392D0242

8.5.92 *EUROOPAN YHTEISÖJEN VIRALLINEN LEHTI* N:o L 123/19

NEUVOSTON PÄÄTÖS,

tehty 31 päivänä maaliskuuta 1992,

tietojärjestelmien turvallisuudesta

(92/242/ETY)

EUROOPAN YHTEISÖJEN NEUVOSTO,

joka ottaa huomioon Euroopan talousyhteisön perustamissopimuksen ja erityisesti sen 235 artiklan,

ottaa huomioon komission ehdotuksen[1],

ottaa huomioon Euroopan parlamentin lausunnon[2],

ottaa huomioon talous- ja sosiaalikomitean lausunnon[3],

sekä katsoo, että

yhteisön päämääränä on yhteismarkkinoiden toteuttamisella ja jäsenvaltioiden talouspolitiikan asteittaisella lähentämisellä edistää taloudellisen toiminnan sopusointuista kehitystä koko yhteisössä, jatkuvaa ja tasapainoista kasvua, vakauden lisääntymistä, elintason nopeutuvaa nousua ja entistä läheisempiä suhteita jäsenvaltioiden välillä,

sähköisesti säilytetyllä, käsitellyllä ja siirretyllä tiedolla on yhä suurempi merkitys taloudellisessa ja yhteiskunnallisessa toiminnassa,

maailmanlaajuisen tehokkaan viestinnän käyttöönottaminen ja sähköisen tietojenkäsittelyn laaja levinneisyys korostavat riittävän suojan tarvetta,

Euroopan parlamentti on keskusteluissaan ja päätöslauselmissaan toistuvasti painottanut tietojärjestelmien turvallisuuden tärkeyttä,

talous- ja sosiaalikomitea on korostanut tarvetta käsitellä tietojärjestelmien turvallisuuteen liittyviä kysymyksiä yhteisön eri toimintamuodoissa, ottaen erityisesti huomioon sisämarkkinoiden toteutumisen vaikutukset,

toiminta kansallisella, kansainvälisellä ja yhteisön tasolla muodostaa hyvän perustan,

televiestintä, tietotekniikka, standardointi, tietopalvelumarkkinat, sekä tutkimuksen ja teknologisen kehittämisen toimintaperiaatteet (TTK) liittyvät läheisesti toisiinsa, samoin kuin työ, johon yhteisö on näillä aloilla jo ryhtynyt,

on suotavaa yhtenäistää toimenpiteet asettamalla olemassa oleva kansallinen ja kansainvälinen työ niiden perustaksi ja edistämällä alan tärkeimpien osapuolten välistä yhteistyötä; näin ollen on tarkoituksenmukaista edetä yhtenäisen toimintasuunnitelman mukaan,

tietojärjestelmien turvallisuuden monimutkaisuus edellyttää sellaisten strategioiden kehittämistä, jotka mahdollistavat tiedon vapaan liikkumisen yhtenäismarkkinoiden sisällä varmistaen kuitenkin samanaikaisesti tietojärjestelmien käytön turvallisuuden koko yhteisössä,

jokaisella jäsenvaltiolla on velvollisuus ottaa huomioon turvallisuuden ja yleisen järjestyksen asettamat rajoitukset,

jäsenvaltioiden velvollisuudet tällä alalla edellyttävät yhteistä lähestymistapaa, joka perustuu kiinteään yhteistyöhön jäsenvaltioiden johtavien virkamiesten kanssa,

on tarpeen säätää toimintasuunnitelman laatimisesta 24 kuukauden pituista aloituskautta varten, sekä sellaisen johtavista virkamiehistä koostuvan komitean perustamisesta, jonka virkamiehillä olisi pitkä toimikausi ja jonka tehtävänä olisi neuvoa komissiota tietojärjestelmien turvallisuutta koskevissa toimintamuodoissa,

toiminnan toteutukseen tarvittavat varat 24 kuukauden pituisen aloituskauden aikana arvioidaan 12 miljoonaksi ecuksi; vuodelle 1992 tarvittavat varat arvioidaan voimassa olevan varainhoito-ohjelman mukaan 2 miljoonaksi ecuksi, ja

ohjelman toteutukseen budjettivuoden 1992 jälkeen osoitettavat varat olisi sisällytettävä voimassa oleviin yhteisön varainhoidon kehyksiin,

ON TEHNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Tällä päätöksellä toteutetaan toimet tietojärjestelmien turvallisuuden alalla. Niihin sisältyy:

— laajojen strategioiden kehittäminen tietojärjestelmien turvallisuutta varten (toimintasuunnitelma) 24 kuukauden alkukaudeksi,

ja

— sellaisen johtavista virkamiehistä koostuvan ryhmän perustaminen, jonka virkamiehillä olisi pitkä toimikausi ja jonka tehtävänä olisi neuvoa komissiota tietojärjestelmien turvallisuuden alalla tarvittavista toimista, jäljempänä "komitea".

(1) EYVL N:o C 277, 5.11.1990, s. 18
(2) EYVL N:o C 94, 13.3.1992
(3) EYVL N:o C 159, 17.6.1991, s. 38

2 artikla

1. Komissio kuulee komiteaa järjestelmällisesti yhteisön eri toimintoihin liittyvistä tietojärjestelmien turvallisuutta koskevista kysymyksistä, erityisesti työskentelystrategioiden ja -ohjelmien määrittelemisestä.

2. Toimintasuunnitelmassa on liitteen mukaisesti seuraavia aiheita koskeva alustava työ:

I. tietojärjestelmien turvallisuuden strategisten puitteiden kehittäminen,

II. käyttäjien ja palveluntuottajien tietojärjestelmien turvallisuudelle asettamien tarpeiden tunnistaminen,

III. ratkaisujen tuottaminen käyttäjien, laitetoimittajien ja palveluntuottajien lyhyen ja keskipitkän aikavälin tarpeisiin,

IV. eritelmien, standardoinnin, arvioinnin ja varmentamisen kehittäminen tietojärjestelmien turvallisuuden osalta,

V. tietojärjestelmien turvallisuuden tekniikan ja toiminnan kehittäminen,

VI. tietojärjestelmien turvallisuuden toteutus.

3 artikla

1. Toimen toteutukseen tarvittavat yhteisön varat on arvioitu aloituskauden aikana 12 miljoonaksi ecuksi, josta 2 miljoonaa on vuosien 1988–92 varainhoito-ohjelmassa tarkoitettu vuodelle 1992.

Summa, joka tarvitaan tätä seuraavaa ohjelman toteutuskautta varten, on sisällytettävä kulloinkin voimassa olevaan yhteisön varainhoidon suunnitelmaan.

2. Budjettivallan käyttäjä määrää kunakin budjettivuonna irrotettavat varat Euroopan yhteisöjen yleiseen talousarvioon sovellettavan varainhoitoasetuksen 2 artiklassa tarkoitettujen hyvän taloudenpidon periaatteiden mukaisesti.

4 artikla

Ryhmä riippumattomia asiantuntijoita arvioi aloituskauden tulokset komission puolesta. Ryhmän kertomus sekä mahdolliset komission siihen liittämät huomautukset annetaan Euroopan parlamentille ja neuvostolle.

5 artikla

1. Komissio vastaa toiminnan toteutuksesta. Sitä avustaa neuvoa-antava komitea, jonka muodostavat jäsenvaltioiden edustajat ja puheenjohtajana komission edustaja.

2. Toimintasuunnitelma toteutetaan 2 artiklassa määriteltyjen tavoitteiden mukaisesti ja se tarkistetaan tarpeen mukaan. Siinä esitetään yksityiskohtaiset tavoitteet ja tarvittavat toimenpiteet sekä rahoitusjärjestelyt niitä varten. Komissio pyytää toimintasuunnitelman perusteella ehdotuksia.

3. Toimintasuunnitelma toteutetaan kiinteässä yhteistyössä alan osapuolten kanssa. Siinä otetaan huomioon, edistetään ja täydennetään tällä alalla meneillään olevia eurooppalaisia ja kansainvälisiä standardointitoimia.

6 artikla

1. Jäljempänä 7 artiklassa säädettyä menettelyä sovelletaan toimenpiteisiin, jotka liittyvät yhteisön toimintaperiaatteisiin tietojärjestelmien turvallisuuden alalla.

2. Jäljempänä 8 artiklassa säädettyä menettelyä sovelletaan:

— edellä 5 artiklassa tarkoitetun toimintasuunnitelman laatimiseen ja tarkistamiseen,

— ehdotuspyyntöjen sisältöön, ehdotusten arvioimiseen ja yhteisön arvioidun taloudellisen osuuden määräämiseen toimenpiteistä, jos osuus ylittää 200 000:ta ecua,

— yhteisön ulkopuolisten järjestöjen tämän päätöksen mukaiseen toimintaan osallistumiseen,

— toimenpiteiden tulosten levittämis-, suojelu- tai käyttämiskeinoihin,

— toiminnan arvioimiseksi tarvittaviin toimenpiteisiin.

3. Jos yhteisön osuus toimenpiteistä on enintään 200 000 ecua, komissio kuulee komiteaa tarvittavista toimenpiteistä ja ilmoittaa arvionsa lopputuloksen komitealle.

7 artikla

Komission edustaja tekee komitealle ehdotuksen tarvittavista toimenpiteistä. Komitea antaa, tarvittaessa äänestettyään, lausuntonsa ehdotuksesta määräajassa, jonka puheenjohtaja asettaa asian kiireellisyyden mukaan.

Lausunto merkitään pöytäkirjaan; lisäksi jokaisella jäsenvaltiolla on oikeus pyytää, että sen kanta merkitään pöytäkirjaan.

Komission on mahdollisuuksien mukaan otettava huomioon komitean lausunto. Sen on ilmoitettava komitealle, millä tavoin lausunto on otettu huomioon.

8 artikla

Komission edustaja tekee komitealle ehdotuksen tarvittavista toimenpiteistä. Komitea antaa lausuntonsa ehdotuksesta määräajassa, jonka puheenjohtaja voi asettaa asian kiireellisyyden mukaan. Lausunto annetaan perustamissopimuksen 148 artiklan 2 kohdassa niiden päätösten

edellytykseksi määrätyllä enemmistöllä, jotka neuvosto tekee komission ehdotuksesta. Komiteaan kuuluvien jäsenvaltioiden edustajien äänet painotetaan mainitussa artiklassa määrätyllä tavalla. Puheenjohtaja ei osallistu äänestykseen.

Komissio päättää suunnitelluista toimenpiteistä, jos ne ovat komitean lausunnon mukaisia.

Jos suunnitellut toimenpiteet eivät ole komitean lausunnon mukaisia tai lausuntoa ei ole annettu, komissio antaa viipymättä neuvostolle ehdotuksen tarvittavista toimenpiteistä. Neuvosto päättää asiasta määräenemmistöllä.

Jos neuvosto ei ole ratkaissut asiaa kolmen kuukauden kuluessa siitä kun asia on tullut vireille neuvostossa, komissio tekee päätöksen ehdotetuista toimenpiteistä, jollei neuvosto ole yksinkertaisella enemmistöllä hylännyt mainittuja toimenpiteitä.

Tehty Brysselissä 31 päivänä maaliskuuta 1992.

Neuvoston puolesta

Puheenjohtaja

Vitor MARTINS

LIITE

Yhteenveto toimintalinjoista

SUUNTAVIIVOJA TOIMINTASUUNNITELMAKSI TIETOJÄRJESTELMIEN TURVALLISUUDEN ALALLA

JOHDANTO

Toimintasuunnitelman tavoitteena on kehittää yleisiä strategioita, joiden tarkoituksena on aikaansaada sähköisesti säilytetyn, käsitellyn tai siirretyn tiedon käyttäjille ja tuottajille asianmukainen tietojärjestelmien suoja tuottamuksellisia tai tahallisia uhkia vastaan.

Toimintasuunnitelmassa otetaan huomioon ja täydennetään tällä alalla meneillään olevia maailmanlaajuisia standardointitoimia.

Se sisältää seuraavat toimintalinjat:

— Tietojärjestelmien turvallisuuden strategisten puitteiden kehittäminen,

— käyttäjien ja palveluntuottajien tietojärjestelmien turvallisuudelle asettamien tarpeiden tunnistaminen,

— ratkaisujen tuottaminen käyttäjien, laitetoimittajien ja palveluntuottajien lyhyen ja keskipitkän ajan tarpeisiin,

— eritelmien, standardoinnin, arvioinnin ja varmentamisen kehittäminen tietojärjestelmien turvallisuuden osalta,

— tietojärjestelmien turvallisuuden tekniikan ja toiminnan kehittäminen,

— tietojärjestelmien turvallisuuden toteutus.

Toimintasuunnitelman toteuttaa komissio kiinteässä yhteistyössä jäsenvaltioiden vastaavien toimien, sekä yhteisön tähän liittyvien tutkimus- ja kehittämistoimien kanssa.

1 Toimintalinja I – tietojärjestelmien turvallisuuden strategisten puitteiden kehittäminen

1.1 *Aihe*

Tietojärjestelmien turvallisuus on todettu ominaisuudeksi, joka on välttämätön kaikkialla nykyaikaisessa yhteiskunnassa. Sähköiset tietopalvelut edellyttävät turvattua teleinfrastruktuuria, turvattuja laitteita ja ohjelmistoja samoin kuin niiden käytön ja hallinnan turvaamista. On laadittava laaja strategia, jossa otetaan huomioon kaikki tietojärjestelmien turvallisuuteen liittyvät näkökohdat ja vältetään hajanaista lähestymistapaa. Sähköisesti käsitellyn tiedon turvallisuutta koskevan strategian on heijastettava yhteiskunnan halua toimia tehokkaasti mutta samalla suojella itseään nopeasti muuttuvassa maailmassa.

1.2 *Tavoite*

On laadittava strategiset puitteet yhteisön yhteiskunnallisten, taloudellisten ja poliittisten tavoitteiden yhteensovittamiseksi teknisiin, toiminnallisiin ja lainsäädännöllisiin vaihtoehtoihin kansainvälisissä yhteyksissä. Eri näkökohtien, tavoitteiden ja rajoitusten herkkä tasapaino voidaan löytää vain siten, että alan osapuolet yhdessä kehittävät yhteisen näkemyksen ja sopivat strategisista puitteista. Nämä seikat ovat perusedellytys etunäkökohtien ja tarpeiden yhteensovittamiseksi niin politiikassa kuin teollisessa kehityksessä.

1.3 *Vallitseva tilanne ja kehityssuunnat*

Tilanteelle on ominaista kasvava tietoisuus siitä, että on tarve toimia. Toimenpiteiden yhteensovittamiseksi tarkoitetun aloitteen puuttuessa vaikuttaa kuitenkin hyvin todennäköiseltä, että eri alojen hajanaiset toimenpiteet luovat tilanteen, joka on itse asiassa vastakkainen tavoitteisiin nähden ja luo yhä vakavampia oikeudellisia, yhteiskunnallisia ja taloudellisia ongelmia.

1.4 *Vaatimukset, vaihtoehdot ja tärkeysjärjestys*

Tällaisten yhteisten puitteiden olisi sisällettävä ja asetettava tärkeysjärjestykseen tiedon ja siihen liittyvien palvelujen haavoittuvuutta koskeva riskianalyysi ja riskienhallinta, tietokoneiden ja televiestinnän väärinkäyttöä koskevan lainsäädännön yhdenmukaistaminen, hallinnolliset perusrakenteet mukaan luettuna turvallisuuspolitiikka ja se, miten eri teollisuuden- ja tieteenalat voivat toteuttaa nämä, sekä yhteiskuntaan ja yksityisyyteen liittyvät näkökohdat (esimerkiksi tunnistus-, todennus-, kiistattomuus- ja mahdollisesti valtuutusjärjestelmien käyttö demokraattisessa ympäristössä).

On laadittava selkeät ohjeet turvattujen hajautettujen tietopalvelujen fyysisten ja loogisten arkkitehtuurien, luotettavia turvallisuustuotteita ja palveluja koskevien standardien, ohjeiden ja määritelmien, sekä erityissektorien tarpeita vastaavien erilaisten hallintorakenteiden, arkkitehtuurien ja standardien toimivuuden toteamiseksi tarvittavien koehankkeiden ja prototyyppien kehittämistä varten.

Käyttäjien asenteiden muokkaamiseksi on luotava turvallisuustietoisuutta, jotta nämä kiinnittäisivät enemmän huomiota tietotekniikan (TT) turvallisuuteen.

2 Toimintalinja II – Käyttäjien ja palveluntuottajien tietojärjestelmien turvallisuudelle asettamien vaatimusten tunnistaminen

2.1 *Aihe*

Tietojärjestelmien turvallisuus on kaupallisten sovellusten eheyden ja uskottavuuden, tekijänoikeuksien ja luottamuksellisuuden ehdoton edellytys. Tämä johtaa väistämättä vaikeaan tasapainotteluun ja joskus valintoihin toisaalta vapaata kauppaa ja toisaalta yksityisyyden ja tekijänoikeuksien suojaamista koskevien sitoumusten välillä. Näiden valintojen ja kompromissien on perustuttava vaatimusten täydelliseen ymmärtämiseen ja tietojärjestelmien turvallisuuden alalla tehtyjen valintojen mahdollisuuksiin vastata näihin vaatimuksiin.

Käyttäjien tarpeet käsittävät tietojärjestelmien turvaamistoimintoja teknisten, toiminnallisten ja lainsäädännöllisten näkökohtien yhteydessä. Sen vuoksi tietojärjestelmien turvallisuusvaatimusten järjestelmällinen selvittäminen on välttämätöntä asianmukaisten ja tehokkaiden toimenpiteiden kehittämiseksi.

2.2 *Tavoite*

Osoittaa käyttäjien ja palveluntuottajien vaatimusten luonne ja ominaisuudet, sekä niiden suhde tietojärjestelmien turvallisuustoimenpiteisiin.

2.3 *Vallitseva tilanne ja kehityssuunnat*

Tähän mennessä ei ole ryhdytty mihinkään yhteisiin toimenpiteisiin tietojärjestelmien turvallisuuden keskeisten osapuolten nopeasti kehittyvien ja muuttuvien tarpeiden tunnistamiseksi. Yhteisön jäsenvaltiot ovat tunnistaneet kansallisten toimintojen (etenkin "tietotekniikan turvallisuuden arviointiperusteiden") yhdenmukaistamisen tarpeen. Yhtenäiset arviointiperusteet ja säännöt arviointitodistusten vastavuoroiseksi tunnustamiseksi ovat erittäin tärkeitä.

2.4 *Vaatimukset, vaihtoehdot ja tärkeysjärjestys*

Perustan luomiseksi alan osapuolten perusteltujen tarpeiden johdonmukaiselle ja avoimelle kohtelulle on katsottu tarpeelliseksi laatia yhteisesti sovittu käyttäjien tarpeiden luokittelu ja sen suhde tietojärjestelmien turvallisuuden toteuttamiseen.

On myös katsottu tärkeäksi tunnistaa lainsäädännön ja eettisten sääntöjen tarve palveluominaisuuksien ja tekniikan arvioitujen kehityssuuntien valossa, osoittaa vaihtoehtoiset strategiat tavoitteiden saavuttamiseksi hallinnollisten, palveluun liittyvien, toiminnallisten ja teknisten määräysten avulla sekä arvioida tietojärjestelmien eri turvallisuusvaihtoehtojen ja strategioiden tehokkuus, käyttäjäystävällisyys ja kustannukset käyttäjien, palveluntuottajien ja toimittajien kannalta.

3 Toimintalinja III – Ratkaisujen tuottaminen käyttäjien, laitetoimittajien ja palveluntuottajien lyhyen ja keskipitkän ajan tarpeisiin

3.1 *Aihe*

Tietokoneet voidaan nykyään suojata riittävästi ulkopuolista luvatonta sisäänpääsyä vastaan "eristämällä", toisin sanoen käyttämällä tavanomaisia organisatorisia ja fyysisiä toimenpiteitä. Tämä koskee myös suljetun käyttäjäryhmän sähköistä viestintää erillisverkossa. Tilanne on täysin toinen, jos useat käyttäjäryhmät käyttävät yhteisiä tietoja tai vaihtavat tietoja yleisen tai laajasti käytettävissä olevan verkon kautta. Näissä tapauksissa ei ole yleisesti saatavilla sellaista tekniikkaa, päätteitä ja palveluja eikä toisiaan vastaavia standardeja ja menettelytapoja, jotka takaisivat tietojärjestelmille vastaavan suojan.

3.2 *Tavoite*

Tavoitteena on tuottaa lyhyessä ajassa ratkaisuja, jotka pystyvät vastaamaan käyttäjien, palveluntuottajien ja valmistajien kiireellisimpiin tarpeisiin. Tähän kuuluu tietotekniikan turvallisuuden yleisten arviointiperusteiden käyttö, jotka on suunniteltava avoimiksi tulevaisuuden vaatimuksia ja ratkaisuja varten.

3.3 *Vallitseva tilanne ja kehityssuunnat*

Jotkin käyttäjäryhmät ovat kehittäneet omaan käyttöönsä tekniikoita ja menetelmiä, jotka vastaavat etenkin todentamisen, eheyden ja kiistattomuuden vaatimuksia. Yleisesti tähän käytetään magneettisia kortteja tai älykortteja. Myös kehittyneitä ja kehittymättömiä salakirjoitustekniikoita on käytössä. Usein tämä merkitsee käyttäjäryhmän omien "viranomaisten" määrittelemistä. Näitä tekniikoita ja menetelmiä on kuitenkin vaikea muuttaa yleisiksi, niin että ne täyttäisivät avoimen ympäristön vaatimukset.

ISO työskentelee OSI-tietoturvastandardin määrittelemiseksi (ISO DIS 7498–2) samoin kuin CCITT puolestaan X400:n yhteydessä. Sanomiin on myös mahdollista liittää turvaussegmenttejä. Todentamista, eheyttä ja kiistattomuutta pidetään sanomien (EDIFACT) osana samoin kuin osana X400 MHS-järjestelmää.

Tällä hetkellä organisaatioiden välisen tiedonsiirron (OVT) oikeudellisia puitteita ollaan vasta suunnittelemassa. Kansainvälinen kauppakamari on julkaissut yhdenmukaiset toimintasäännöt kaupallisten tietojen vaihtoon tietoliikenteen välityksellä.

Useat valtiot (esimerkiksi Saksa, Ranska, Yhdistynyt kuningaskunta ja Yhdysvallat) ovat kehittäneet tai ovat kehittämässä tietotekniikan ja teletuotteiden ja -järjestelmien luotettavuuden arviointiperusteita sekä vastaavia menettelyjä arvioinnin suorittamiseksi. Nämä perusteet on laadittu yhteistyössä kansallisten valmistajien kanssa, ja niiden myötä luotettavien tuotteiden ja järjestelmien määrä lisääntyy yksinkertaisista tuotteista alkaen. Tätä kehitystä tukee sellaisten kansallisten järjestöjen luominen, joiden tehtävänä on suorittaa arviointeja ja myöntää todistuksia.

Useimmat käyttäjät eivät pidä luottamuksellisuuden aikaansaamista kovin kiireellisenä. Tilanne kuitenkin muuttunee tulevaisuudessa kehittyneiden viestintäpalvelujen ja etenkin matkaviestinpalvelujen yleistyessä.

3.4 *Vaatimukset, vaihtoehdot ja tärkeysjärjestys*

On olennaista kehittää mahdollisimman nopeasti menettelyt, standardit, tuotteet ja välineet, jotka soveltuvat turvallisuuden takaamiseen sekä itse tietojärjestelmissä (tietokoneet, oheislaitteet) että yleisissä viestintäverkoissa. Todentaminen, eheys ja kiistattomuus olisi asetettava etusijalle. Esitettyjen ratkaisujen kelpoisuus olisi määriteltävä koehankkeiden avulla. Ratkaisuja OVT:n kiireellisimpiin tarpeisiin tarkastellaan TEDIS-ohjelmassa, joka on liitetty tämän toimintasuunnitelman yleiseen sisältöön.

4 Toimintalinja IV – Tietojärjestelmien turvallisuuteen liittyvien eritelmien, standardoinnin, arvioinnin ja varmentamisen kehittäminen

4.1 *Aihe*

Tietojärjestelmien turvallisuuden vaatimukset ulottuvat monille aloille, ja yhteiset eritelmät ja standardit ovat tämän vuoksi ratkaisevan tärkeitä. Tietotekniikan turvaamiseksi sovittujen standardien ja eritelmien puuttuminen saattaa olla suuri este tietoon perustuvien menetelmien ja palvelujen kehittymiselle kaikkialla taloudessa ja yhteiskunnassa. Toimenpiteitä on toteutettava myös tekniikan ja standardien kehittämisen ja käytön nopeuttamiseksi useilla toisiaan lähellä olevilla viestinnän ja tietokoneverkkojen alueilla, jotka ovat ratkaisevan tärkeitä käyttäjille, teollisuudelle ja hallinnolle.

4.2 *Tavoite*

On tarpeellista luoda keinot erityisten turvatoimintojen tukemiseksi ja toteuttamiseksi OSI:n, ONP:n, ISDN/IBC:n sekä verkonhallinnan alueilla. Standardointiin ja eritelmiin liittyvät olennaisesti ne tekniikat ja lähestymistavat, jotka ovat tarkistamisen edellytyksenä, mukaan luettuna vastavuoroiseen tunnustamiseen johtava varmentaminen. Mikäli mahdollista, kansainvälisesti sovittuja ratkaisuja on tuettava. On edistettävä myös atk-järjestelmien, joissa on turvatoiminnot, kehittämistä ja käyttöä.

4.3 *Vallitseva tilanne ja kehityssuunnat*

Etenkin Yhdysvallat on tehnyt tietojärjestelmien turvallisuutta koskevia tärkeitä aloitteita. Euroopassa asiaa käsitellään osana ETSI- ja CEN/CENELEC -järjestelmiä yhdessä tietotekniikan ja televiestinnän standardoinnin kanssa CCITT- ja ISO- järjestelmien tämän alan työn valmisteluna.

Huolestumisen lisääntyessä työ Yhdysvalloissa kiihtyy nopeasti, ja sekä toimittajat että palveluntuottajat lisäävät toimenpiteitään tällä alalla. Euroopassa Ranska, Saksa ja Yhdistynyt kuningaskunta ovat toisistaan riippumatta ryhtyneet samankaltaisiin toimiin, mutta Yhdysvaltain tilannetta vastaava yhteistoiminta kehittyy vain hitaasti.

4.4 *Vaatimukset, vaihtoehdot ja tärkeysjärjestys*

Tietojärjestelmien turvallisuuden alalla vallitsee hyvin läheinen suhde lainsäädännöllisten, toiminnallisten, hallinnollisten ja teknisten näkökohtien kesken. Lainsäädännön on heijastuttava standardeihin, ja tietojärjestelmien turvallisuutta koskevien toimenpiteiden on todistettavalla tavalla noudatettava standardeja ja lainsäädäntöä. Lainsäädäntö vaatii monissa suhteissa eritelmiä, jotka ulottuvat perinteistä standardointia laajemmalle, toisin sanoen sisältävät käytännesäännöt. Standardeihin ja käytännesääntöihin liittyvät vaatimukset koskevat kaikkia tietojärjestelmien turvallisuuden alueita, ja on syytä erottaa toisistaan toisaalta suojavaatimukset, jotka vastaavat turvallisuustavoitteita ja toisaalta jotkin sellaiset tekniset vaatimukset, jotka voidaan uskoa toimivaltaisille eurooppalaisille standardointielimille (CEN/CENELEC/ETSI).

Eritelmien ja standardien on käsitettävä tietojärjestelmien turvapalvelualat (henkilöiden ja yritysten todennus, kiistattomuuskäytännöt, oikeudessa hyväksyttävät sähköiset todisteet, valtuuksien valvonta), niiden viestintäpalvelut (kuvallisen viestinnän yksityisyys, puheen ja tietokannan siirron yksityisyys matkaviestinnässä, tietokannan ja kuvatietokantojen suojaaminen, integroitujen palvelujen turvallisuus), niiden viestinnän ja turvallisuuden hallinta (yleiset/yksityiset avainjärjestelmät avoimen verkon toiminnassa, verkonhallinnan suoja, palveluntuottajien suoja) sekä näiden varmentaminen (varmistuskriteerit ja -tasot, menettelytavat turvattujen tietojärjestelmien suojauksen varmistukselle).

5 Toimintalinja V – Tietojärjestelmien turvallisuuden tekniikan ja toiminnan kehittäminen

5.1 *Aihe*

Tekniikan järjestelmällinen tutkiminen ja kehittäminen taloudellisesti toteuttamiskelpoisten ja toiminnallisesti tyydyttävien ratkaisujen löytämiseksi tietojärjestelmän turvallisuuden nykyisiin ja tuleviin vaatimuksiin on palvelumarkkinoiden kehittymisen ja koko Euroopan talouden kilpailukyvyn perusedellytys.

Tietojärjestelmien turvallisuuden tekniikan kehittämisessä on otettava huomioon sekä tietokoneiden että viestinnän turvallisuus, sillä useimmat nykyisistä järjestelmistä ovat hajautettuja, ja niihin pääsee tietoliikennepalvelujen kautta.

5.2 *Tavoite*

Tekniikan järjestelmällinen tutkiminen ja kehittäminen taloudellisesti toteuttamiskelpoisten ja toiminnallisesti tyydyttävien ratkaisujen löytämiseksi tietojärjestelmien turvallisuuden nykyisiin ja tuleviin vaatimuksiin.

5.3 *Vaatimukset, vaihtoehdot ja tärkeysjärjestys*

Tietojärjestelmien turvallisuuden alalla tehtävän työn olisi suuntauduttava kehittämisen ja täytäntöönpanon strategioihin, tekniikkaan, integraatioon ja tarkistamiseen.

Strategisen T&K-työn olisi katettava turvattujen järjestelmien käsitemallit (suoja vaarantumista, valtuutonta muuttamista ja palvelun kieltämistä vastaan), toiminnallisten vaatimusten mallit, riskimallit ja turva-arkkitehtuurit.

Teknisesti suuntautuneen T&K-työn olisi sisällettävä käyttäjän ja viestin todennus (esimerkiksi puheanalyysien ja sähköisten allekirjoitusten avulla), tekniset rajapinnat ja salakirjoituskäytännöt, todistettavasti turvattujen järjestelmien pääsynvalvontamekanismit ja toteuttamismenetelmät.

Teknisen järjestelmän turvallisuuden tarkistaminen ja kelvolliseksi osoittaminen, sekä sen sovellettavuus olisi tutkittava integraatio- ja tarkistushankkeiden avulla.

Turvallisuustekniikan lujittamisen ja kehittämisen lisäksi tarvitaan oheistoimenpiteitä, jotka koskevat standardien laatimista, ylläpitoa ja johdonmukaista soveltamista, ja tietotekniikka- ja teletuotteiden kelvolliseksi osoittamista ja varmentamista ottaen huomioon niiden turvallisuusominaisuudet, mukaan lukien järjestelmien suunnittelu- ja toteutusmenetelmien kelvolliseksi osoittaminen ja varmentaminen.

Yhteisön kolmatta TTK-puiteohjelmaa voitaisiin käyttää yhteistyöprojektien edistämiseksi esikilpailullisella ja esinormatiivisella tasolla.

6 Toimintalinja VI – Tietojärjestelmien turvallisuuden toteutus

6.1 *Aihe*

Tietojärjestelmien turvallisuusominaisuuksien kulloisenkin luonteen mukaan tarvittavat toiminnot on sisällytettävä tietojärjestelmän eri osiin, kuten päätteet/tietokoneet, palvelut, salakirjoituskeksintöjen verkonhallinta, toimikortit, julkiset ja yksityiset avaimet, jne. Eräät näistä voitaneen liittää myyjien toimittamiin laitteisiin tai ohjelmistoihin, kun taas toiset voivat muodostaa osan hajautettua järjestelmää (esim. verkonhallinta), olla yksittäisen käyttäjän hallussa (esimerkiksi toimikortit) tai erikoistuneen organisaation toimittamia (esim. julkiset/yksityiset avaimet).

Useimmat turvallisuustuotteet ja -palvelut ovat luultavasti laitetoimittajien, palveluntuottajien tai operaattorien toimitettavissa. Erityistoimintoja kuten julkisten/yksityisten avainten toimittamista tai tarkastusvaltuuksien myöntämistä varten voi olla tarve osoittaa ja valtuuttaa asianmukaisia organisaatioita.

Sama koskee palvelun laadun varmentamista, arviointia ja todentamista, joita hoitavien järjestöjen on oltava laitetoimittajien, palveluntuottajien ja operaattorien eduista riippumattomia. Ne voivat olla yksityisiä, valtiollisia tai valtion myöntämän toimiluvan nojalla valtuutettuja toimintoja harjoittavia organisaatioita.

6.2 *Tavoite*

Yhdenmukaisen kehityksen edesauttamiseksi yhteisön tietojärjestelmien turvallisuuden luomisessa yleisten ja liikeelämän etujen suojaamiseksi on välttämätöntä kehittää johdonmukainen lähestymistapa yhteisön tietojärjestelmien turvallisuuden toteuttamiseksi. Jos on tarpeen valtuuttaa riippumattomia järjestöjä, näiden toiminnat sekä toiminnan edellytykset on määriteltävä ja sovittava ja tarvittaessa sisällytettävä lainsäädäntöön. Tavoitteena olisi saavuttaa selkeästi määritelty ja sovittu eri osapuolten välinen vastuunjako yhteisön tasolla, mikä on vastavuoroisen tunnustamisen edellytys.

6.3 *Vallitseva tilanne ja kehityssuunnat*

Nykyisin tietojärjestelmien turvallisuus on hyvin järjestettyä vain tietyillä aloilla ja rajoittuu niiden erityistarpeista huolehtimiseen. Euroopan tasolla järjestelyt ovat useimmiten epävirallisia, ja suljettuja ryhmiä lukuun ottamatta tarkistamisen ja varmentamisen vastavuoroista tunnustamista ei ole toistaiseksi saatu aikaan. Tarve määritellä johdonmukainen lähestymistapa tietojärjestelmien turvallisuuteen Euroopassa ja kansainvälisesti on tietojärjestelmien turvallisuuden merkityksen kasvaessa muodostunut todella tärkeäksi.

6.4 *Vaatimukset, vaihtoehdot ja tärkeysjärjestys*

Koska asia koskee lukuisia osapuolia ja koska asia liittyy läheisesti lainsäädännöllisiin kysymyksiin, on erityisen tärkeää sopia ennalta periaatteista, joita olisi noudatettava toteutettaessa tietojärjestelmien turvallisuutta.

Kehitettäessä johdonmukaista lähestymistapaa tähän kysymykseen on huolehdittava sellaisen toiminnan tunnistamisesta ja määrittelystä, joka jo ominaisuutensa vuoksi edellyttää riippumattomien järjestöjen (tai yhdessä toimivien järjestöjen) olemassaoloa. Tällainen toiminta voisi olla esimerkiksi julkisten/yksityisten avainjärjestelmien hallinto.

Lisäksi on suotavaa tunnistaa ja eritellä jo varhaisessa vaiheessa toiminta, joka yleisen edun vuoksi on syytä uskoa riippumattomille järjestöille (tai yhdessä toimiville järjestöille). Tällaista voisi olla esimerkiksi valvonta, laadunvarmistus, tarkistaminen, varmentaminen ja vastaava toiminta.