

ÁKVÖRÐUN RÁÐSINS

frá 31. mars 1992

um öryggi upplýsingakerfa

(92/242/EEC)

RÁÐ EVRÓPUBANDALAGANNA HEFUR,

með hliðsjón af stofnsáttmála Efnahagsbandalags Evrópu, einkum 235. gr.,

með hliðsjón af tillögu framkvæmdastjórnarinnar ⁽¹⁾,

með hliðsjón af álitum Evrópuþingsins ⁽²⁾,

með hliðsjón af álitum efnahags- og félagsmálanefndarinnar ⁽³⁾,

og að teknu tilliti til eftirfarandi:

Markmið bandalagsins, með því að stofna sameiginlegan markað og samræma stig af stigi efnahagsstefnur aðildarríkjanna, er að stuðla að samfelldri þróun efnahagsmála í bandalaginu, stöðugum og jöfnum vexti, auknum stöðugleika, batnandi lífskjörum og nánari samvinnu meðal aðildarríkjanna.

Upplýsingar sem eru skráðar, unnar og sendar í gegnum tölvu gegna æ mikilvægara hlutverki í efnahags- og samfélagsmálum.

Með tilkomu hraðvirkra tölvusamskipta um heim allan og sívaxandi notkun tölvuvinnslu á öllum sviðum verður þörfin fyrir viðeigandi vernd æ brýnni.

Í umfjöllun sinni og ályktunum hefur Evrópuþingið hvað eftir annað lagt áherslu á nauðsyn þess að tryggja öryggi upplýsingakerfa.

Efnahags- og félagsmálanefndin hefur bent á þörfina á því að bandalagið geri ráðstafanir til að tryggja öryggi upplýsingakerfa, einkum vegna áhrifa sem fylgja tilkomu hins innri markaðar.

Mynda má góðan grundvöll með því að efna til aðgerða innanlands, á alþjóðavettvangi og í bandalaginu.

Náin tengsl eru á milli fjarskipta, upplýsingatækni, stöðlunarmála og upplýsingamarkaðarins og stefnu bandalagsins

⁽¹⁾ Stjtið. EB nr. C 277, 5. 11. 1990, bls. 18.

⁽²⁾ Stjtið. EB nr. C 94, 13. 3. 1992.

⁽³⁾ Stjtið. EB nr. C 159, 17. 6. 1991, bls. 38.

varðandi rannsóknir, þróun og tækni svo og vinnu sem þegar hefur farið fram á þessum sviðum á vegum bandalagsins.

Rétt er að samstillta aðgerðir með því að byggja á vinnu sem þegar er í gangi á innlendum og alþjóðlegum vettvangi og efla samstarf helstu aðila sem í hlut eiga. Því er rétt að framkvæma aðgerðir innan ramma markvissrar aðgerðaáætlunar.

Eigi að tryggja öryggi upplýsingakerfa krefst það flókin framkvæmdar til að upplýsingar geti fengist án hindrana á hinum sameiginlega markaði en öryggi sé jafnframt tryggt við notkun upplýsingakerfa alls staðar í bandalaginu.

Hvert aðildarríki ber ábyrgð á að virða þær takmarkanir sem krafist er vegna öryggis og allsherjarreglu.

Ábyrgð aðildarríkjanna á þessu sviði kallar á samstilltar aðgerðir og náð samráð milli háttsettra embættismanna aðildarríkjanna.

Kveða skal á um aðgerðaáætlun til tveggja ára í fyrstu og stofnun nefndar háttsettra embættismanna með langtímaumboð til að vera framkvæmdastjórninni til ráðgjafar um aðgerðir til að tryggja öryggi upplýsingakerfa.

Áætlað er að það fjármagn sem þörf er á til að framkvæma aðgerðirnar á tuttugu og fjögurra mánaða upphafstímabili nemi tólf milljónum evrópskra mynteininga (ECU). Fyrir árið 1992, miðað við fjárhagsáætlanir sem nú gilda, nemur þessi fjárhæð tveimur milljónum evrópskra mynteininga.

Gera þarf ráð fyrir þeirri fjárhæð sem þörf er á til að fjármagna áætlunina eftir 1992 innan núgildandi fjárhagsramma bandalagsins.

ÁKVEDIÐ EFTIRFARANDI:

I. gr.

Samþykkt er hér með að efna til aðgerða vegna öryggis upplýsingakerfa. Meðal annars skal:

- þróa heildaráætlun til að tryggja öryggi upplýsingakerfa (aðgerðaáætlun) á tuttugu og fjögurra mánaða upphafstímabili,
- stofna nefnd háttsettra embættismanna með langtímaumboð til að vera framkvæmdastjórninni til ráðgjafar um aðgerðir til að tryggja öryggi upplýsingakerfa, hér eftir kölluð „nefndin“.

2. gr.

1. Framkvæmdastjórnin skal hafa reglubundið samráð við nefndina um mál er varða öryggi upplýsingakerfa og aðgerðir sem bandalagið efnir til, einkum að því er lýtur að starfsáætlunum og útfærslu þeirra.

2. Í aðgerðaáætluninni skal, eins og fram kemur í viðaukanum, fjallað um undirbúningsvinnu að því er varðar:

- I. þróun langtímaskipulags til að tryggja öryggi upplýsingakerfa;
- II. skilgreiningu á þörfum notenda og þeirra sem þjónustu veita að því er lýtur að öryggi upplýsingakerfa;
- III. lausnir sem fullnægja þörfum notenda, birgja og þjónustuaðila nú þegar og til skamms tíma;
- IV. þróun forskrifa, stöðlunar og leiða til að meta og staðfesta öryggi upplýsingakerfa;
- V. framfarir í tækni og notkun upplýsingakerfa sem varða öryggi þeirra;
- VI. ráðstafanir til að tryggja öryggi upplýsingakerfa.

3. gr.

1. Áætlað er að nauðsynlegt fjármagn frá bandalaginu til að framkvæma aðgerðirnar nemi tólf milljónum evrópskra mynteininga (ECU) á tuttugu og fjögurra mánaða tímabili; af því eru tvær milljónir evrópskra mynteininga áætlaðar fyrir tímabilið 1991/1992, miðað við fjárhagsáætlanir frá 1988 til 1992.

Gera verður ráð fyrir þeirri fjárhæð sem þörf er á til að fjármagna síðari hluta af áætluninni innan núgildandi fjárhagsramma bandalagsins.

2. Fjármálayfirvaldið skal ákveða fjárveitingar fyrir hvert fjárhagsár með hliðsjón af meginreglunum um trausta stjórnun sem um getur í 2. gr. fjárhagsreglugerðarinnar um fjárlög Evrópubandalaganna.

4. gr.

Á vegum framkvæmdastjórnarinnar skal hópur óháðra sérfræðinga leggja mat á árangur aðgerðanna á upphafstímabilinu. Matsskýrsla hópsins, ásamt athugasemdum framkvæmdastjórnarinnar, skal send Evrópuþinginu og ráðinu.

5. gr.

1. Framkvæmdastjórnin ber ábyrgð á framkvæmd áætlunarinnar. Hún skal njóta aðstoðar ráðgjafarnefndar sem skipuð er fulltrúum aðildarríkjanna undir formennsku fulltrúa framkvæmdastjórnarinnar.

2. Framkvæma ber aðgerðaáætlunina í samræmi við þau markmið sem sett eru í 2. gr., og uppfæra skal ef þörf krefur. Í henni skal greina nánar frá einstökum markmiðum

og tegundum aðgerða sem beita skal og hvernig þær verði fjármagnaðar. Framkvæmdastjórnin auglýsir síðan eftir tillögum á grundvelli áætlunarinnar.

3. Framkvæma ber aðgerðaáætlunina í nánu samráði við alla aðila í greininni. Við framkvæmd ber að taka tillit til vinnu sem í gangi er á þessu sviði hjá evrópskum og alþjóðlegum staðlastofnunum, efla hana og auka við.

6. gr.

1. Málsmeðferð sem mælt er fyrir um í 7. gr. gildir um: — ráðstafanir til að móta stefnu bandalagsins í því að tryggja öryggi upplýsingakerfa.

2. Málsmeðferð sem mælt er fyrir um í 8. gr. gildir um: — samningu og endurskoðun aðgerðaáætlunarinnar sem um getur í 5. gr.;

— texta auglýsinga eftir tillögum, mat á tillögum og áætlanir um framlag bandalagsins sé það meira en tvö hundruð þúsund evrópskar mynteiningar (ECU);

— þátttöku stofnana utan bandalagsins í aðgerð sem heyrir undir þessa ákvörðun;

— fyrirkomulag við að dreifa, vernda eða hagnýta niðurstöður af þessum ráðstöfunum;

— ráðstafanir sem gera skal til að meta árangurinn af aðgerðunum.

3. Sé framlag bandalagsins tvö hundruð þúsund evrópskar mynteiningar (ECU) eða minna skal framkvæmdastjórnin hafa samráð við nefndina um ráðstafanir sem gera skal og tilkynna nefndinni um niðurstöður mats á ráðstöfunum.

7. gr.

Fulltrúi framkvæmdastjórnarinnar leggur fyrir nefndina drög að þeim ráðstöfunum sem gera skal. Nefndin skal skila álit sínu á drögum innan þeirra tímamarka sem formanni er heimilt að setja eftir því hversu brýnt málið er, með atkvæðagreiðslu ef þörf krefur.

Álitið skal skráð í fundargerð; þar að auki hefur hvert aðildarríki rétt á að láta bóka afstöðu sína í fundargerðina.

Framkvæmdastjórnin skal taka ýtrasta tillit til álits nefndarinnar. Henni ber að greina nefndinni frá því með hvaða hætti álit hennar var haft til hliðsjónar.

8. gr.

Fulltrúi framkvæmdastjórnarinnar leggur fyrir nefndina drög að þeim ráðstöfunum sem gera skal. Nefndin skal skila álit sínu innan þeirra tímamarka sem formanni er heimilt að setja eftir því hversu brýnt málið er. Álitið skal samþykkt

með þeim meirihluta sem kveðið er á um í 2. mgr. 148. gr. sáttmálans þegar um er að ræða ákvarðanir sem ráðinu ber að samþykka að tillögu framkvæmdastjórnarinnar. Atkvæði fulltrúa aðildarríkjanna vega eins og kveðið er á um í þeirri grein. Formaður greiðir ekki atkvæði.

Framkvæmdastjórnin skal samþykka fyrirhugaðar ráðstafanir ef þær eru í samræmi við álit nefndarinnar.

Séu fyrirhugaðar ráðstafanir ekki í samræmi við álit nefndarinnar, eða skili nefndin ekki álit, ber framkvæmdastjórninni án tafar að leggja tillögu fyrir ráðið um ráðstafanir sem

gera skal. Ráðið tekur ákvörðun með auknum meirihluta.

Hafi ráðið ekkert aðhafst innan þriggja mánaða frá því að tillagan var lögð fyrir það skal framkvæmdastjórnin samþykka fyrirhugaðar ráðstafanir, svo fremi þær hafi ekki verið felldar í ráðinu með einföldum meirihluta atkvæða.

Gjört í Brussel 31. mars 1992.

Fyrir hönd ráðsins

Vitor MARTINS

forseti.

VIÐAUKI

Yfirlit yfir framkvæmdaáætlanir

STEFNUMÍÐ VIÐ GERÐ AÐGERÐAÁÆTLUNAR UM ÖRYGGI UPPLÝSINGAKERFA

INNGANGUR

Markmið aðgerðaáætlunarinnar er að þróa heildaraðgerðir sem miða að því að veita framleiðendum gagna sem eru geymd, unnin eða send í gegnum tölvu viðeigandi vernd upplýsingakerfa gegn hættu sem skapast vegna gáleysis eða af ásetningi.

Í aðgerðaáætluninni skal taka tillit til og auka við stöðlunarstarfsemi sem nú er í gangi á þessu sviði á alþjóðavettvangi.

Í henni skal m.a. fjallað um:

- þróun langtímaskipulags til að tryggja öryggi upplýsingakerfa;
- skilgreiningu á þörfum notenda og þeirra sem þjónustu veita að því er lýtur að öryggi upplýsingakerfa;
- lausnir sem fullnægja þörfum notenda, birgja og þjónustuaðila nú þegar og til skamms tíma;
- þróun forskrifta, stöðlunar og leiða til að meta og staðfesta öryggi upplýsingakerfa;
- framfarir í tækni og notkun upplýsingakerfa sem varða öryggi þeirra;
- ráðstafanir til að tryggja öryggi upplýsingakerfa.

Framkvæmdastjórnin sér um framkvæmd aðgerðaáætlunarinnar í nánnum tengslum við samsvarandi aðgerðir í aðildarríkjunum og rannsóknar- og þróunaradgerðir bandalagsins sem hún tengist.

1. I. framkvæmdaáætlun — Þróun langtímaskipulags til að tryggja öryggi upplýsingakerfa

Þetta er óhjákvæmilegt eigi að samræma ólíka hagsmuni og þarfir bæði við stefnumótun og í framkvæmd.

1.1. Málafni

Nauðsyn á að tryggja á viðeigandi hátt öryggi upplýsingakerfa er almennt viðurkennd í nútímaþjóðfélögum. Tölvuvædd upplýsingaþjónusta er háð öruggu fjarskiptakerfi og öruggum vél- og hugbúnaði, en einnig öryggi í notkun og stjórnun. Því ber að koma á langtímaskipulagi sem tekur til allra hliða öryggismála upplýsingakerfa og koma þannig í veg fyrir sundurleitar hlutalausnir. Skipulag fyrir öryggi upplýsingakerfa verður að endurspegla þörf þjóðfélagsins á tímum hraðra breytinga á að nýta upplýsingatækni á hagkvæman hátt en vernda sig jafnframt.

1.2. Markmið

Nauðsynlegt er að koma á langtímaskipulagi sem sameinar félagsleg, efnahagsleg og pólitísk markmið og veitir bandalaginu möguleika á mismunandi tæknilegum og lagalegum valmöguleikum í framkvæmd í alþjóðlegu samhengi. Til að halda jafnvægi milli ólíkra hagsmuna, markmiða og takmarkana ber fulltrúum allra þátttakenda í atvinnugreininni að standa saman að því að skilgreina vandamálið og samþykkja skipulagið.

1.3. Staða og horfur

Sem stendur er áhugi fyrir því að gripið verði til aðgerða. Verði hins vegar ekki víðtæk samstaða um að samræma þessar aðgerðir má telja líklegt að óskipulagðar aðgerðir á ýmsum sviðum muni leiða til ástands sem er innbyrðis ósamrýmanlegt og skapa síversnandi lagaleg, félagsleg og efnahagsleg vandkvæði.

1.4. Þarfir, valmöguleikar og forgangsverkefni

Innan sameiginlegs ramma er þörf á að taka afstöðu til hættugreiningar og stýringar, með hliðsjón af því hversu viðkvæmar upplýsingarnar eru og þjónusta sem tengist þeim, hvernig aðlaga megi lög og reglugerðir um misnotkun og óheimilaða notkun á tölvu- eða fjarskiptatækni, hvaða stjórnunargrundvöllur er þegar fyrir hendi, þ.m.t. ráðstafanir í öryggismálum, hvernig unnt sé að framfylgja lögnum innan ýmissa atvinnu- eða starfsgreina og félagslegra atriða og upplýsingaleyndar (t.d. með því að taka upp aðferðir til að þekkja og staðfesta notendur, koma í veg fyrir óréttmæta brottvísun og heimila þeim aðgang að kerfunum á lýðræðislegan hátt).

Setja þarf skýrar reglur um hönnun kerfa og hugbúnaðar sem tryggja öryggi upplýsingamiðlunar um staðla, skilgreiningar og vinnureglur sem tryggja öruggan búnað og þjónustu í upplýsingaiðnaði og stuðla að æfinga- og kynningarverkefnum til að fylgja eftir ýmis konar stjórnsýslulegri uppbyggingu, kerfum og stöðlum til að fullnægja þörfum í einstökum atvinnugreinum.

Nauðsynlegt er að vekja athygli á öryggismálum til að notendur verði meðvitaðri um öryggi í upplýsingatækni.

2. II. framkvæmdaáætlun — Skilgreining á þörfum notenda og þeirra sem veita þjónustu að því er lýtur að öryggi upplýsingakerfa

2.1. Málefni

Öryggi upplýsingakerfa er algjört skilyrði fyrir því að hægt sé að tryggja heildstæða og trausta notkun þeirra í viðskiptum, vernda hugverkarétt og gæta trúnaðar við meðferð gagna. Þetta leiðir óhjákvæmilega til ójafnvægis og stundum verður að meta hvort vegur þyngra, viðleitni til að stuðla að firjalsum viðskiptum eða vernda einkamál og hugverkarétt. Nauðsynlegt er að höfð sé hliðsjón af öllum þörfum og hugsanlegum áhrifum ýmissa valmöguleika á öryggi upplýsingakerfa þegar ákvarðanir og málamiðlanir eru gerðar.

Til að fullnægja þörfum notenda verður að tengja tæknilegar ráðstafanir ráðstöfunum um notkun kerfa og eftirlit með þeim. Þess vegna er kerfisbundin rannsókn á öryggisþörf í sambandi við upplýsingakerfi verulegur hluti af vinnunni við að þróa heppilegar og árangursríkar aðferðir.

2.2. Markmið

Markmiðið er að skilgreina eðli og eiginleika þeirra þarfa sem notendur og þeir sem þjónustu veita hafa og tengsl þeirra við öryggisráðstafanir vegna upplýsingakerfa.

2.3. Staða og horfur

Hingað til hefur ekki verið efnt til samræmds átaks í að skilgreina þörf hinna mismunandi aðila fyrir örugg upplýsingakerfi en sú þörf er sibreytileg. Aðildarríkin hafa skilgreint þörfina fyrir samræmdar innlendar aðferðir (einkum að því er snertir viðmiðanir við mat á öryggi upplýsingatækni). Mjög mikilvægt er að beitt sé sömum forsendum og reglum við gagnkvæma viðurkenningu á matsvottorðum.

2.4. Þarfir, valmöguleikar og forgangsverkefni

Talið er nauðsynlegt að flokka þarfir notenda og leiðir til að tryggja öryggi upplýsingakerfa, til að mynda grundvöll fyrir

samkvæmum og skýrum lausnum á þörfum allra þátttakenda í greininni.

Þar að auki er nauðsynlegt að skilgreina þörfina fyrir löggjöf, reglugerðir og siðareglur í ljósi horfanna í þjónustu- og tækni- iðnaði, að benda á hugsanlega valmöguleika til að uppfylla markmiðin, með ákvæðum á sviði stjórnsýslu eða varðandi þjónustu, notkun og tækni og að meta árangur, notendaviðmót og kostnað við að taka upp aðra valmöguleika eða fyrirætlanir um öryggi upplýsingakerfa, fyrir notendur, þá sem þjónustu veita og þá sem starfrækja slík kerfi.

3. III. framkvæmdaáætlun — Lausnir sem fullnægja þörfum notenda, birgja og þjónustuaðila nú þegar og til skamms tíma

3.1. Málefni

Sem stendur er unnt að tryggja upplýsingakerfi fullkomlega fyrir aðgangi með „einangrun“, þ.e. með því að beita hefðbundnum öryggisráðstöfunum við uppbyggingu og tengingu kerfa. Það sama gildir um tölvusamskipti notenda í lokuðum hópi sem tengjast í gegnum einkanet. Aðstæður eru allt aðrar ef fleiri hópar notenda hafa aðgang að upplýsingunum eða kerfið er tengt almenningsneti eða neti sem menn hafa mjög greiðan aðgang að. Í slíkum tilvikum er yfirleitt hvorki fyrir hendi tækni, útstöðvar og þjónustueiningar, né reglur og staðlar sem tengjast þeim, til að tryggja öryggi upplýsingakerfa.

3.2. Markmið

Markmiðið er að finna, með stuttum fyrirvara, lausnir á brýnustu þörfum notenda, þeirra er þjónustu veita og framleiðenda. Þetta felur í sér m.a. notkun hinna sameiginlegu viðmiðana til að meta öryggi upplýsingatækni. Hanna ber slíkar lausnir með tilliti til hugsanlegra þarfa og lausna síðar.

3.3. Staða og horfur

Nokkrir hópar notenda hafa þróað tækni og aðferðir sem henta notkun þeirra sjálfra og svara einkum þörfinni fyrir sannprófun, heildstæðni og vörn gegn brottvísun („non-repudiation“). Þetta felur yfirleitt í sér notkun segulkorta eða aðgangskorta. Ýmsir nota einfaldar eða flóknar aðferðir til að þekkja skrift manna. Slík tækni krefst yfirleitt að skilgreindar verði heimildir fyrir takmarkaðan hóp „viðurkenndra notenda“. Erfitt er hins vegar að aðlaga þessar aðferðir og tækni að þörfum opins kerfis.

Alþjóðastaðlastofnunin vinnur nú að öryggisstöðlum fyrir samtengingu opinna kerfa (OSI) (ISO DIS 7498-2) og ráðgjafarnefndin um tækninýjungar og -yfirfærslu (CCITT) fjallar um málin sem hluta af X400-verkefninu. Einnig er hugsanlegt að bæta öryggisbútm inn í sendingarnar. Verið er að skoða leiðir til að tryggja sannprófun, heildstæðni og vörn gegn brottvísun í sambandi við boðsendingar (EDIFACT) og X400.

Sem stendur er löggjöf um gagnaskipti með tölvum (EDI) enn á frumstigi. Alþjóðaverslunarráðið hefur birt siðareglur um skipti á viðskiptagögnum í gegnum fjarskiptakerfi.

Nokkur lönd (t.d. Þýskaland, Frakkland, Breska konungsríkið og Bandaríki Norður-Ameríku) hafa þróað eða eru að þróa viðmiðanir til að meta öryggi vara og -kerfa fyrir upplýsingatækni og fjarskipti og reglur um hvernig slíkt mat eigi að fara fram. Þessar reglur hafa verið unnar í samstarfi við innlenda framleiðendur og munu leiða til aukningar á öruggum búnaði og kerfum sem í boði er, einföldum búnaði til að byrja með. Með stofnun innlendra samtaka til að meta og votta öryggi kerfanna verður unnt að efla þessa þróun.

Flestir notendur telja ekki eins aðkallandi að gera ráðstafanir til að gæta trúnaðar við meðferð gagna. Líklegt má þó telja að þetta eigi eftir að breytast eftir því sem fjarskiptatækni, einkum sem tengist farsímaþjónustu, verður algengari.

3.4. Þarfir, valmöguleikar og forgangsverkefni

Nauðsynlegt er að þróa eins fljótt og framast er unnt reglur, staðla, vörur og búnað til að tryggja öryggi, bæði í kerfunum sjálfum (tölvum og jaðartækjum) og opinberum fjarskiptakerfum. Leggja ber aðaláherslu á sannpröfun, heildstæðni og vörn gegn brottvísun í kerfunum. Setja ber á stofn æfingaverkefni til að prófa gæði lausnanna sem fyrirhugaðar eru. Verið er að athuga lausnir varðandi þörf á forgangi í sambandi við EDI innan TEDIS-áætlunarinnar.

4. IV. framkvæmdaáætlun — Þróun forskrifa, stöðlunar og leiða til að meta og staðfesta öryggi upplýsingakerfa

4.1. Málefni

Alls staðar þarf að tryggja öryggi upplýsingakerfa og þess vegna gegna sameiginlegar forskrifa og staðlar lykilhlutverki. Skortur á samþykktum stöðlum og forskriftum fyrir öryggi upplýsingatækni getur verið mikil hindrun við framfarir í upplýsingavinnslu og þjónustu í þjóðfélaginu og í viðskiptalífi. Aðgerða er einnig þörf til að hraða þróun og notkun tækni og staðla á ýmsum sviðum sem tengjast tölvunetum og fjarskiptum og hafa grundvallarþýðingu fyrir notendur, atvinnulíf og stjórnsýslu.

4.2. Markmið

Nauðsynlegt er að leita leiða til að stuðla að og koma á sérstökum öryggisráðstöfunum á almennum sviðum eins og samtengingu opinna kerfa (OSI), frjálsum aðgangi að netum (ONP), stafrænu samþætту þjónustuneti (ISDN/IBC) og netstjórnun. Náteyndar staðla- og forskriftamállum eru spurningar um tækni og leiðir sem nota eigi við sannpröfun, þar á meðal vottun sem leið til gagnkvæmrar viðurkenningar. Þegar við verður komið skal styðja lausnir sem fengið hafa alþjóðasamþykki. Stuðla ber einnig að þróun og notkun tölvukerfa með innbyggðum öryggisráðstöfunum.

4.3. Staða og horfur

Þýðingarmiklar aðgerðir hafa verið samþykktar til að tryggja öryggi upplýsingakerfa, einkum í Bandaríkjum Norður-Ameríku. Í Evrópu er fjallað um þessi mál í sambandi við upplýsingatækni almennt og stöðlun fjarskipta á vegum Fjarskiptastaðlastofnunar Evrópu (ETSI) og Staðla- og Rafstaðlastofnunar Evrópu (CEN/CENELEC), í ráðgjafarnefndinni um tækninýjungar og -yfirfærslu (CCITT) og hjá Alþjóðastaðlastofnuninni (ISO).

Vaxandi áhyggjur manna hafa orðið til þess að vinna á þessu sviði hefur aukist í Bandaríkjunum og bæði seljendur og þeir sem þjónustu veita leggja aukna áherslu á þessi mál. Í Frakklandi, Þýskalandi og Breska konungsríkinu hafa svipaðar ráðstafanir verið gerðar en hægt miðar að þróa sameiginlegt átak í Evrópu er samsvarar því gerist í Bandaríkjunum.

4.4. Þarfir, valmöguleikar og forgangsverkefni

Til að tryggja öryggi upplýsingakerfa er óhjákvæmilegt að tengja saman vinnu á sviði löggjafar, notkunar, stjórnunar og tækni. Innihald reglugerða verður að koma fram í stöðlum og ráðstafanir vegna öryggis upplýsingakerfa verða að vera í samræmi við staðla og reglugerðir þannig að unnt sé að sannprófa þær. Á ýmsum sviðum krefjast reglugerðir forskrifa sem hafa víðara gildi en almennir staðlar og fela í sér t.d. siðareglur. Kröfur um staðla og siðareglur eru til staðar öllum sviðum sem tengjast öryggi upplýsingakerfa og gera verður greinarmun á kröfum um vernd, sem falla undir öryggismarkmið, og tæknilegum kröfum sem falla undir lögsögu lögbærra stöðlunarstofnana (CEN/CENELEC/ETSI).

Nauðsynlegt er að forskrifa og staðlar nái yfir öryggisþjónustu við upplýsingakerfi (sannpröfun einstaklinga og fyrir-tækja, aðferðir gegn óréttmætri brottvísun, tölvuvitnisburður sem hefur lagalegt gildi, eftirlit með veitingu heimilda), viðskiptaþjónustu sem í boði er (til að gæta öryggis í myndflutningi, farsímasendingum á tali eða gögnum, gagna- og myndgagnasendingum og samþættri þjónustu), stjórnun á samskiptum og öryggismálum (opinbert lykla- eða einkalyklakerfi fyrir aðgang að opnum netum, vernd fyrir netstjórnun og fyrir þá sem þjónustu veita) og vottun þeirra (kröfur um öryggi á mismunandi stigum, reglur um hvaða kröfur má gera um örugg upplýsingakerfi).

5. V. framkvæmdaáætlun — framfarir í tækni og notkun upplýsingakerfa sem varða öryggi þeirra

5.1. Málefni

Skipuleg rannsókn og þróun tækni sem leiðir til hagkvæmra og fullnægjandi lausna í framkvæmd á margs konar þörfum vegna öryggis upplýsingakerfa nú og síðar er algjört skilyrði fyrir þróun markaðarins í upplýsingaþjónustu og til að tryggja samkeppnisstöðu evrópsks iðnaðar almennt.

Við þróun tækni sem lýtur að öryggi upplýsingakerfa verður að leitast við að tryggja öryggi bæði tölvugagna og tölvusamskipta, vegna þess að nú eru flest kerfi tengd dreifinganetum og aðgangur að þeim er veittur í gegnum fjarskiptaþjónustu.

5.2. *Markmið*

Skipuleg rannsókn og þróun tækni sem leiðir til hagkvæmra og fullnægjandi lausna á margs konar þörfum vegna öryggis upplýsingakerfa nú og síðar.

5.3. *Þarfir, valmöguleikar og forgangsverkefni*

Aðgerðir til að tryggja öryggi upplýsingakerfa verða að fela í sér fyrirætlanir um þróun og framkvæmd, nýta tækni og gera ráð fyrir samþættingu og sannprófun.

Með rannsóknar- og þróunarvinnu til langs tíma skal leitast við að þróa heildarlíkön fyrir örugg kerfi (sem eru vernduð gegn skemmdum, óheimilum breytingum og óréttmætri brottvísun), vinnslulíkön fyrir þarfir við notkun, áhættulíkön og uppbyggingu öryggiskerfa.

Rannsóknar- og þróunarvinna á tæknisviði skal ná yfir staðfestingu á notendum og boðum (t.d. með raddgreiningu og tölvuundirskriftum), tæknilega skilfleti og aðferðir við brenglun, búnað til að takmarka aðgang og leiðir til að taka í notkun kerfi sem eru örugg og unnt er að sannprófa.

Rannsaka skal sannprófun og staðfestingu á öryggi tæknikerfa og nothæfi þeirra innan verkefna á sviði samþættingar og sannprófunar.

Þörf er á, til viðbótar við samhæfingu og þróun öryggistækni, ýmsum hliðarráðstöfunum sem lúta að gerð, viðhaldi og samkvæmri beitingu staðla og sannprófun og vottun upplýsingatækni og fjarskiptabúnaðar að því er varðar öryggi þeirra, þar með talið sannprófun og vottun aðferða til að hanna og taka í notkun kerfi.

Nota má þriðju rammaáætlun bandalagsins um rannsóknir og þróun til að efla samstarfsverkefni á forstigum, áður en til samkeppni eða stöðlunar kemur.

6. **VI. framkvæmdaáætlun — ráðstafanir til að tryggja öryggi upplýsingakerfa**6.1. *Málefni*

Með tilliti til eðlis upplýsingakerfisins, verður að gera ráðstafanir sem þarf til að tryggja öryggi á ýmsum stöðum í upplýsingakerfinu, m.a. í tölvum/útstöðvum, í þjónustukerfinu og við netstjórnun með því að nota brenglunarþúnað, aðgangskort, opinbera lykla, einkalykla, o.s.frv. Búast má við að seljendur bjóði ýmis konar vél- og hugbúnað með innbyggðum vörnum en aðrar fylgi dreifingakerfunum (t.d. netstjórnun), tilheyri notendum (t.d. aðgangskort) eða fáist frá sérstökum aðilum (t.d. opinberir lykjar/einkalyklar).

Búast má við að seljendur, þeir sem þjónustu veita og þeir sem starfrækja kerfi sjái um meirihluta öryggisbúnaðarins. Ef til vill getur verið þörf á að tilgreina viðeigandi stofnanir eða samtök og veita þeim umboð til að gegna tilteknu hlutverki, t.d. við að útvega opinbera lykla/einkalykla eða halda reiðu á veitingu aðgangsheimilda.

Það sama gildir um vottun, mat og sannprófun á gæðum þjónustunnar, en sjá verður til þess að stofnanir eða samtök sem annast það séu óháð seljendum, þeim sem þjónustu veita og þeim sem starfrækja kerfi. Slíkir aðilar geta starfað á eigin vegum, á vegum hins opinbera eða með opinberu leyfi til að sinna tilteknum verkefnum.

6.2. *Markmið*

Til að greiða fyrir samfelldri þróun í öryggismálum upplýsingakerfa í bandalaginu og til að vernda hagsmuni hins opinbera og einkaaðila verður nauðsynlegt að gæta samkvæmni í að tryggja öryggi. Þar sem heimila verður starfsemi sjálfstæðra stofnana eða samtaka skal skilgreina og samþykkja hlutverk þeirra og starfsskilyrði og, ef þörf krefur, setja lagaákvæði um það. Markmiðið er að ná samkomulagi um skýrt afmarkaða skiptingu ábyrgðar milli allra þátttakenda á þessu sviði í bandalaginu, sem er forsenda fyrir gagnkvæmri viðurkenningu.

6.3. *Staða og horfur*

Sem stendur eru ráðstafanir til að tryggja öryggi upplýsingakerfa einungis vel skipulagðar á ákveðnum sviðum og takmarkast við að fullnægja sérþörfum þeirra. Heildarskiptulag í bandalaginu er almennt á könnunarstigi og engin gagnkvæm viðurkenning á sannprófun og vottun er fyrir hendi fyrir utan lokaðra hópa. Eftir því sem mikilvægi upplýsingakerfa eykst verður þörfin æ brýnni fyrir samræmd viðbrögð til að tryggja öryggi upplýsingakerfa í Evrópu og um heim allan.

6.4. *Þarfir, valmöguleikar og forgangsverkefni*

Vegna þess hversu margir eiga hér hlut að máli og hversu háð lögum og reglugerðum málið er, er afar brýnt að ná samkomulagi fyrirfram um reglurnar sem gilda eiga um öryggisráðstafanir fyrir upplýsingakerfi.

Til að vinna verkið á samhentan og samkvæman hátt verður að fjalla um hvernig greina má og skilgreina starfsemi sem, vegna eðlis síns, þarf sjálfstæð samtök eða stofnanir (eða samstarfsstofnanir) til að sinna. Undir þetta fellur m.a. umsjón með opinberum lykklum/einkalyklum.

Þar að auki er nauðsynlegt að greina og skilgreina á byrjunarstigi hvaða starfsemi ber að fela sjálfstæðum stofnunum eða samtökum (eða samstarfsstofnunum) til þess að gæta hagsmuna almennings. M.a. gæti verið um endurskoðun, gæðatryggingu, sannprófun, vottun og sambærileg störf að ræða.