Eiropas Savienības
Padome

Briselē, 2016. gada 21. aprīlī
(OR. en)

5581/16
ADD 1

Starpiestāžu lieta:
2013/0027 (COD)

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84

PADOMES PASKAIDROJUMA RAKSTA PROJEKTS

Temats:	Padomes nostāja pirmajā lasījumā, lai pieņemtu EIROPAS PARLAMENTA UN PADOMES DIREKTĪVU par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā – Padomes paskaidrojuma raksta projekts

I. IEVADS

1. Komisija 2013. gada 12. februārī iesniedza priekšlikumu Eiropas Parlamenta un Padomes Direktīvai par *pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā* (turpmāk – "direktīva"); juridiskais pamats – LESD 114. pants.

2. Eiropas Ekonomikas un sociālo lietu komiteja par savu atzinumu balsoja 2013. gada 22. maijā, un Reģionu komiteja par savu atzinumu – 2013. gada 3. un 4. jūlijā.

3. Eiropas Parlaments par normatīvo rezolūciju pirmajā lasījumā balsoja 2014. gada 13. martā [1], pieņemot 138 grozījumus.

4. Padome un Eiropas Parlaments sāka sarunas, lai 2014. gada oktobrī panāktu agrīnu otrā lasījuma vienošanos. Sarunas veiksmīgi noslēdzās 2015. gada 7. decembrī, Eiropas Parlamentam un Padomei panākot provizorisku vienošanos par kompromisa tekstu.

5. Pastāvīgo pārstāvju komiteja 2015. gada 18. decembrī apstiprināja direktīvas kompromisa tekstu, par ko abas minētās iestādes bija vienojušās.

6. Eiropas Parlamenta Iekšējā tirgus un patērētāju aizsardzības komitejas (*IMCO*) priekšsēdētāja 2016. gada 28. janvārī nosūtīja vēstuli Pastāvīgo pārstāvju komitejas priekšsēdētājam, kurā paziņoja, ka, ja Padome oficiāli nosūtīs Eiropas Parlamentam savu nostāju, par kuru panākta vienošanās un kuru būs pārbaudījuši juristi lingvisti, viņa ieteiks plenārsēdei Padomes nostāju pieņemt bez grozījumiem Parlamenta otrajā lasījumā.

7. Padome 2016. gada 29. februārī apstiprināja savu politisko vienošanos par direktīvas kompromisa tekstu.

---

[1] Eiropas Parlamenta 2014. gada 13. marta normatīvā rezolūcija par priekšlikumu Eiropas Parlamenta un Padomes Direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā.

II. MĒRĶIS

8. No sarunu rezultātiem izriet, ka direktīvā ir noteikti pasākumi ar mērķi panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību Eiropas Savienībā, lai uzlabotu iekšējā tirgus darbību.

III. PADOMES PIRMĀ LASĪJUMA NOSTĀJAS ANALĪZE

A. Vispārīgi

9. Pēc balsojuma plenārsēdē Eiropas Parlaments un Padome risināja sarunas ar mērķi panākt vienošanos otrajā lasījumā, pamatojoties uz Padomes nostāju pirmajā lasījumā, kuru Parlaments pēc būtības varētu apstiprināt. Padomes nostāja pirmajā lasījumā pilnībā atspoguļo abu likumdevēju panākto kompromisu.

B. Būtiskākās problēmas

10. Turpmāk ir izklāstīti galvenie elementi kompromisā, kas panākts ar Eiropas Parlamentu.

a. *Valstu spējas*

11. Saskaņā ar kompromisu dalībvalstīm ir konkrēti pienākumi attiecībā uz savām valsts spējām kiberdrošības jomā. Pirmkārt, dalībvalstīm ir jāpieņem valsts stratēģija, kurā noteikti stratēģiskie mērķi un atbilstīgi politikas un reglamentējoši pasākumi, lai panāktu un saglabātu tīklu un informācijas sistēmu drošību augstā līmenī.

12. Otrkārt, dalībvalstis izraugās vienu vai vairākas par tīklu un informācijas sistēmu drošību atbildīgas valsts kompetentās iestādes, kas pārrauga direktīvas piemērošanu valsts līmenī.

13. Treškārt, dalībvalstīm ir arī jāizraugās valsts vienotais kontaktpunkts tīklu un informācijas sistēmu drošības jautājumos, kurš veiks koordinācijas funkciju, lai nodrošinātu dalībvalstu iestāžu pārrobežu sadarbību un sadarbību ar attiecīgajām iestādēm citās dalībvalstīs un ar sadarbības grupu un datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu. Vienotais kontaktpunkts sadarbības grupai arī iesniegs ikgadēju ziņojumu par saņemtajiem paziņojumiem.

14. Visbeidzot, dalībvalstis izraugās vienu vai vairākas datordrošības incidentu reaģēšanas vienības (*CSIRT*), kas atbild par incidentu un risku risināšanu. Kompromisa tekstā, direktīvas I pielikumā, ir izklāstīti *CSIRT* pienākumi un uzdevumi.

b. *Sadarbība*

15. Ar kompromisa tekstu tiek izveidota sadarbības grupa, lai atbalstītu un atvieglotu stratēģisku sadarbību starp dalībvalstīm, lai vairotu uzticību un paļāvību un lai Savienībā panāktu vienādi augsta līmeņa tīklu un informācijas sistēmu drošību. Grupu veidos dalībvalstu, Komisijas un Eiropas Savienības Tīklu un informācijas drošības aģentūras (*ENISA*) pārstāvji, un tai būs konkrēti uzdevumi, kas uzskaitīti minētajā tekstā, piemēram, apmainīties ar paraugpraksi un informāciju par vairākiem jautājumiem vai apspriest dalībvalstu spējas un sagatavotību.

16. Turklāt ar kompromisa tekstu izveido valstu *CSIRT* tīklu, lai palīdzētu vairot paļāvību un uzticēšanos starp dalībvalstīm un lai sekmētu ātru un efektīvu operatīvo sadarbību. Tīklu veidos dalībvalstu *CSIRT* un ES Datorapdraudējumu reaģēšanas vienības (*CERT-EU*) pārstāvji, un Komisija tīklā piedalīsies kā novērotāja. *ENISA* nodrošinās sekretariātu un aktīvi atbalstīs sadarbību starp *CSIRT*. Kompromisa tekstā ir uzskaitīti uzdevumi, kas tīklam jāveic, piemēram, jāapmainās ar informāciju par *CSIRT* pakalpojumiem, darbībām un sadarbības spējām, jāatbalsta dalībvalstis pārrobežu incidentu risināšanā vai konkrētos apstākļos jāapmainās ar informāciju par incidentiem un ar tiem saistītiem riskiem un jāapspriež tā.

c. *Drošības un paziņošanas prasības*

17. Direktīvā ir noteiktas konkrētas prasības attiecībā uz divām tirgus dalībnieku grupām – pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem.

18. Direktīvas II pielikumā ir uzskaitītas vairākas sabiedrībai un ekonomikai svarīgas nozares, proti, enerģētika, transports, banku nozare, finanšu tirgus infrastruktūras, veselības nozare, dzeramā ūdens piegāde un izplatīšana un digitālā infrastruktūra. Šajās nozarēs dalībvalstis, pamatojoties uz direktīvā izklāstītiem skaidriem kritērijiem, identificēs pamatpakalpojumu sniedzējus.

19. Direktīvas III pielikumā ir uzskaitīti trīs to digitālo pakalpojumu veidi, kuru sniedzējiem būs jāievēro direktīvā noteiktās prasības; tās ir tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas un mākoņdatošanas pakalpojumi. Visiem digitālo pakalpojumu sniedzējiem, kuri sniedz uzskaitītos pakalpojumus, būs jāievēro direktīvā noteiktās prasības, izņemot mikrouzņēmumus un mazos uzņēmumus.

20. Abām tirgus dalībnieku grupām būs jāveic organizatoriski un tehniski pasākumi, ar ko pārvalda tīklu un informācijas sistēmu drošībai radītos riskus un novērš un līdz minimumam samazina tādu incidentu sekas, kuri ietekmē minēto sistēmu drošību. Turklāt par incidentiem, kas attiecīgos pakalpojumus ietekmē konkrētā līmenī, būs jāziņo valsts kompetentajām iestādēm vai *CSIRT*. Direktīvā ir paredzēti kritēriji, pēc kuriem nosaka šādu incidentu ietekmes līmeni.

21. Direktīvā ir paredzēta diferencēta pieeja attiecībā uz abām dalībnieku kategorijām. Drošības un paziņošanas prasības digitālo pakalpojumu sniedzējiem ir vieglākas nekā pamatpakalpojumu sniedzējiem, kas atbilst tam, cik lielu apdraudējumu šo sniedzēju pakalpojumu traucējumi var radīt sabiedrībai un ekonomikai. Turklāt, ņemot vērā to, ka digitālo pakalpojumu sniedzēji bieži vien darbojas daudzās dalībvalstīs, un lai nodrošinātu augstu saskaņotības līmeni, direktīva liedz dalībvalstīm piemērot minētajiem pakalpojumu sniedzējiem jebkādas papildu drošības un paziņošanas prasības.

22. Kompromisa tekstā ir arī paredzēts, ka vienības, kas nav identificētas kā pamatpakalpojumu sniedzēji un kas nav digitālo pakalpojumu sniedzēji, var brīvprātīgi ziņot par konkrētiem incidentiem.

d. *Transponēšana*

23. Dalībvalstīm direktīva būs jātransponē 21 mēneša laikā pēc tās stāšanās spēkā, un tām būs vēl seši mēneši laika, lai identificētu savus pamatpakalpojumu sniedzējus.

IV. SECINĀJUMS

24. Padomes nostāja pilnībā atspoguļo kompromisu, kas panākts Eiropas Parlamenta un Padomes sarunās un kam Komisija ir piekritusi. Kompromiss ir apstiprināts *IMCO* komitejas priekšsēdētājas 2016. gada 28. janvāra vēstulē Pastāvīgo pārstāvju komitejas priekšsēdētājam.