I

(Rezolūcijas, ieteikumi un atzinumi)

REZOLŪCIJAS

PADOME

PADOMES REZOLŪCIJA

(2009. gada 18. decembris)

par Eiropas sadarbības pieeju tīklu un informācijas drošībai

(2009/C 321/01)

EIROPAS SAVIENĪBAS PADOME,

I. ŅEMOT VĒRĀ:

1. Komisijas 2006. gada 31. maija paziņojumu par "Drošas informācijas sabiedrības stratēģiju", kurā ierosina "dialoga, partnerības un iespēju" procesu, iesaistot dalībvalstis un privātā sektora ieinteresētās puses;

2. Komisijas 2006. gada 12. decembra paziņojumu par "Eiropas programmu kritisko infrastruktūru aizsardzībai (EPKIA)", kura mērķis ir aizsargāt būtiski svarīgas infrastruktūras, kas atrodas ES, un izveidot ES sistēmu kritisko infrastruktūru aizsardzībai;

3. Padomes Direktīvu (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību;

4. Padomes 2007. gada 22. marta rezolūciju par drošas informācijas sabiedrības stratēģiju Eiropā;

5. Padomes 2007. gada 19.–20. aprīļa secinājumus par Eiropas programmu kritisko infrastruktūru aizsardzībai;

6. Komisijas 2009. gada 30. marta paziņojumu par informācijas kritiskās infrastruktūras aizsardzību (IKIA);

7. pašreiz notiekošas apspriedes (tostarp attiecīga sabiedriska apspriešana) par Eiropas Tīklu un informācijas drošības aģentūras (*ENISA*) nākotni un tās lomu IKIA;

8. prezidentvalsts secinājumus par IKIA, kurus pieņēma ministru konferencē Tallinā 2009. gada 27.–28. aprīlī;

9. Lisabonas mērķus attiecībā uz konkurētspēju un izaugsmi, kā arī pašlaik notiekošo darbu, lai pārskatītu Lisabonas stratēģiju;

10. drošības pasākumus, kas ierosināti elektronisku sakaru, tīklu un pakalpojumu reglamentējošo noteikumu pārskatā;

11. lai izveidotu efektīvu turpmāko politiku attiecībā uz tīklu un informācijas drošību, šajā rezolūcijā pausts uzskats, ka vēl nav pieņemti secinājumi par grozījumiem, kas būtu jāveic *ENISA* regulā. Tā kā Komisija pašreiz pārskata tīklu un informācijas drošības politikas turpmāko virzību, šīs pārskatīšanas rezultātam attiecībā uz *ENISA* regulas grozījumiem nevajadzētu būt atkarīgam no šīs rezolūcijas, pirms Komisija nav publicējusi pārskata rezultātus,

II. ŅEMOT VĒRĀ:

1. tā kā elektroniskā saziņa, infrastruktūra un pakalpojumi ir svarīgi kā pamats tautsaimnieciskai un sociālai darbībai, tīklu un informācijas drošība palīdz stiprināt sabiedrībā svarīgas vērtības un mērķus, piemēram, demokrātiju, privātumu, ekonomisko izaugsmi, ideju brīvu plūsmu un ekonomikas un politisko stabilitāti;

2. informācijas un komunikāciju tehnoloģiju sistēmas, infrastruktūra un pakalpojumi, tostarp internets, ir būtiski svarīgas sabiedrībai, un to darbības traucējumi vai iznīcināšana var radīt lielus bojājumus tautsaimniecībā, un uzsverot tādu pasākumu svarīgumu, ko veic, lai palielinātu aizsardzību un elastīgumu ar mērķi nodrošināt kritisko pakalpojumu nepārtrauktību;

3. drošības incidenti var graut lietotāju uzticības līmeni. Smagi tīklu un informācijas sistēmu darbības traucējumi varētu spēcīgi ietekmēt tautsaimniecību un sabiedrību; arī ikdienas problēmas un neērtības varētu graut sabiedrības uzticību tehnoloģijām, tīkliem un pakalpojumiem;

4. apdraudējumu spektrs izvēršas un palielinās – tas palielina vajadzību nodrošināt tiešos lietotājus, uzņēmumus un valdības ar elektronisku sakaru infrastruktūru, kas jau pamatos ir stabila un uzticama, un apzināt atbilstīgus stimulus, kas pakalpojumu sniedzējiem ļautu to izdarīt laicīgi;

5. tīklu un informācijas drošība jāpastiprina un jāiekļauj visās politikas jomās un sabiedrības grupās un jārisina problēma, kā nodrošināt pietiekamas prasmes gan ar valsts, gan Eiropas darbībām un kā palielināt informācijas un komunikācijas tehnoloģiju (IKT) lietotāju informētību;

6. iekšējā tirgus veidošanu varēs pabeigt, un tas varēs darboties, ja tīkla īpašnieki un pakalpojumu sniedzēji sadarbosies pāri robežām, jo iespējamie darbības traucējumi vienā dalībvalstī var ietekmēt arī citas dalībvalstis un ES kopumā;

7. saistībā ar jauniem lietojuma veidiem, tādiem kā, piemēram, datu izkaisītā apstrāde (*cloud computing*) un programmatūra kā pakalpojums, tīklu un informācijas drošība ir vēl jo svarīgāka;

8. tīklu un informācijas drošība ir visu pušu mērķis visās sabiedrības grupās, lai varētu uzticēties informācijas sistēmām, tādēļ ir vajadzīga starpnozaru un pārrobežu pieeja;

9. sabiedrībā arvien vairāk izmanto IKT – tīklu un informācijas drošība ir priekšnoteikums uzticamai, drošai un neapdraudētai sabiedrisko pakalpojumu (piemēram, e-valdība) sniegšanai;

10. *ENISA* ir iespējas palielināt svarīgo lomu, kas tai jau ir tīklu un informācijas drošības jomā,

III. UZSVER, KA:

1. Eiropas Savienībā ir vajadzīga augsta līmeņa tīklu un informācijas drošība, lai atbalstītu:

   a) pilsoņu brīvības un tiesības, tostarp tiesības uz privātumu;

   b) sabiedrību, kas efektīvi veic kvalitatīvu informācijas apstrādi;

   c) tirdzniecības un rūpniecības rentabilitāti un izaugsmi;

   d) pilsoņu un organizāciju uzticēšanos informācijas apstrādei un IKT sistēmām;

2. IKT nozare ir būtiski svarīga lielākajai daļai sabiedrības, padarot tīklu un informācijas drošību par visu iesaistīto pušu, tostarp, operatoru, pakalpojumu sniedzēju, datoraprīkojuma un programmatūras piegādātāju, tiešo lietotāju, valsts iestāžu un valstu valdību kopēju atbildību,

IV. ATZĪST:

1. nozīmi, kāda ir aktīvai un labi informētai Eiropas tīklu un informācijas drošības kopienai, kas palīdz uzlabot sadarbību starp dalībvalstīm un privāto sektoru;

2. priekšrocības, kādas attiecīgā gadījumā ir saskaņotai starptautisku drošības standartu izmantošanai visā Eiropas Savienībā tīklu un informācijas drošības vajadzībām;

3. vajadzību izveidot uz sadarbību balstītu Eiropas pieeju tīklu un informācijas drošībai starptautiskajā arēnā, jo tas ir pasaules mēroga uzdevums;

4. to, cik dalībvalstīm un ES iestādēm svarīga ir pieeja uzticamiem statistikas datiem par tīklu un informācijas drošību Eiropā;

5. vajadzību palielināt visu ieinteresēto pušu informētību par apdraudējumu pārvaldības instrumentiem;

6. to, cik svarīgi ir pastiprināt dalībvalstu centienus uzlabot informētību, apmainīties ar labāko praksi un izstrādāt pamatnostādnes dalībvalstīm;

7. to, cik svarīgi ir daudzu ieinteresēto pušu modeļi (piemēram, publiskā un privātā sektora partnerība (PPP)), kas paredzēti ilgtermiņam, un augšupvērsti modeļi, lai cīnītos pret atklātajiem apdraudējumiem, ja šāda pieeja sniedz papildu vērtību, palīdzot nodrošināt augsta līmeņa tīkla elastīgumu;

8. būtisko lomu, kāda ir pakalpojumu sniedzējiem, kas nodrošina sabiedrību ar stabilu un uzticamu elektronisku sakaru infrastruktūru;

9. to, cik noderīgas ir Eiropā veiktas mācības tīklu un informācijas drošības jomā, kas var sniegt vērtīgu pieredzi tīkla operatoriem un pakalpojumu sniedzējiem, kā arī valdībām;

10. to, ka valstu vai valdību datorapdraudējumu reakcijas komandas (*CERT*) vai cits reaģēšanas mehānisms, kas reaģē uz apdraudējumiem un ar ko mazina neaizsargātību, var palīdzēt izveidot augsta līmeņa elastīgumu un spēju izturēt un likvidēt tīklu un informācijas sistēmu darbības traucējumus;

11. ka ir svarīgi pētīt stratēģisko ietekmi, apdraudējumus un Eiropas Savienības iestāžu iespējas izveidot reaģēšanas grupas datorapdraudējumu gadījumos un apsvērt iespējamo lomu, kāda šajā jautājumā nākotnē būs *ENISA*;

12. līdzšinējo darbu, ko *ENISA* ir veikusi tīklu un informācijas drošības jomā, un nepieciešamību turpināt veidot *ENISA* par efektīvu struktūru, kas radītu skaidras priekšrocības Eiropas tīklu un informācijas drošības jomā,

V. UZSVER, KA:

1. pastiprināta un vienota Eiropas stratēģija tīklu un informācijas drošībai ar skaidri noteiktiem Eiropas Komisijas, dalībvalstu un *ENISA* pienākumiem ir ārkārtīgi svarīga, lai atrisinātu pašreizējās un turpmāk iespējamās problēmas;

2. pēc atbilstīgām konsultācijām un analīzes likumdošanas procesā būtu jāpievēršas *ENISA* modernizēšanai un nostiprināšanai, piešķirot pilnvaras, kas nodrošina elastību un dalībvalstu un Komisijas pārraudzību, kā arī piešķirot efektīvu lomu privātā sektora ieinteresēto pušu pārstāvjiem. Tās pilnvarās būtu jāņem vērā elektroniskās saziņas, tīklu un pakalpojumu tiesiskā bāze, un tām būtu jāatbilst Lisabonas darba kārtības centieniem un būtu jāietver ar pētniecību, novatorismu, konkurētspēju, ekonomikas izaugsmi un uzticamības nodrošināšanu saistīti mērķi;

3. *ENISA* varētu atbalstīt Komisijas un dalībvalstu politikas veidošanas un īstenošanas pienākumus, it īpaši tuvinot tehnoloģiju un politiku, un būtu jāstrādā cieši kopā ar dalībvalstīm un citām ieinteresētajām pusēm, lai nodrošinātu tās darbību pienācīgu saskaņotību ar ES prioritātēm;

4. saskaņā ar pārskatītajām pilnvarām *ENISA* būtu jākļūst par Eiropas Savienības kompetences centru ar ES saistīto tīklu un informācijas drošības jautājumos. Tādēļ Eiropas iestādēm būtu jālūdz *ENISA* viedoklis un tas rūpīgi jāņem vērā, izstrādājot un īstenojot politikas, kas varētu ietekmēt šo jomu;

5. *ENISA* vajadzētu būt iespējai pēc lūguma palīdzēt dalībvalstīm uzlabot to tīklu un informācijas drošību, ka arī to spēju novērst drošības incidentus,

VI. AICINA DALĪBVALSTIS:

1. turpināt darbu, lai ar informācijas kampaņām palielinātu tiešo lietotāju uzticību IKT;

2. organizēt valsts mācības un/vai piedalīties regulārās Eiropas mācībās tīklu un informācijas drošības jomā, ņemot vērā izvērstu plānošanu saistībā ar nozares sarežģītību un privātā sektora iesaistīšanos. Šajā sakarā *ENISA* varētu pēc lūguma palīdzēt dalībvalstīm. Mācību darbības jomai un ģeogrāfiskajam tvērumam pakāpeniski būtu dabiski jāattīstās un būtu jābalstās uz konstatētiem apdraudējumiem;

3. izveidot datorapdraudējumu reakcijas komandas (*CERT*) visās dalībvalstīs, kuras šādas komandas vēl nav izveidojušas, un pastiprināt Eiropas mēroga sadarbību starp valstu datorapdraudējumu reakcijas komandām; šajā sakarā *ENISA* varētu palīdzēt dalībvalstīm;

4. pastiprināt centienus saistībā ar izglītības, mācību un pētniecības programmām tīklu un informācijas drošības jomā, lai nodrošinātu to, ka Eiropas Savienībai ir pieejamas vajadzīgās tehniskās prasmes un šīs nozares speciālisti, kā arī uzlabot viņu profesionalitāti;

5. kopīgi reaģēt, kad notiek pārrobežu pārkāpums, un palielināt valstu spēju rīkoties atbilstīgi – lai to panāktu, jāstiprina dialogs starp iesaistītajiem lēmumu pieņēmējiem, it īpaši attiecībā uz konfidencialitāti,

VII. AICINA KOMISIJU:

1. attiecīgi atbalstīt dalībvalstis šīs rezolūcijas īstenošanā;

2. regulāri informēt Eiropas Parlamentu un Padomi par ES līmenī pieņemtām ierosmēm attiecībā uz tīklu un informācijas drošību;

3. sadarbībā ar *ENISA* sākt informācijas kampaņu starp Eiropas publiskā un privātā sektora dalībniekiem par atbilstīgas apdraudējuma pārvaldības lielo nozīmi attiecībā uz tīklu un informācijas drošību;

4. sadarbībā ar dalībvalstīm turpināt meklēt stimulus, lai elektronisku sakaru infrastruktūru veidotāji sagatavotu jau pamatos stabilas un uzticamas infrastruktūras tiešajiem lietotājiem, uzņēmumiem un valdībām;

5. sadarbībā ar dalībvalstīm izstrādāt metodes, kas ES līmenī ļaus veikt salīdzinošu izvērtējumu attiecībā uz incidentu sociālekonomisko ietekmi un preventīvu pasākumu efektivitāti;

6. veicināt vairāku ieinteresēto pušu modeļu izveidi un uzlabot to – tiem ir jābūt ar skaidru papildu vērtību, kas dod labumu tiešajiem lietotājiem un nozarei;

7. nākt klajā ar tīklu un informācijas drošības vienotu stratēģiju, [1] tostarp ar priekšlikumiem par paplašinātām un elastīgām *ENISA* pilnvarām, kā arī pastiprinātu dalībvalstu un Komisijas pārraudzību;

8. sadarbībā ar dalībvalstīm analizēt datorapdraudējumu reakcijas komandu darbu, lai noteiktu jomas, kurās būtu vajadzīga turpmāka sadarbība;

9. turpināt izpēti, kā panākt kopēju vai savstarpēji saistītu pieeju, ES iestādēm iegādājoties drošas IKT sistēmas un pakalpojumus,

VIII. AICINA *ENISA:*

1. arī turpmāk aktīvi atbalstīt dalībvalstis, Eiropas Komisiju un citas attiecīgas ieinteresētās puses Eiropas tīklu un informācijas drošības politikas un IKIA rīcības plāna īstenošanā;

2. sadarbībā ar dalībvalstīm, Komisiju un statistikas iestādēm izstrādāt tādu statistikas datu sistēmu, kas atspoguļotu tīklu un informācijas drošības stāvokli Eiropā,

IX. AICINA IEINTERESĒTĀS PUSES:

1. pastiprināt tīklu un informācijas drošības uzlabošanas centienus, it īpaši attiecībā uz to, lai piedāvātu drošus, uzticamus un vienkārši lietojamus produktus un pakalpojumus;

2. atbilstīgi informē lietotājus par drošības apdraudējumiem, kas saistīti ar produktiem un pakalpojumiem, un par to, kā viņi var sevi aizsargāt;

3. veikt visus atbilstīgos tehniskos un organizatoriskos pasākumus, lai nodrošinātu elektronisku sakaru tīklu un pakalpojumu nepārtrauktību, integritāti un konfidencialitāti;

4. turpināt darbu pie tīklu un informācijas drošības standartizēšanas, lai censtos rast saskaņotus un savstarpēji izmantojamus risinājumus;

5. kopā ar dalībvalstīm piedalīties pasākumos, lai atbilstīgi reaģētu ārkārtas situācijās.

---

[1] Komisija ierosina pievienot šeit vārdu "iespējams".