EUROOPA ÜHENDUSTE KOMISJON

Brüssel 31.5.2006
KOM(2006) 251 lõplik

KOMISJONI TEATIS NÕUKOGULE, EUROOPA PARLAMENDILE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE JA REGIOONIDE KOMITEELE

Turvalise infoühiskonna strateegia – dialoog, partnerlus ja aktiivne osalemine

{SEK(2006) 656}

SISUKORD

1. Sissejuhatus 3
2. Infoühiskonna turvalisuse parandamine: põhiprobleemid 4
3. Dünaamiline lähenemisviis turvalisele infoühiskonnale 6
3.1. Dialoog 7
3.2. Partnerlus 8
3.3. Aktiivne osalemine 9
4. Järeldused 10

KOMISJONI TEATIS NÕUKOGULE, EUROOPA PARLAMENDILE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE JA REGIOONIDE KOMITEELE

Turvalise infoühiskonna strateegia – dialoog, partnerlus ja aktiivne osalemine

1. SISSEJUHATUS

Teatises „i2010 - Euroopa infoühiskond majanduskasvu ja tööhõive eest“[1] tõsteti esile võrgu- ja teabeturbe tähtsust ühtse Euroopa inforuumi loomisel. Majanduse ja ühiskonna ülesehituse seisukohalt on võrkude ja infosüsteemide kättesaadavus, usaldusväärsus ja turvalisus järjest kesksema tähtsusega.

Käesoleva teatise eesmärk on anda uut hoogu Euroopa Komisjoni strateegiale, mis esitati aastal 2001 teatises „Võrgu- ja teabeturve: ettepanek Euroopa poliitilise lähenemisviisi kohta“[2]. Teatises vaadatakse läbi infoühiskonda ähvardavate ohtude hetkeseisu ja määratakse kindlaks, missuguseid lisameetmeid tuleks võrgu- ja teabeturbe parandamiseks võtta.

Eesmärgiks on Euroopas jätkuvalt arendada liikmesriikide ja Euroopa Ühenduse tasandil saadud kogemustele toetudes dünaamilist globaalset strateegiat, mis on rajatud turvakultuurile ja põhineb **dialoogil, partnerlusel ja aktiivsel osalemisel**.

Infoühiskonna turvaprobleemidega tegelemiseks on Euroopa Ühendus arendanud välja kolmesuunalise lähenemisviisi, mis hõlmab: konkreetseid võrgu- ja teabeturbe meetmeid, elektroonilist sidet reguleerivat raamistikku (mis sisaldab ka eraelu puutumatuse ja andmekaitse küsimusi) ja võitlust küberkuritegude vastu. Kuigi neid kolme tahku on teatud määral võimalik arendada iseseisvalt, on arvukate vastastikuste mõjude tõttu parem kasutada kooskõlastatud strateegiat. Käesolevas teatises sätestatakse võrgu- ja teabeturbe sidusa lähenemisviisi edasiarendamise ja täiustamise strateegia ning esitatakse selle raamistik.

2001. aasta teatises määratletakse võrgu- ja teabeturve kui *võrgu- või infosüsteemi võime kaitsta end teatava kindlusega õnnetuste või pahatahtlike tegevuste eest, mis seavad ohtu salvestatud või edastatud andmete ja nende võrkude ja süsteemide poolt pakutavate või nende kaudu juurdepääsetavate teenuste kättesaadavuse, autentsuse, terviklikkuse ja konfidentsiaalsuse*. Euroopa Ühendus on võtnud viimastel aastatel kasutusele mitmeid meetmeid võrgu- ja teabeturbe parandamiseks.

Elektroonilist sidet reguleeriv raamistik, mida praegu läbi vaadatakse, sisaldab turvalisusega seotud sätteid. Eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv[3] hõlmab üldkasutatavate elektrooniliste sideteenuste osutajate kohustust tagada oma teenuste turvalisus. Sätestatud on rämpsposti[4] ja nuhkvara[5] vastased normid.

Euroopa Ühenduse teadusuuringute ja arendustegevuse programmides on usaldusel ja turvalisusel samuti tähtis koht. Teadusuuringute kuues raamprogramm käsitleb neid küsimusi

---

1 KOM(2005) 229 (lõplik), 1.6.2005.
2 KOM(2001) 298 (lõplik), 6.6.2001.
3 Direktiiv 2002/58/EÜ.
4 Või pealesunnitud kommertsteadaanded.
5 Nuhkvara on jälgimistarkvara, mida kasutatakse kasutaja teadmata, nõusolekuta ja kontrollita.

väga paljudes projektides. Euroopa turvalisusuuringute programmi (ESRP)[6] loomisega tugevdatakse seitsmendas raamprogrammis turvalisusega seotud uurimistegevust veelgi. Lisaks eelnevale toetatakse võrguprojekte ja heade tavade vahetust võitluses infovõrkudes leviva kahjuliku materjali vastu programmiga Safer Internet Plus.

2004. aastal otsustas Euroopa Ühendus luua vastumeetmena turvaohtudele Euroopa Võrgu- ja Infoturbe Ameti (ENISA). ENISA aitab kogu Euroopa Liidu (EL) kodanike, tarbijate, ettevõtete ja avaliku sektori organisatsioonide huvides kaasa võrgu- ja teabeturbe kultuuri edendamisele.

EL on kõnesolevate teemade käsitlemisel aktiivne ka rahvusvahelistel foorumitel, nagu OECD, Euroopa Nõukogu ja ÜRO. Infoühiskonda käsitleval tippkohtumisel Tuneesias toetas EL innukalt arutelusid võrkude ja teabe kättesaadavuse, usaldusväärsuse ja turvalisuse kohta. Tuneesia agendas[7], milles koos Tuneesia deklaratsiooniga sätestatakse maailma riigijuhtide poolt heaks kiidetud globaalse infoühiskonna teemalise poliitikaarutelu edasised etapid, tõstetakse esile vajadus jätkata võitlust küberkuritegude ja rämpsposti vastu, kindlustades ühtlasi eraelu puutumatuse ja sõnavabaduse. Selles tuuakse välja vajadus tagada kõigi sidusrühmade vahel üksmeel Interneti turvalisust käsitlevates küsimustes ja edasise koostöö vajadus turvaalase teabe kogumise ja levitamise ning turvaohtudega võitlemise meetmetega seotud heade tavade vahetamise lihtsustamiseks.

2. INFOÜHISKONNA TURVALISUSE PARANDAMINE: PÕHIPROBLEEMID

Vaatamata rahvusvahelisel, Euroopa ja siseriiklikul tasandil tehtavatele pingutustele on turvalisusega jätkuvalt seotud tõsised probleemid.

Rünnakuid infosüsteemidele motiveerib üha enam pigem kasusaamise võimalus kui soov põhjustada häireid häirete endi pärast. Kuna õelvara[8] versioonide arv (ja arengutempo) kiirelt kasvab, otsitakse andmed järjest sagedamini välja ebaseaduslikult, kasutaja teadmata. Rämpspost, mis on muutumas nuhkvara, andmepüügi[9] ja muude õelvara liikide näol viiruste, pettuse ja kriminaalse tegevuse vahendiks, on niisuguse arengu heaks näiteks. Selle laialdane levitamine põhineb üha enam *zombi*-võrkudel[10], st kompromiteeritud serveritel ja personaalarvutitel, mida kasutatakse omanike teadmata vahelülidena.

Mobiilseadmete, kaasa arvatud 3G mobiiltelefonide, kaasaskantavate videomängude jms järjest suurenev kasutamine ja mobiilsidel põhinevad võrguteenused pakuvad uusi väljakutseid, kuna IP-põhised teenused arenevad kiiresti. Seega võivad need muutuda palju üldlevinumaks ründekanaliks kui personaalarvutid, kuna viimaste puhul on turvatase juba märkimisväärne. Kõik sideplatvormide ja infosüsteemide uued liigid toovad paratamatult kaasa uusi võimalusi pahatahtlikeks rünnakuteks.

---

6 ESPR valmib aastatel 2004-2006 turvalisusalast uurimistegevust ettevalmistava tegevuse käigus.

7 „Globaalse partnerluse poole infoühiskonnas: infoühiskonna maailma tippkohtumise (WSIS) Tunise faasi jätkumeetmed“, KOM(2006) 181 (lõplik), 27.4.2006.

8 Õelvara tähendab kahjulikku tarkvara.

9 Andmepüük on Interneti-pettuse vorm, mille eesmärgiks on väärtusliku info, nagu krediitkaardi andmete ja kontonumbrite, kasutajanimede ja salasõnade varastamine.

10 *Zombi*-võrgud on *bot*-rakenduste poolt nakatatud arvutitest moodustunud võrgud, mis töötavad autonoomselt kaugjuhtimise abil ja mis paigaldatakse salaja ohvri arvutisse.

Teiseks oluliseks arengujooneks on aruka keskkonna süsteemide väljakujunemine, milles informaatika ja võrkude loomise tehnoloogial tuginevad arukad seadmed muutuvad laialdaselt kasutatavateks, nt RFID[11], IPv6 ja sensorvõrkude kaudu. Täielikult vastastikku seotud ja võrku ühendatud igapäevaelu pakub tähelepanuväärseid võimalusi. Siiski tekitab see ka turvalisuse ja eraelu puutumatusega seotud täiendavaid riske. Kuigi ühised platvormid ja rakendused mõjutavad koostalitlusvõimet ning info- ja sidetehnoloogiate kasutuselevõttu positiivselt, võivad nad suurendada ka riskiohtu. Näiteks, mida rohkem kasutatakse saritarkvara, seda enam mõjub turvaaukude ärakasutamine või vigade teke. Kindlat tüüpi monokultuuride tekkimine tarkvaraplatvormides ja rakendustes võib õelvara ja viiruste taoliste turvariskide suurenemist ja levikut oluliselt lihtsustada. **Mitmekesisus, avatus ja koostalitlusvõime on turvalisuse lahutamatu osa ning neid tuleks edendada**.

Info- ja sidetehnoloogia sektori olulisus Euroopa majanduse ja Euroopa ühiskonna kui terviku seisukohalt on vaieldamatu. Info- ja sidetehnoloogia on uuenduste üliolulise koostisosa, mis annab ligi 40% tootlikkuse kasvust. Kõnesoleva äärmiselt uuendusliku sektori arvele langeb enam kui veerand Euroopa kogu uurimis- ja arendustegevusest ning majanduse seisukohalt tervikuna on sellel majanduskasvu ja töökohtade loomise osas keskne koht. Järjest rohkem eurooplasi elab tõeliselt teabepõhises ühiskonnas, kus info- ja sidetehnoloogia kasutamine inimeste sotsiaalse ja majandusliku suhtlemise põhifunktsioonina on kiiresti kasvanud. Eurostati andmete kohaselt kasutas 2004. aastal ELi ettevõtetest 89% aktiivselt Internetti ja umbes 50% tarbijatest oli seda äsja teinud[12].

Võrgu- ja teabeturbe rikkumine võib tuua kaasa majandusmõõtmest oluliselt kaugemale ulatuvaid tagajärgi. Arvestades asjaolu, et kättesaadavus, usaldusväärsus ja turvalisus on siduskeskkonnas põhiõiguste tagamise eeltingimus, kardetakse üldiselt, et turvaprobleemid võivad kasutajaid heidutada ning info- ja sidetehnoloogia kasutuselevõttu aeglustada.

Lisaks sellele muutuvad muud ülitähtsad infrastruktuurid, nagu transport ja energeetika, võrkudevahelise suurenenud ühenduvuse tõttu vastavate infosüsteemide terviklikkusest üha enam sõltuvaks.

Euroopas alahindavad veel ohtu nii äriettevõtted kui kodanikud. Sellel on mitmeid põhjuseid, millest ettevõtete puhul näib kõige olulisem olevat see, et turvalisusesse investeerimisest saadav tulu ei ole käegakatsutav, ja kodanike puhul asjaolu, et nad ei ole teadlikud oma vastutusest ülemaailmses turvaahelas.

Arvestades info- ja sidetehnoloogia ning infosüsteemide laialdast kasutatavust, on võrgu- ja teabeturve muidugi kõigi probleem:

- **riiklikud haldusasutused** peavad tegelema oma süsteemide turvalisusega mitte ainult avaliku sektori alase teabe kaitsmiseks, vaid ka selleks, et olla teistele heade tavade kasutamisel eeskujuks;

- **ettevõtted** peavad käsitlema võrgu- ja teabeturvet pigem kasu ja konkurentsieeliseid andva asjaoluna kui negatiivse kuluna;

---

[11] Raadiosagedustuvastus.

[12] Eurostat, Interneti-tegevus Euroopa Liidus, 40/2005.

- **üksikkasutajad** peavad mõistma, et nende kodusüsteemid on üldise turvaahela jaoks otsustava tähtsusega.

Eespool kirjeldatud probleemidega edukaks tegelemiseks vajavad kõik sidusrühmad usaldusväärseid andmeid teabeturbega seotud intsidentide ja suundumuste kohta. Mitmel põhjusel on raske saada usaldusväärseid ja põhjalikke andmeid niisuguste intsidentide kohta, alates kiirusest, millega turvaprobleemid võivad esile kerkida, kuni mõnede organisatsioonide soovimatuseni turvariketest teatada ja neid avalikustada. Sellele vaatamata on **teadlikkuse tõstmine kõnesoleva probleemi kohta** üks turvakultuuri arendamise nurgakividest.

Oluline on see, et turvaohtudest märku andmiseks ettenähtud teavitusprogrammid ei kahandaks tarbijate ja kasutajate usaldust sellega, et neis keskendutakse üksnes turvalisuse negatiivsetele aspektidele. Seetõttu tuleks võimaluse korral **võrgu- ja teabeturvet tutvustada pigem eelise ja võimalusena** kui kohustuse ja kuluna. Sellesse tuleks suhtuda kui usaldusväärsuse tekitamise ja tarbijate usalduse võitmise vahendisse, infosüsteeme kasutavate ettevõtete konkurentsieelisesse ning avaliku ja erasektori teenuseosutajate teenuse kvaliteedi küsimusse.

Tervikliku lähenemisviisi saavutamine selles küsimuses on poliitikakujundajate jaoks peamiseks väljakutseks. Kõnealuses lähenemisviisis peaks arvestama erinevate sidusrühmade rolli. See peaks tagama paljude avalikku korda käsitlevate ja muude õigusnormide kooskõlastamise, mis võrgu- ja teabeturvet otseselt või kaudselt mõjutavad. Ülesannet ei tee kergemaks see, et liberaliseerimine, riikliku sekkumise vähendamine ja ühtlustamine on tekitanud erinevate sidusrühmade hulgas arvukalt kõnesolevas valdkonnas tegutsejaid. ENISA võib anda olulise panuse selle eesmärgi saavutamisse. Info- ja sidetehnoloogia tööstuse konkurentsivõime ja hästitoimiva siseturu huvides võiks ENISA olla nii Euroopa-siseselt kui muu maailmaga teabevahenduse, kõigi sidusrühmade koostöö ja väärtuslike kogemuste vahetamise keskuseks.

3. DÜNAAMILINE LÄHENEMISVIIS TURVALISELE INFOÜHISKONNALE

Turvaline infoühiskond peab olema rajatud **täiustatud võrgu- ja teabeturbele** ja üldisele **turvakultuurile**. Selles osas teeb Euroopa Komisjon ettepaneku **dünaamilise ja ühtse lähenemisviisi** kohta, mis hõlmaks kõiki sidusrühmi ja oleks rajatud **dialoogile, partnerlusele ja aktiivsele osalemisele**. Arvestades avaliku ja erasektori vastastikku täiendavat rolli turvakultuuri loomisel, peavad kõnealuse valdkonna poliitikaalgatused põhinema **paljude sidusrühmade osalusega avatud arutelul**.

Kõnesolev lähenemisviis ja sellega seonduvad meetmed täiendavad ja rikastavad komisjoni kavatsust jätkata 2006. aastal laiahaardelise ja dünaamilise poliitikaraamistiku väljaarendamist mitmete algatustega:

(1) käsitledes rämpsposti ja niisuguste ohtude nagu nuhkvara ja muude õelvara liikide arenemist teatises nende konkreetsete küsimuste kohta;

(2) tehes õiguskaitseasutuste vahelise koostöö parandamise ettepanekuid ja käsitledes kuritegeliku tegevuse uusi vorme, mis kasutavad ära Internetti ja kahjustavad ülitähtsate infrastruktuuride tööd. Sellele temaatikale keskendub kavandatav küberkuritegusid käsitlev teatis.

Eespool nimetatud poliitikaalgatused täiendavad ka 2004. aasta detsembri ülemkogu palvel komisjoni koostatud Euroopa esmatähtsa infrastruktuuri kaitse programmi käsitleva rohelise raamatu[13] eesmärkide saavutamiseks kavandatud tegevust. Kõnealuse tegevuse tulemusel koostatakse tõenäoliselt tegevuskava, milles esmatähtsa infrastruktuuri kaitse üldine lähenemisviis ühendatakse erinevate valdkondade vajaliku poliitikaga, muu hulgas info- ja sidetehnoloogia valdkonna poliitikaga. Info- ja sidetehnoloogia valdkondlik poliitika vaatleb **paljude sidusrühmadega peetava dialoogi** abil asjakohaseid majanduslikke, äritegevusalaseid ja ühiskondlikke liikumapanevaid jõude, et täiustada võrkude ja infosüsteemide turvalisust ja vastupidavust.

2006. aastal toimuval elektroonilist sidet reguleeriva raamistiku läbivaatamisel võetakse arvesse ka võrgu- ja teabeturbe parandamist soodustavaid asjaolusid, nagu teenuse osutaja poolt võetavad tehnilised ja organisatsioonilised meetmed, turvariketest teatamist käsitlevad sätted ning konkreetsed abinõud ja karistused kohustuste täitmata jätmise puhul.

Lõppkasutajale lahenduste, teenuste ja turbetoodete pakkumine sõltub palju erasektorist. Seetõttu on strateegiliselt tähtis, et **Euroopa tööstus oleks nii** turbetoodete ja -teenuste **nõudlik kasutaja kui ka** võrgu- ja teabeturbe toodete ja teenuste **konkurentsivõimeline pakkuja**.

Riikide valitsused peavad poliitika väljatöötamiseks suutma kindlaks määrata ja kasutada häid tavasid ning näitama oma valmidust neid poliitikaeesmärke oma infosüsteemide turvalise haldamise abil täita. Liikmesriikide ja ELi tasandi ametiasutustel on tähtis roll kasutajate põhjalikus teavitamises, et võimaldada neil anda oma panus iseenda turvalisuse ja ohutuse tagamisse. Prioriteetideks peaksid olema teadlikkuse tõstmine võrgu- ja teabeturbe küsimustes ning sihtotstarbeliste e-turvalisuse Interneti-portaalide vahendusel asjakohase ja õigeaegse teabe andmine nii ohtude, riskide ja hoiatuste kui ka heade tavade kohta. Seepärast võiks ENISA peamiseks eesmärgiks olla võimaluste uurimine sellise **Euroopa mitmekeelse teabevahenduse ja hoiatussüsteemi loomiseks**, mis koguks ja koondaks kokku liikmesriikide olemasolevad või kavandatavad avaliku ja erasektori algatused.

Võrgu- ja teabeturbe globaalne ulatus sunnib komisjoni suurendama pingutusi **võrgu- ja teabeturbealase ülemaailmse koostöö edendamisel** nii rahvusvahelisel kui liikmesriikidega kooskõlastamise tasandil, eriti 2005. aasta novembris toimunud maailma infoühiskonna tippkohtumisel vastuvõetud agenda rakendamise alal.

Uurimis- ja arendustegevus, iseäranis Euroopa Liidu tasandil, aitab välja arendada uusi ja uuenduslikke partnerlusi üldisemalt Euroopa info- ja sidetehnoloogia tööstuse ja eriti Euroopa info- ja sidetehnoloogiaalase turvatööstuse kasvu hoogustamiseks. Seepärast püüab komisjon tagada ELi seitsmenda raamprogrammi raames asjakohaste rahaliste vahendite määramise võrgu- ja teabeturbe ning usaldusväärsuse tehnoloogiate alasele uurimistegevusele.

3.1. Dialoog

*3.1.1. Komisjon teeb ettepaneku algatada ametiasutuste vahelise dialoogi intensiivistamise esimese etapina **siseriiklike võrgu- ja teabeturbealaste tegevuspõhimõtete** (sealhulgas avaliku sektori konkreetsete tegevuspõhimõtete) **võrdlev hindamine**. See tegevus aitab välja selgitada kõige tõhusamad lahendused, et neid võimaluse korral*

[13] KOM(2005) 576 (lõplik), 17.11.2005.

edaspidi kogu ELis laialdasemalt kasutada ja muuta riiklikud haldusasutused turvalisusalaste heade tavade liikumapanevaks jõuks. Selles suhtes võib olla tähtis koht tööl elektroonilise tuvastamise vallas, näiteks äsjase e-valitsuse tegevuskava osana.

Niisuguse õigesti struktureeritud võrdlusuuringu tulemusena on võimalik **kindlaks teha head tavad, mille abil suurendada VKEde ja kodanike teadlikkust** nende endi konkreetsete võrgu- ja teabeturbe probleemide ja nõuetega **tegelemise vajalikkusest** ja parandada nende suutlikkust seda praktiliselt teha. ENISA peaks selles dialoogis ning heade tavade koondamises ja vahendamises aktiivselt osalema.

*3.1.2. Tarvis on **struktureeritud ja paljusid sidusrühmi ühendavat arutelu** selle kohta, kuidas kasutada kõige paremini olemasolevaid vahendeid ja õigusakte, et kaitsta turvalisust ning põhiõigusi, kaasa arvatud eraelu puutumatust, asjakohase ühiskondliku tasakaalu saavutamiseks. Kavandatav konverents „i2010 – Euroopa kõikehõlmava infoühiskonna suunas", mille viib läbi järgmine eesistujamaa Soome, ja konsultatsioonid raadiosagedustuvastuse mõjust turvalisusele ja eraelu puutumatusele, mis on osaks hiljaaegu komisjoni käivitatud ulatuslikumast konsultatsiooniprotsessist, aitavad sellele arutelule kaasa. Lisaks sellele organiseerib komisjon:*

- ürituse ettevõtjatele, et ergutada neid võtma suurema pühendumisega tarvitusele tõhusaid abinõusid turvakultuuri rakendamiseks oma **tootmisharus**;

- seminari mõttevahetuseks elektrooniliste võrgu- ja infosüsteemide kasutamisel turvateadlikkuse tõstmise ja **lõpp-kasutajate** usalduse tugevdamise võimaluste üle.

3.2. Partnerlus

*3.2.1. Poliitika tõhusaks elluviimiseks tuleb probleemide iseloomu ja ulatust täielikult mõista. Selleks on lisaks teabeturbega seotud intsidente ning tarbija ja kasutaja usaldustaset käsitlevatele usaldusväärsetele ning ajakohastele statistika- ja majandusandmetele vaja ka ajakohastatud andmeid info- ja sidetehnoloogiaalase turvatööstuse suuruse ja suundumuste kohta Euroopas. Komisjon kavatseb teha ENISAle ettepaneku luua **liikmesriikide ja sidusrühmadega usaldusväärne partnerlus**, et töötada välja **asjakohane raamistik andmete kogumiseks**, sealhulgas turvaintsidente ja tarbijate usaldust käsitlevate, kogu ühendust hõlmavate andmete kogumise ja analüüsi kord ja mehhanismid.*

ELi turu äärmise killustatuse ja selle üsna spetsiifilise iseloomu tõttu kutsub komisjon samal ajal liikmesriike, erasektorit ja teadlaskonda **looma strateegilist partnerlust**, et tagada info- ja sidetehnoloogiaalast turvatööstust ning ELi toodete ja teenuste turusuundumusi käsitlevate andmete kättesaadavus.

*3.2.2. Selleks et parandada Euroopa suutlikkust võrgu turvalisusega seotud ohtudele reageerida, teeb komisjon ENISAle ülesandeks uurida **Euroopa teabevahenduse ja hoiatussüsteemi loomise võimalusi**, et lihtsustada tõhusate meetmete kasutuselevõttu elektroonilisi võrke ähvardavate olemasolevate ja tekkivate ohtude puhul. Niisuguse süsteemi eelduseks on **mitmekeelse ELi portaali** olemasolu, mis annaks eriotstarbelist teavet ohtude, riskide ja hoiatuste kohta.*

3.3. Aktiivne osalemine

Võrgu- ja teabeturbe edendamiseks turvavajadustest ja -riskidest teadlikkuse tõstmise eelduseks on kõikide sidusrühmade aktiivne osalemine.

*3.3.1. Selles suhtes kutsub komisjon **liikmesriike** üles:*

- aktiivselt osalema kavandatud võrgu- ja teabeturbe siseriikliku poliitika võrdlusuuringutes;
- edendama tihedas koostöös ENISAga teavituskampaaniaid tõhusate turvatehnoloogiate, -lahenduste ja -käitumise kasutuselevõtu hüvedest ja eelistest;
- hoogustama e-valitsuse teenuste käivitamist, et tutvustada ja edendada häid turvalahendusi, mida saaks seejärel muudes sektorites kasutusele võtta;
- ergutama kõrghariduse õppekavade osana võrgu- ja teabeturbe programmide arendamist.

***3.3.2.** Komisjon kutsub initsiatiivi haarama ka **erasektori** sidusrühmi, et:*

- määrata kindlaks tarkvaratootjate ja Interneti-teenuse osutajate kohustused seoses nende poolt tagatavate adekvaatsete ja auditeeritavate turvalisustasemetega. Selleks on vaja toetada standardprotsesse, mis vastaksid üldiselt aktsepteeritud turvastandarditele ja heade tavade eeskirjadele;
- edendada turvalisuse põhihoobadena mitmekesisust, avatust, koostalitlusvõimet, kasutatavust ja konkurentsi ning ergutada ID varguse ja muude eraelu puutumatust rikkuvate rünnakute ärahoidmiseks ja nende vastu võitlemiseks turvalisust tõstvate toodete, protsesside ja teenuste kasutamist;
- levitada võrguoperaatorite, teenuseosutajate ja VKEde seas turvalisuse ja äritegevuse järjepidevuse võrdlusalusena häid turvalahendusi;
- edendada ärisektoris, eriti VKEde jaoks, koolitusprogramme, et varustada teenistujad turvalahenduste tõhusaks rakendamiseks vajalike teadmiste ja oskustega;
- välja töötada Euroopa Liidu, eeskätt eraelu puutumatusega seotud vajadusi rahuldavaid ning mõistliku hinnaga turvalisuse sertifitseerimise skeeme toodete, protsesside ja teenuste jaoks;

- kaasata kindlustussektor asjakohasete riskijuhtimisvahendite ja -meetodite väljaarendamisse, et tulla toime info- ja sidetehnoloogiaga seotud riskidega, ning edendada organisatsioonides ja äriühingutes, eriti VKEdes, riskijuhtimise kultuuri.

4. JÄRELDUSED

Infosüsteemide ja võrkudega seotud turvaprobleemide tuvastamiseks ja lahendamiseks ELis on vaja kõigi sidusrühmade täispanust. Käesolevas teatises esitatud poliitika abil püütakse seda saavutada **paljusid sidusrühmi ühendava lähenemisviisi tugevdamise kaudu**. Kõnealune lähenemisviis põhineks vastastikustel huvidel, selles määrataks kindlaks vastavad rollid ja arendataks välja dünaamiline raamistik, et edendada tõhusat avaliku sektori poliitikat ja erasektori algatusi.

2007. aasta keskel annab komisjon nõukogule ja parlamendile aru käivitatud meetmete, esialgsete järelduste ja üksikalgatuste olukorra kohta, kaasa arvatud ENISA, liikmesriikide ja erasektori algatuste kohta. Vajaduse korral esitab komisjon ettepaneku võrgu- ja teabeturbe kohta.