldavad ühise lähenemisviisi olemasolu, mis põhineb tihedal koostööl liikmesriikide kõrgemate ametnikega;

tuleks ette näha tegevuskava esimeseks 24 kuuks ning moodustada kõrgemate ametnike komitee, kellel on pikaajalised volitused nõustada komisjoni infosüsteemide turvalisuse valdkonda käsitlevate tegevuskavade osas;

tegevuse elluviimiseks on esimese 24 kuu jooksul vaja hinnanguliselt 12 miljonit eküüd; käesolevas finantsperspektiivis peetakse 1992. aastaks vajalikuks 2 miljonit eküüd;

pärast 1992. eelarveaastat programmi rahastamiseks eraldatavad summad peavad moodustama osa ühenduse kehtivast finantssüsteemist,

ON VASTU VÕTNUD JÄRGMISE OTSUSE:

Artikkel 1

Käesolevaga võetakse vastu infosüsteemide turvalisuse valdkonda käsitlev meede. See koosneb järgmistest osadest:

— infosüsteemide turvalisust käsitlevate üldstrateegiate (tegevuskava) koostamine esimeseks 24 kuuks, ning

— kõrgemate ametnike rühma (edaspidi "komitee") moodustamine, kellel on pikaajalised volitused nõustada komisjoni infosüsteemide turvalisuse valdkonda käsitlevate meetmete osas.

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

Artikkel 2

1. Komisjon konsulteerib komiteega järjekindlalt ühenduse eri meetmetega seotud infosüsteemide turvalisust käsitlevates küsimustes, eelkõige tööstrateegiate ja programmide määratlemisel.

2. Lisas esitatud tegevuskava hõlmab ettevalmistavat tööd järgmistes küsimustes:

I. infosüsteemide turvalisust käsitleva strateegilise raamistiku koostamine;

II. kasutajate ja teenuste pakkujate poolt infosüsteemide turvalisusele esitatavate nõuete kindlakstegemine;

III. kasutajate, tarnijate ja teenuste pakkujate lühikese ja keskpika tähtajaga vajaduste rahuldamine;

IV. infosüsteemide turvalisust käsitlevate spetsifikatsioonide, standardimise, hindamise ja sertifitseerimise väljatöötamine;

V. infosüsteemide turvalisusega seotud tehnoloogia ja tegevuse arendamine;

VI. infosüsteemide turvalisuse tagamine.

Artikkel 3

1. Meetme rakendamiseks vajalikud ühenduse vahendid on algperioodil hinnanguliselt 12 miljonit eküüd, sealhulgas 2 miljonit eküüd 1992. aastaks, arvestades aastate 1988–1992 finantsperspektiivi.

Programmi edasisel elluviimisel peab finantsvahendite hulk moodustama osa ühenduse kehtivast finantssüsteemist.

2. Eelarve täitmist korraldav asutus määrab igaks rahandusaastaks saadavad vahendid, võttes arvesse Euroopa ühenduste üldeelarve suhtes kohaldatava finantsmääruse artiklis 2 osutatud usaldusväärse juhtimise põhimõtteid.

Artikkel 4

Algperioodil tehtud edusamme hindab komisjoni nimel sõltumatute ekspertide rühm. Rühma aruanne koos komisjoni võimalike märkustega esitatakse Euroopa Parlamendile ja nõukogule.

Artikkel 5

1. Komisjon vastutab meetme rakendamise eest. Komisjoni abistab nõuandekomitee, kuhu kuuluvad liikmesriikide esindajad ja eesistujana komisjoni esindaja.

2. Tegevuskava rakendamine toimub kooskõlas artiklis 2 sätestatud eesmärkidega ja seda ajakohastatakse vastavalt vajadusele. Selles esitatakse üksikasjalikud eesmärgid ja võetavate meetmete liigid ning nendega seotud rahastamiskord. Komisjon teeb üleskutse tegevuskaval põhinevate ettepanekute esitamiseks.

3. Tegevuskava rakendamine toimub tihedas koostöös sektori ettevõtjatega. Seejuures võetakse arvesse, edendatakse ja täiustatakse kõnealuses valdkonnas Euroopa ja rahvusvahelisel tasandil juba olemasolevaid standardimismeetmeid.

Artikkel 6

1. Artiklis 7 sätestatud korda kohaldatakse:

— meetmete suhtes, mis on seotud ühenduse poliitikaga infosüsteemide turvalisuse valdkonnas.

2. Artiklis 8 sätestatud korda kohaldatakse järgmistel juhtudel:

— artiklis 5 nimetatud tegevuskava ettevalmistamine ja ajakohastamine,

— ettepanekute esitamist käsitlevate üleskutsete sisu, ettepanekute hindamine ja ühenduse hinnangulise osaluse kindlaksmääramine meetmetes, kui see ületab 200 000 eküüd,

— ühenduseväliste organisatsioonide koostöö käesoleva otsuse kohases tegevuses,

— meetmete tulemuste levitamise, kaitsmise ja kasutamise kord,

— tegevuse hindamiseks võetavad meetmed.

3. Kui ühenduse osalus meetmetes on kõige rohkem 200 000 eküüd, konsulteerib komisjon komiteega vajalike meetmete osas ning teavitab komiteed hindamise tulemustest.

Artikkel 7

Komisjoni esindaja esitab komiteele võetavate meetmete eelnõu. Tähtaja jooksul, mille määrab eesistuja lähtuvalt küsimuse kiireloomulisusest, esitab komitee eelnõu kohta oma arvamuse, vajaduse korral hääletades.

Arvamus protokollitakse; lisaks sellele on liikmesriigil õigus taotleda oma seisukoha protokollimist.

Komisjon arvestab võimalikult suurel määral komitee arvamust. Ta teatab komisjonile, kuidas arvamust on arvesse võetud.

Artikkel 8

Komisjoni esindaja esitab komiteele võetavate meetmete eelnõu. Tähtaja jooksul, mille määrab eesistuja lähtuvalt küsimuse kiireloomulisusest, esitab komitee eelnõu kohta arvamuse. Arvamus esitatakse sellisehäälteenamusega, nagu on sätestatud

asutamislepingu artikli 148 lõikes 2 nõukogu otsuste vastuvõtmiseks komisjoni ettepaneku põhjal. Liikmesriikide esindajate hääli komitees arvestatakse kõnealuses artiklis sätestatud viisil. Eesistuja ei hääleta.

Kui meetmed on komitee arvamusega kooskõlas, võtab komisjon need vastu.

Kui kavandatud meetmed ei ole komitee arvamusega kooskõlas või kui arvamust ei ole esitatud, esitab komisjon võetavate meetmete kohta viivitamata ettepaneku nõukogule. Nõukogu teeb otsuse kvalifitseeritud häälteenamusega.

Kui nõukogu ei ole kolme kuu jooksul alates ettepaneku saamisest otsust teinud, võtab komisjon ettepandud meetmed vastu, juhul kui nõukogu ei ole lihthäälteenamusega mainitud meetmete vastu.

Brüssel, 31. märts 1992

Nõukogu nimel

eesistuja

Vitor MARTINS

LISA

Tegevussuuniste kokkuvõte

SUUNISED TEGEVUSKAVA KOOSTAMISEKS INFOSÜSTEEMIDE TURVALISUSE VALDKONNAS

SISSEJUHATUS

Tegevuskava eesmärk on üldstrateegiate koostamine selleks, et tagada elektrooniliselt salvestatava, töödeldava või edastatava teabe kasutajatele ja tootjatele infosüsteemide asjakohane kaitse juhuslike või tahtlike ohtude eest.

Tegevuskavas võetakse arvesse ja täiustatakse kõnealuses valdkonnas ülemaailmsel tasandil juba olemasolevaid standardimismeetmeid.

See hõlmab järgmisi tegevussuuniseid:

— infosüsteemide turvalisust käsitleva strateegilise raamistiku koostamine,

— kasutajate ja teenuste pakkujate poolt infosüsteemide turvalisusele esitatavate nõuete kindlakstegemine,

— kasutajate, tarnijate ja teenuste pakkujate lühikese ja keskpika tähtajaga vajaduste rahuldamine,

— infosüsteemide turvalisust käsitlevate spetsifikatsioonide, standardimise, hindamise ja sertifitseerimise väljatöötamine,

— infosüsteemide turvalisusega seotud tehnoloogia ja tegevuse arendamine,

— infosüsteemide turvalisuse tagamine.

Tegevuskava rakendab komisjon tihedas koostöös liikmesriikide seonduvate meetmetega ning ühenduse asjakohaste uurimis- ja arendustegevuse meetmetega.

1. **Tegevussuunis I — Infosüsteemide turvalisust käsitleva strateegilise raamistiku koostamine**

1.1. *Teema*

Infosüsteemide turvalisust peetakse kaasaegse ühiskonna vältimatult vajalikuks aspektiks. Elektrooniliste infoteenuste jaoks on vaja turvalist telekommunikatsiooni infrastruktuuri, turvalist riist- ja tarkvara ning turvalist kasutus- ja halduskeskkonda. Tuleb koostada üldstrateegia, milles võetakse arvesse infosüsteemide kõiki aspekte ning välditakse killustatud lähenemisviisi. Elektrooniliselt töödeldava informatsiooni turvalisust käsitlev strateegia peab kajastama mis tahes ühiskonna soovi toimida tõhusalt, kuid kaitsta end samal ajal kiiresti muutuvas maailmas.

1.2. *Eesmärk*

Tuleb koostada strateegiline raamistik ühiskondlike, majanduslike ja poliitiliste eesmärkide kooskõlastamiseks ühenduse tehniliste, toimimisega seotud ja õiguslike valikuvõimalustega rahvusvahelises kontekstis. Sektori ettevõtjad peavad leidma tundliku tasakaalu erinevate seisukohtade, eesmärkide ja piirangute vahel, tehes koostööd ühise arusaama kujundamisel ja kooskõlastatud strateegilise raamistiku koostamisel. Need tingimused on eeltingimuseks huvide ja vajaduste kooskõlastamisele nii poliitiliste otsuste tegemisel kui ka tööstuse arendamisel.

1.3. *Praegune olukord ja suundumused*

Olukorda iseloomustab suurenev teadlikkus vajadusest tegutseda. Tegevust kooskõlastava algatuse puudumisel tundub väga tõenäoline, et eri sektorites võetavad hajutatud meetmed loovad *de facto* vastuolulise olukorra, mis tekitab üha tõsisemaid juriidilisi, ühiskondlikke ja majanduslikke probleeme.

1.4. *Nõuded, valikuvõimalused ja prioriteedid*

Sellise ühise raamistiku kontekstis tuleb käsitleda ja piiritleda riskianalüüsi ja riskijuhtimist, mis on seotud informatsiooni ja seonduvate teenuste haavatavusega, arvutite/telekommunikatsiooni kuritarvitamist ja väärtarvitamist käsitlevate õigusnormide vastavusseviimisega, halduslike infrastruktuuridega, sealhulgas julgeolekupoliitikaga, ja nende tõhusa rakendamisega eri tööstusharudes/valdkondades, ning ühiskondlikku elu ja eraelu puudutavate küsimustega (nt identifitseerimis-, autentimis-, tunnustamis- ja võimalike autoriseerimiskavade kohaldamine demokraatlikus keskkonnas).

Tuleb koostada selged juhised, et töötada välja turvaliste hajutatud teabeteenuste füüsilised ja loogilised arhitektuurid, usaldusväärseid turbetooteid ja -teenuseid käsitlevad standardid, juhised ja määratlused, ning katseprojektid ja prototüübid, mida on vaja selleks, et teha kindlaks konk-reet-se-te sektorite vajadustega seotud erinevate haldusstruktuuride, arhitektuuride ja standardite elujõulisus.

Tuleb tõsta teadlikkust turvalisusega seotud küsimustes, et kasutajad pööraksid infotehnoloogia turvalisusele rohkem tähelepanu.

2. **Tegevussuunis II — Kasutajate ja teenuste pakkujate poolt infosüsteemide turvalisusele esitatavate nõuete kindlakstegemine**

2.1. *Teema*

Infosüsteemide turvalisus on vältimatu eeltingimus ärirakenduste terviklikkuse ja usaldusväärsuse ning intellektuaalomandi ja konfidentsiaalsuse kaitse tagamisel. Sellega kaasneb paratamatult keerukas tasakaalu saavutamine ja valikute tegemine ühelt poolt vabakaubandust ning teiselt poolt eraelu puutumatuse ja intellektuaalomandi kaitset käsitlevate kohustuste vahel. Need valikud ja kompromissid peavad põhinema nõuete täielikul mõistmisel ning kaalutlusel, kas infosüsteemide turvalisuse valdkonnas tehtavad võimalikud valikud suudavad neid nõudeid täita.

Kasutajate nõuded käsitlevad infosüsteemide turbefunktsioone tehnoloogiliste, toimimisega seotud ja regulatiivsete aspektide kontekstis. Seepärast on infosüsteemide turvanõuete süsteemsel uurimisel oluline osa asjakohaste ja tõhusate meetmete kavandamisel.

2.2. *Eesmärk*

Tuleb teha kindlaks kasutajate ja teenuste pakkujate nõuete laad ja olemus ning nende seotus infosüsteemide turbemeetmetega.

2.3. *Praegune olukord ja suundumused*

Seni ei ole tehtud ühiseid jõupingutusi, et selgitada välja põhiliste ettevõtjate kiiresti arenevad ja muutuvad nõuded infosüsteemide turvalisusele. Ühenduse liikmesriigid on välja selgitanud siseriikliku tegevuse (eelkõige "infotehnoloogia turvalisuse hindamiskriteeriumide") ühtlustamisega seotud nõuded. Väga olulise tähtsusega on ühtsed hindamiskriteeriumid ja hindamissertifikaatide vastastikust tunnustamist käsitlevad eeskirjad.

2.4. *Nõuded, valikuvõimalused ja prioriteedid*

Sektori ettevõtjate põhjendatud vajaduste järjekindla ja läbipaistva käsitlemise lähtealusena on vaja koostada kasutajanõuete kooskõlastatud liigitus ja teha kindlaks selle seotus infosüsteemide turvalisuse tagamisega.

Peale selle on oluline teha kindlaks vajadus õigus-ak-ti-de, määruste ja tegevusjuhiste järele, pidades silmas teenuste omaduste ja tehnoloogia suundumuste hindamist, määrata kindlaks alternatiivsed strateegiad eesmärkide saavutamiseks halduslike, teenuseid ja tegevust käsitlevate ning tehniliste sätete kaudu, ning hinnata infosüsteemide alternatiivsete turbevõimaluste ja -strateegiate tõhusust, kasutajasõbralikkust ja kulusid kasutajate, teenuste pakkujate ja operaatorite seisukohalt.

3. **Tegevussuunis III — Kasutajate, tarnijate ja teenuste pakkujate lühikese ja keskpika tähtajaga vajaduste rahuldamine**

3.1. *Teema*

Praegu on võimalik arvuteid piisavalt kaitsta kõrvaliste isikute volitamata juurdepääsu eest "eraldamise" abil, st kohaldades tavapäraseid korralduslikke ja füüsilisi meetmeid. See kehtib ka kinnise kasutajarühma poolt erivõrgus kasutatava elektroonilise side puhul. Olukord on hoopis teistsugune, kui teavet jagatakse eri kasutajarühmade vahel või seda vahetatakse avaliku või üldiselt ligipääsetava võrgu kaudu. Sellistel juhtudel puuduvad infosüsteemide võrreldava turbe tagamiseks vajalik tehnoloogia, terminalid ja teenused ning ka seonduvad standardid ja menetlused.

3.2. *Eesmärk*

Tuleb leida lühikese aja jooksul lahendused kasutajate, teenuste pakkujate ja tootjate kõige kiireloomulisemate vajaduste rahuldamiseks. See hõlmab infotehnoloogia turvalisuse ühiste hindamiskriteeriumide kasutamist. Neid peaks olema võimalik kohandada, et võtta arvesse edasisi nõudeid ja lahendusi.

3.3. *Praegune olukord ja suundumused*

Mõningad kasutajarühmad on koostanud enda konkreetseid kasutusvajadusi arvestavad meetodid ja menetlused, mis vastavad eelkõige autentimise, ehtsuse ja tunnustamisega seotud nõuetele. Üldjuhul kasutatakse magnetkaarte või kiipkaarte. Kasutatakse ka lihtsamaid ja keerukamaid krüptograafilisi meetodeid. See tähendab sageli kasutajarühmade enda "ametivõimude" määratlemist. Selliseid meetodeid on siiski raske üldistada, et vastata avatud keskkonna vajadustele.

ISO püüab praegu välja töötada OSI infosüsteemide turbestandardit (ISO DIS 7498-2) ning sama teeb X400 kontekstis ka CCITT. Turbesegmente on võimalik lisada ka sõnumitele. Autentimist, ehtsust ja tunnustamist käsitletakse osana sõnumitest (EDIFACT) ja süsteemist X400 MHS.

Elektroonilist andmevahetust käsitlev õiguslik raamistik on praegu alles kavandamisjärgus. Rahvusvaheline Kaubanduskoda on avaldanud ühtsed tegutsemiseeskirjad äriandmete vahetuseks telekommunikatsioonivõrkude kaudu.

Mitmed riigid (nt Saksamaa, Prantsusmaa, Ühendkuningriik ja Ameerika Ühendriigid) on välja töötamas või juba välja töötanud infotehnoloogia ning telekommunikatsioonitoodete ja -süsteemide usaldusväärsuse hindamiskriteeriumeid ning asjakohaseid hindamismenetlusi. Need kriteeriumid on kooskõlastatud siseriiklike tootjatega ja tänu nendele on võimalik välja töötada üha rohkem usaldusväärseid tooteid ja süsteeme, alustades väga lihtsatest toodetest. Seda suundumust toetab hindamisi läbiviivate ja sertifikaate väljastavate siseriiklike organisatsioonide loomine.

Konfidentsiaalsuse tagamist peab valdav osa kasutajaid vähem kiireloomuliseks küsimuseks. Tulevikus see olukord tõenäoliselt muutub seoses kõrgetasemeliste sideteenuste, eelkõige mobiilsideteenuste üldise ulatusliku levikuga.

3.4. *Nõuded, valikuvõimalused ja prioriteedid*

On oluline võimalikult kiiresti välja töötada asjakohased menetlused, standardid, tooted ja vahendid nii infosüsteemide kui selliste (arvutid, välisseadmed) kui ka üldkasutatavate sidevõrkude turvalisuse tagamiseks. Esmatähtsaks tuleb pidada autentimise, ehtsuse ja tunnustamisega seotud küsimusi. Esitatud lahenduste asjakohasuse väljaselgitamiseks tuleb korraldada katseprojekte. Elektroonilise andmevahetuse esmatähtsate vajaduste lahendusi käsitletakse programmis TEDIS käesoleva tegevuskava üldisemas kontekstis.

4. Tegevussuunis IV — Infosüsteemide turvalisust käsitlevate spetsifikatsioonide, standardimise, hindamise ja sertifitseerimise väljatöötamine

4.1. *Teema*

Infosüsteemide turbenõuded puudutavad eri valdkondi ning seetõttu on ühistel spetsifikatsioonidel ja standarditel otsustav tähtsus. Infotehnoloogia turvalisust käsitlevate kokkulepitud standardite ja spetsifikatsioonide puudumine võib oluliselt takistada teabepõhiste protsesside ja teenuste arengut majanduses ja ühiskonnas tervikuna. Peale selle tuleb võtta meetmeid tehnoloogia ja standardite arendamise ja kasutamise kiirendamiseks paljudes side- ja arvutivõrkudega seotud valdkondades, millel on kasutajate, tööstuse ja halduse seisukohalt otsustav tähtsus.

4.2. *Eesmärk*

Tuleb leida vahendid konk-reet-se-te turbefunktsioonide toetamiseks ja rakendamiseks OSI, ONP, ISDN/IBC üldistes valdkondades ning võrkude haldamisel. Standardimise ja spetsifikatsioonidega on lahutamatult seotud kontrollimiseks vajalikud meetodid ja põhimõtted, sealhulgas vastastikust tunnustamist võimaldav sertifitseerimine. Võimaluse korral tuleks toetada rahvusvaheliselt kokkulepitud lahendusi. Ühtlasi tuleks soodustada turbefunktsioonidega arvutisüsteemide arendamist ja kasutamist.

4.3. *Praegune olukord ja suundumused*

Eelkõige Ameerika Ühendriigid on teinud märkimisväärseid algatusi infosüsteemide turvalisuse valdkonnas. Euroopas käsitlevad seda teemat infotehnoloogia ja telekommunikatsiooni standardimise valdkonnas ETSI ja CEN/CENELEC, et valmistada ette CCITT ja ISO tegevust nimetatud valdkonnas.

Kuna kõ-ne-alu-ne teema muutub järjest aktuaalsemaks, hoogustub tegevus Ameerika Ühendriikides järjest enam ning nii tarnijad kui ka teenuste pakkujad püüavad võtta rohkem asjakohaseid meetmeid. Euroopas on Prantsusmaa, Saksamaa ja Ühendkuningriik alustanud üksteisest sõltumatult samalaadset tegevust, kuid Ameerika Ühendriikides tehtava koostööga võrreldav ühistegevus areneb siiski väga aeglaselt.

4.4. *Nõuded, valikuvõimalused ja prioriteedid*

Infosüsteemide turvalisuse valdkonnas on omavahel väga tihedalt seotud regulatiivsed, tegevust käsitlevad, halduslikud ja tehnilised aspektid. Õigusaktid peavad kajastuma standardites ning infosüsteemide turvalisuse tagamiseks võetavad meetmed peavad olema kontrollitavalt kooskõlas standardite ja määrustega. Õigusaktidega tuleb mitmetes küsimustes kehtestada spetsifikatsioonid, mis on standardimise tavapärasest mõistes ulatuslikumad, st hõlmavad tegevusjuhiseid. Standardite ja tegevusjuhistega seotud nõuded puudutavad kõiki infosüsteemide turvalisuse valdkondi ning seetõttu tuleb eristada turbe-eesmärkidele vastavaid kaitsenõudeid ja mõningaid tehnilisi nõudeid, mille täitmise võib usaldada pädevatele Euroopa standardiorganisatsioonidele (CEN/CENELEC/ETSI).

Spetsifikatsioonid ja standardid peavad hõlmama infosüsteemide turbeteenuste valdkondi (isikute ja ettevõtete autentimine, tunnustamise protokollid, õiguslikult vastuvõetav elektrooniline tõendamine, autoriseerimiskontroll), nende sideteenuseid (piltsõnumite privaatsus, kõne- ja andmeedastusteenuste privaatsus mobiilsides, andmebaaside ja pildimaterjali sisaldavate andmebaaside kaitse, integraalteenuste turve), nende side ja turvalisuse haldust (avalik/isiklik võtmesüsteem avatud võrgu toimimisel, võrguhalduse kaitse, teenuste pakkujate kaitse) ning nende sertifitseerimist (turvalisuse tagamise kriteeriumid ja tasandid, turvatud infosüsteemide turvalisuse tagamise menetlused).

5. Tegevussuunis V — Infosüsteemide turvalisusega seotud tehnoloogia ja tegevuse arendamine

5.1. *Teema*

Tehnoloogia süsteemne uurimine ja arendamine majanduslikult elujõuliste ja rahuldavalt toimivate lahenduste leidmiseks mitmetele praegustele ja tulevastele infosüsteemide turbenõuetele on teenusteturu arengu ja Euroopa majanduse kui terviku konkurentsivõimelisuse tagamise eeltingimus.

Infosüsteemide turvalisusega seotud tehnoloogia areng peab hõlmama nii arvuti- kui ka sideturbe aspekte, sest valdav osa tänapäeva süsteemidest on hajutatud ning juurdepääs sellistele süsteemidele toimub sideteenuste kaudu.

5.2. *Eesmärk*

Tehnoloogiat tuleb süsteemselt uurida ja arendada, et leida majanduslikult elujõulised ja rahuldavalt toimivad lahendused mitmetele praegustele ja tulevastele infosüsteemide turbenõuetele.

5.3. *Nõuded, valikuvõimalused ja prioriteedid*

Infosüsteemide turvalisusega seotud tegevus peaks käsitlema arengu- ja rakendusstrateegiaid, tehnoloogiaid ning integreerimist ja kontrollimist.

Strateegiline uurimis- ja arendustegevus peaks hõlmama turvatud süsteemide teoreetilisi mudeleid (kaitse kahju tekitamise, volitamata muutmise ja teenustest keeldumise eest), funktsionaalsete nõuete mudeleid, riskimudeleid ja turbearhitektuure.

Tehnoloogiale suunatud uurimis- ja arendustegevus peaks hõlmama kasutajate ja sõnumite autentimist (nt hääleanalüüsi ja elektrooniliste allkirjade abil), tehnilisi liideseid ja krüpteerimise protokolle, juurdepääsu kontrollimehhanisme ning tõendatavalt turvatud süsteemide rakendusmeetodeid.

Tehnilise süsteemi turvalisuse kontrollimist ja kinnitamist ning selle kasutatavust uuritakse integratsiooni- ja kontrolliprojektide kaudu.

Lisaks turbetehnoloogia edendamisele ja arendamisele on vaja ka mitmeid kaasnevaid meetmeid, mis on seotud standardite loomise, säilitamise ja järjekindla kohaldamisega ning infotehnoloogia- ja telekommunikatsioonitoodete heakskiitmise ja sertifitseerimisega, pidades silmas nende turvalisusega seotud omadusi, sealhulgas süsteemide kavandamis- ja rakendamismeetodite heakskiitmise ja sertifitseerimisega.

Ühenduse kolmandat TTA-tegevuse raamprogrammi võib kasutada koostööprojektide edendamiseks konkurentsieelsetel ja normimisele eelnevatel tasanditel.

6. **Tegevussuunis VI — Infosüsteemide turvalisuse tagamine**

6.1. *Teema*

Infosüsteemide turvaelementide täpsest laadist olenevalt tuleb nõutavad funktsioonid lülitada infosüsteemi eri osadesse, sealhulgas nii terminalid/arvutid, teenused ja võrguhaldus kui ka krüptograafilised seadmed, kiipkaardid, avalikud ja isiklikud võtmed jne. Mõningad neist võivad sisalduda tarnijate pakutavas riist- või tarkvaras, ning teised võivad moodustada osa hajutatud süsteemidest (nt võrguhaldus), olla üksikkasutaja käsutuses (nt kiipkaardid) või neid võivad pakkuda eriorganisatsioonid (nt avalikud võtmed/isiklikud võtmed).

Valdavat osa turbetooteid ja -teenuseid pakuvad tõenäoliselt tarnijad, teenuste pakkujad või operaatorid. Teatavate erifunktsioonide täitmiseks, nt avalike/isiklike võtmete väljastamine, auditilubade andmine, võib osutuda vajalikuks asjakohaste organisatsioonide kindlaksmääramine ja volitamine.

Sama kehtib ka teenuse kvaliteedi sertifitseerimise, hindamise ja kontrollimise puhul, sest neid funktsioone peavad täitma tarnijate, teenuste pakkujate ja operaatorite huvidest sõltumatud organisatsioonid. Need võivad olla eraõiguslikud organisatsioonid või valitsusorganisatsioonid, või valitsuse väljastatud tegevusloa alusel teatavaid delegeeritud ülesandeid täitvad organisatsioonid.

6.2. *Eesmärk*

Harmoonilise arengu hõlbustamiseks ühenduse infosüsteemide turvalisuse tagamisel, mille eesmärk on avalikkuse ja ärihuvide kaitse, on vaja koostada turvalisuse tagamist käsitlev järjekindel lähenemisviis. Kui on vaja volitada sõltumatuid organisatsioone, tuleb määratleda ja kokku leppida nende ülesanded ja tegevustingimused ning lülitada need vajaduse korral õiguslikku raamistikku. Eesmärgiks on vastastikuse tunnustamise eeltingimusena saavutada selgelt määratletud ja kokku lepitud ülesannete jaotus eri ettevõtjate vahel ühenduse tasandil.

6.3. *Praegune olukord ja suundumused*

Praegu on infosüsteemide turvalisuse tagamine hästi korraldatud ainult teatavates valdkondades, piirdudes nende erivajaduste rahuldamisega. Euroopa tasandil on tegevus korraldatud mitteametlikul tasandil ning väljaspool kinniseid rühmi ei ole kontrollimise ja sertifitseerimise vastastikuse tunnustamise kord veel välja kujunenud. Infosüsteemide turvalisuse kasvavat tähtsust silmas pidades muutub üha olulisemaks vajadus määrata kindlaks järjekindel lähenemisviis Euroopa ja rahvusvaheliste infosüsteemide turvalisuse tagamiseks.

6.4. **Nõuded, valikuvõimalused ja prioriteedid**

Pidades silmas asjaomaste ettevõtjate arvukust ja asjaolu, et kõnealune küsimus on tihedalt seotud reguleerivate ja seadusandlike küsimustega, on eriti oluline leppida eelnevalt kokku infosüsteemide turvalisuse tagamisel järgitavad põhimõtted.

Seda küsimust käsitleva järjekindla lähenemisviisi koostamisel tuleb pöörata tähelepanu selliste funktsioonide identifitseerimisele ja spetsifikatsioonidele, mille laad eeldab mõningate sõltumatute organisatsioonide (või koostoimivate organisatsioonide) olemasolu. See võib hõlmata näiteks selliseid funktsioone nagu avaliku/isikliku võtmesüsteemi haldamine.

Peale selle on vaja aegsasti identifitseerida ja kindlaks määrata funktsioonid, mille täitmine tuleb üldisi huvisid silmas pidades usaldada sõltumatutele organisatsioonidele (või koostoimivatele organisatsioonidele). Need võivad hõlmata näiteks auditeerimist, kvaliteedi tagamist, kontrollimist, sertifitseerimist ja muid samalaadseid funktsioone.