I

(Rezoliucijos, rekomendacijos, gairės ir nuomonės)

REZOLIUCIJOS

TARYBA

TARYBOS REZOLIUCIJA

2007 m. kovo 22 d.

dėl saugios informacinės visuomenės strategijos Europoje

(2007/C 68/01)

EUROPOS SĄJUNGOS TARYBA

PRIĖMĖ ŠIĄ REZOLIUCIJĄ IR

PALANKIAI VERTINA

2006 m. gegužės 31 d. Komisijos komunikatą Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui — Saugios informacinės visuomenės strategija — „Dialogas, partnerystė ir teisių suteikimas“;

ATKREIPIA DĖMESĮ Į

2006 m. lapkričio 15 d. Komisijos komunikatą Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl kovos su nepageidaujamais elektroniniais laiškais, interneto naudotojų veiklos stebėjimo ir kenksminga programine įranga;

PRIMENA

1. 2002 m. sausio 28 d. Tarybos rezoliuciją dėl bendro požiūrio ir konkrečių veiksmų tinklų ir informacijos saugumo srityje ([1]);

2. 2003 m. vasario 18 d. Tarybos rezoliuciją dėl europinio požiūrio į tinklų ir informacijos saugumo kultūrą ([2]);

3. 2004 m. kovo 8–9 d. Tarybos išvadas dėl neužsakytų komercinių pranešimų tiesioginės rinkodaros tikslais arba nepageidaujamų elektroninių laiškų ir 2004 m. gruodžio 9–10 d. Tarybos išvadas dėl kovos su nepageidaujamais elektroniniais laiškais;

4. 2005 m. kovo mėn. Europos Vadovų Tarybos išvadas dėl Lisabonos strategijos atnaujinimo ir 2006 m. kovo mėn. Europos Vadovų Tarybos išvadas, kuriose Komisija ir valstybės narės raginamos aktyviai įgyvendinti naująją i2010 strategiją;

5. ES reguliavimo sistemą, skirtą elektroniniams ryšiams ([3]), ir pirmiausia nuostatoms, susijusioms su ryšių saugumu, privatumu ir konfidencialumu, kurios padėjo užtikrinti aukštą asmens duomenų ir privatumo apsaugos lygį bei viešųjų ryšių tinklų vientisumą ir saugumą,.

6. 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 460/2004, įsteigiantį Europos tinklų ir informacijos apsaugos agentūrą (ENISA) ([4]);

7. Tuniso darbotvarkę ir Pasaulio aukščiausio lygio susitikime informacinės visuomenės klausimais (WSIS) prisiimtą Tuniso įsipareigojimą, kuriame pabrėžiamas poreikis toliau kovoti su elektroniniais nusikaltimais ir nepageidaujamais elektroniniais laiškais, užtikrinant privatumo apsaugą ir išraiškos laisvę, bei bendradarbiaujant su visais suinteresuotais subjektais toliau skatinti, plėtoti ir įgyvendinti pasaulinę elektroninio saugumo kultūrą;

8. Pirmininkaujančios valstybės narės išvadas, padarytas metinėje Europos informacinės visuomenės konferencijoje 2006 m. rugsėjo 27–28 d.) „i2010 — universalios Europos informacinės visuomenės link“, kuri vyko Suomijos mieste Espoo;

([1]) OL C 43, 2002 2 16, p. 2.
([2]) OL C 48, 2003 2 28, p. 1.
([3]) Direktyvos 2002/58/EB (Direktyva dėl privatumo ir elektroninių ryšių), 2002/20/EB (Leidimų direktyva), 2002/22/EB (Universaliųjų paslaugų direktyva) (atitinkamai OL L 201, 2002 7 31, p. 37, OL L 108, 2002 4 24, p. 21 ir OL L 108, 2002 4 24, p. 51).
([4]) OL C 77, 2004 3 13, p. 1.

TODĖL PABRĖŽIA, KAD:

1. Mūsų visuomenė sparčiai artėja prie naujo plėtros etapo, universalios informacinės visuomenės link, kur vis daugiau kasdieninės piliečių veiklos yra pagrįsta informacinių ir ryšių technologijų (IRT) bei elektroninių ryšių tinklų naudojimu; tinklų ir informacijos saugumas turėtų būti laikomas viena iš svarbiausių šios plėtros ir jos sėkmės sąlygų;

2. Pasitikėjimas yra vienas iš esminių naujosios informacinės visuomenės sėkmės elementų; pasitikėjimas taip pat yra susijęs su galutinių vartotojų patirtimi ir su būtinybe gerbti jų privatumą; todėl tinklų ir informacijos saugumas neturėtų būti laikomas tik techniniu klausimu;

3. Tinklų ir informacijos saugumas yra viena iš esminių dalių kuriant Europos informacinę erdvę pagal i2010 iniciatyvą, tokiu būdu prisidedant prie atnaujintos Lisabonos strategijos sėkmės; IRT taip pat yra būtinas inovacijų, ekonomikos augimo ir užimtumo komponentas visoje ekonomikos sistemoje;

4. Jau kuriamos naujos technologijos, kurios sudarys mums sąlygas sukurti universalią informacinę visuomenę; atsiradus naujoviškoms technologijoms (pavyzdžiui, didelės spartos bevieliams tinklams, radijo dažnių identifikavimo (RFID) priemonėms, daviklių tinklams) ir inovacinėms turinio paslaugoms (pavyzdžiui, interneto protokolo televizijai (IPTV), interneto telefonijos protokolui (VoIP), mobiliajai televizijai ir kitoms mobiliosioms paslaugoms), būtina užtikrinti atitinkamą tinklų ir informacijos saugumo lygį nuo pat kūrimo etapo pradžios, kad būtų pasiekta faktinė komercinė vertė; greitas naujų daug žadančių inovacijų naudojimas yra labai svarbus informacinės visuomenės plėtrai ir Europos konkurencingumui; vyriausybiniai organai ir įmonės turėtų kuo greičiau pradėti naudoti tinkamas saugias, atsirandančias naujas technologijas ir paslaugas, kad būtų paspartintas platus jų naudojimas;

5. ES strategiškai svarbu, kad Europos pramonė būtų tinklų ir saugumo produktų bei paslaugų reikalaujantis vartotojas ir konkurencingas tiekėjas; įvairovė, atvirumas ir sąveikumas yra neatskiriami saugumo komponentai ir turėtų būti skatinami;

6. Tinklų ir informacijos saugumo žinios bei gebėjimai taip pat turi tapti neatskiriama kiekvieno asmens ir suinteresuoto visuomenės subjekto kasdienio gyvenimo dalimi; nacionaliniu ir ES lygiu vyko nemažai informuotumo didinimo kampanijų, tačiau vis dar liko darbo, kurį reikia atlikti, šioje srityje, ypač susijusio su galutiniais vartotojais bei mažosiomis ir vidutinėmis įmonėmis (MVĮ); ypatingą dėmesį reikėtų skirti tiems vartotojams, kurie turi specialių poreikių arba yra mažai informuoti tinklų ir informacijos saugumo klausimais; visi suinteresuoti subjektai turėtų žinoti, kad jie yra pasaulinės saugumo grandies dalis ir turėtų galėti atitinkamai veikti; į tinklų ir informacijos saugumo klausimus reikėtų atsižvelgti visoje švietimo ir mokymo srityje, susijusioje su IRT;

7. ENISA įsteigimas yra svarbus žingsnis ES dedant pastangas spręsti problemas, susijusias su tinklų ir informacijos saugumu; ENISA veiklos sritis, tikslai, užduotys ir veikimo laikotarpis yra apibrėžti Reglamente Nr. 460/2004;

8. Ištekliai, skirti moksliniams tyrimams ir plėtrai bei inovacijoms nacionaliniu ir ES lygiu yra vienas iš pagrindinių elementų didinant naujų sistemų, taikomųjų programų ir paslaugų informacijos ir tinklų saugumo lygį; reikėtų stiprinti pastangas ES lygiu su moksliniais tyrimais ir inovacijomis susijusiose srityse, pirmiausia įgyvendinant 7-ąją bendrąją programą (FP7) bei Bendrąją konkurencingumo ir inovacijų programą (CIP); pastangas taip pat reikėtų nukreipti į priemones, skirtas skleisti ir skatinti komercinį gautų rezultatų naudojimą, įskaitant jų naudingumo platesnei visuomenei įvertinimą; tai pagerins Europos tiekėjų galimybes teikti saugumo sprendimus, kurie atitiks konkrečius Europos rinkos poreikius;

9. Universali informacinė visuomenė teikia didelės naudos, tačiau taip pat kelia rimtų problemų, tokiu būdu sukuriant naujas galimos rizikos aplinkybes; grėsmė saugumui ir privatumui, be kita ko neteisėtai perimant ir naudojant duomenis, tampa vis rimtesnė, tikslingesnė ir turinti aiškų tikslą — ekonominę naudą; naudojantis novatoriškais būdais reikėtų parengti naujus atsakus į kylančias ir jau esamas grėsmes, kurie be kita ko turėtų apimti klausimus, atsirandančius dėl sistemų sudėtingumo, klaidų, atsitiktinumų ar neaiškių gairių; reikėtų skatinti ir toliau propaguoti nacionalinių kompiuterinių incidentų tyrimo tarnybų, kurių veikla būtų skirta įvairiems subjektams, sukūrimą ir plėtojimą, šių tarnybų tarpusavio bendradarbiavimą ir jų bendradarbiavimą su atitinkamais suinteresuotais subjektais;

10. Produktų, paslaugų ir valdymo sistemų standartizavimui ir sertifikavimui, visų pirma vykdomam jau egzistuojančių institucijų, turėtų būti skirtas ypatingas dėmesys ES tinklų ir informacijos saugumo politikoje, kadangi tai yra priemonė skleisti gerą praktiką ir profesionalumą ryšių ir informacijos saugumo srityje; laiku priėmus potencialiai besiformuojančius atvirus ir sąveikius standartus, tai būtų naudinga ypač naujoms atsirandančioms technologijoms, pavyzdžiui, RFID ir mobiliajai televizijai; reikėtų skatinti Europos standartizavimo organų veiklą šioje srityje;

11. Kadangi elektroniniai tinklai ir informacinės sistemos atlieka vis svarbesnį vaidmenį ypatingos svarbos infrastruktūros objektų veikloje, galimybė jais naudotis ir jų patikimumas tampa būtini administracijų, įmonių ir piliečių saugumui bei gyvenimo kokybei ir bendram visuomenės funkcionavimui;

12. Šiuo metu labiau nei bet kada anksčiau būtinas bendradarbiavimas ir praktinis požiūris; įvairūs suinteresuoti subjektai turėtų apsibrėžti ir pripažinti atitinkamus savo vaidmenis, atsakomybę bei teises.

TODĖL RAGINA VALSTYBES NARES:

1. Remti mokymo programas ir didinti informuotumą tinklų bei informacijos saugumo klausimais, pavyzdžiui, vykdant informacines kampanijas tinklų ir informacijos saugumo klausimais, skirtas visiems piliečiams/vartotojams ir ekonomikos sektoriams, ypač MVĮ ir galutiniams vartotojams, turintiems specialių poreikių arba mažai informuotiems; iki 2008 m. galėtų būti parinkta bendra data, kuri būtų skirta Europos informuotumo didinimo dienai (pavyzdžiui, „Informacijos ir tinklų saugumo diena“) ir kuri būtų kasmet neprivalomai minima kiekvienoje valstybėje narėje;

2. Didinti įnašą į su saugumu susijusius mokslinius tyrimus ir plėtrą bei gerinti galimybę naudoti ir skleisti gautus rezultatus; skatinti novatoriškų partneryščių kūrimą, kad išaugtų Europos IRT saugumo pramonės augimas ir išankstinis naujų tinklų ir informacijos saugumo technologijų bei paslaugų naudojimas, siekiant padidinti komercinę šių technologijų ir paslaugų vertę;

3. Skirti reikiamą dėmesį būtinybei užkirsti kelią naujoms ir esamoms grėsmėms elektroninių ryšių tinklams, įskaitant neteisėtą duomenų perėmimą ir naudojimą, bei su jomis kovoti, pripažinti susijusią riziką ir spręsti šį klausimą bei, atitinkamais atvejais bendradarbiaujant su ENISA, skatinti atitinkamų organizacijų bei agentūrų efektyvų keitimąsi informacija ir bendradarbiavimą nacionaliniu lygiu; įsipareigoti kovoti su nepageidaujamais elektroniniais laiškais, interneto naudotojų veiklos stebėjimo ir kenksminga programine įranga, visų pirma kompetetingoms institucijoms veiksmingiau bendradarbiaujant nacionaliniu ir tarptautiniu lygiu;

4. Stiprinti jų tarpusavio bendradarbiavimą pagal i2010 programą, siekiant nustatyti efektyvią ir novatorišką praktiką, skirtą didinti tinklų ir informacijos saugumą bei savanoriškai skleisti žinias apie šią praktiką visoje ES;

5. Skatinti nuolatinį nacionalinių kompiuterinių incidentų tyrimo tarnybų veiklos gerinimą;

6. Propaguoti tokią aplinką, kuri skatintų paslaugų teikėjus ir tinklų operatorius teikti tvirtas paslaugas savo vartotojams ir užtikrinti atsparumą bei tai, kad vartotojams būtų suteikta galimybė rinktis teikiant saugumo paslaugas bei priimant sprendimus; skatinti arba atitinkamais atvejais reikalauti, kad tinklų operatoriai ir paslaugų teikėjai užtikrintų atitinkamą tinklų ir informacijos saugumo lygį savo vartotojams;

7. Tęsti strategines diskusijas i2010 aukšto lygio grupėje, atsižvelgiant į vykstančią informacinės visuomenės plėtrą, ir užtikrinti reguliavimo, bendro reguliavimo, mokslinių tyrimų ir plėtros bei e. vyriausybės aspektų nuoseklumą su ryšiais ir švietimu;

8. Pagal i2010 e. vyriausybės veiksmų planą numatyti vientisų e. vyriausybės paslaugų plėtojimą, skatinti sąveikius autentifikavimo sprendimus ir imtis vykdyti visus atitinkamus pokyčius viešojo sektoriaus struktūroje; vyriausybės ir viešojo administravimo institucijos, skatindamos saugias e. vyriausybės paslaugas visiems piliečiams turėtų būti geriausios praktikos pavyzdys.

PALANKIAI VERTINA KOMISIJOS KETINIMĄ:

1. Toliau plėtoti išsamią ir dinamišką visos ES tinklų ir informacijos saugumo strategiją. Ypač svarbus yra Komisijos siūlomas visa apimantis požiūris;

2. Spręsti tinklų ir informacijos saugumo klausimus kaip vieną iš tikslų ES elektroninių ryšių reguliavimo sistemos peržiūroje;

3. Tęsti savo vaidmenį, siekiant didesnio informuotumo apie bendro politinio įsipareigojimo kovoti su nepageidaujamais elektroniniais laiškais, interneto naudotojų veiklos stebėjimo ir kenksminga programine įranga būtinybę; stiprinti dialogą ir bendradarbiavimą su trečiosiomis šalimis, pirmiausia su jomis sudarant susitarimus, apimančius kovą su nepageidaujamais elektroniniais laiškais, interneto naudotojų veiklos stebėjimo ir kenksminga programine įranga;

4. Intensyvinti ENISA dalyvavimą remiant šioje rezoliucijoje išdėstytą saugios informacinės visuomenės Europoje strategiją, atsižvelgiant į Reglamente (EB) Nr. 460/2004 nustatytus tikslus ir užduotis, ir glaudžiau bendradarbiaujant bei palaikant glaudesnius darbo santykius su valstybėmis narėmis ir suinteresuotais subjektais;

5. Įgyvendinant i2010 programą, bendradarbiaujant su valstybėmis narėmis ir visais suinteresuotais subjektais, ypač su statistikos ir valstybių narių informacijos saugumo ekspertais, parengti atitinkamus rodiklius Bendrijos apžvalgoms su saugumu ir pasitikėjimu susijusiais aspektais;

6. Surengiant daugelio suinteresuotų subjektų dialogą, skatinti valstybes nares nagrinėti ekonominius, verslo ir socialinius veiksnius, siekiant parengti politiką konkrečiai IRT sektoriui, kuria būtų skatinamas tinklų bei informacinių sistemų saugumas ir atsparumas, tokiu būdu galbūt prisidedant prie planuojamos Europos ypatingos svarbos infrastruktūros objektų apsaugos programos;

7. Savo veiklą derinant su valstybėmis narėmis, tęsti pastangas skatinti dialogą su atitinkamais tarptautiniais partneriais ir organizacijomis siekiant propaguoti pasaulinį bendradarbiavimą tinklų ir informacijos saugumo srityje, pirmiausia įgyvendinant Pasaulio aukščiausio lygio susitikime informacinės visuomenės klausimais apibrėžtas veiklos kryptis ir reguliariai teikiant pranešimus Tarybai.

IR RAGINA:

1. ENISA toliau dirbti glaudžiai bendradarbiaujant su valstybėmis narėmis, Komisija ir kitais suinteresuotais subjektais, siekiant įvykdyti tas užduotis bei tikslus, apibrėžtus Reglamente (EB) Nr. 460/2004, ir padėti Komisijai ir valstybėms narėms joms dedant pastangas vykdyti tinklų ir informacijos saugumo reikalavimus, tokiu būdu prisidedant prie šiame reglamente išdėstytos saugios informacinės visuomenės strategijos Europoje įgyvendinimo ir tolesnio plėtojimo;

2. Visus suinteresuotus subjektus didinti programinės įrangos saugumą ir tinklų bei informacinių sistemų saugumą bei atsparumą pagal šiame reglamente išdėstytą saugios informacinės visuomenės strategiją Europoje ir dalyvauti struktūriniuose daugelio suinteresuotų subjektų debatuose, kaip geriausiai pasinaudoti esamomis priemonėmis ir reguliavimo instrumentais;

3. Įmones laikytis teigiamo požiūrio į informacijos ir tinklų saugumą, siekiant sukurti pažangesnius ir saugesnius produktus bei paslaugas, investicijas į tokius produktus ir paslaugas laikant konkurenciniu privalumu;

4. Gamintojus ir paslaugų teikėjus atitinkamais atvejais saugumo, privatumo ir konfidencialumo reikalavimus įdiegti į savo produktų ir paslaugų projektus bei naudojamą tinklų infrastruktūrą, taikomąsias programas ir programinę įrangą, įgyvendinti ir stebėti su saugumu susijusius sprendimus;

5. Suinteresuotus subjektus bendradarbiauti ir kurti eksperimentinę aplinką naujų saugių technologijų ir paslaugų saugiam testavimui ir bandymui; naujas technologijas ir paslaugas pateikus rinkai, suinteresuotus subjektus laiku pradėti jas įdiegti;

6. Visus suinteresuotus subjektus toliau stengtis kovoti su nepageidaujamais elektroniniais laiškais ir kitokiu internetiniu piktnaudžiavimu ir aktyviai bendradarbiauti su kompetentingomis valdžios institucijomis nacionaliniu bei tarptautiniu lygiu;

7. Paslaugų teikėjus ir IRT pramonę daugiausia dėmesio skirti produktų, procesų ir paslaugų saugumo, privatumo ir galimybės juos naudoti didinimui, siekiant užtikrinti patikimumą, užkirsti kelią tapatybės vagystėms bei kitiems privatumą pažeidžiantiems veiksmams ir su jais kovoti;

8. Tinklų operatorius, paslaugų teikėjus ir privatųjį sektorių dalintis gera saugumo praktika bei ją taikyti ir skatinti rizikos analizę bei valdymą organizacijose ir įmonėse, remiant atitinkamas mokymo programas ir rengiant planus nenumatytiems atvejams, bei sudaryti galimybę savo klientams naudotis saugumo sprendimais kaip teikiamų paslaugų dalimi.