Eiropas Savienības
Padome

Briselē, 2019. gada 20. martā
(OR. en)

7737/19

CYBER 101	**RELEX 287**
COPEN 118	**TELECOM 141**
COPS 92	**DAPIX 109**
COSI 52	**CATS 43**
DATAPROTECT 98	**CSC 111**
IND 102	**CSCI 47**
JAI 313	**IA 106**
JAIEX 44	**EJUSTICE 44**
POLMIL 31	

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Datums:	2019. gada 19. marts
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	6866/19
Temats:	Padomes secinājumi par kiberdrošības spēju un spēju veidošanu ES

Pielikumā pievienoti Padomes secinājumi par kiberdrošības spēju un spēju veidošanu ES, kurus Vispārējo lietu padome pieņēma 2019. gada 19. marta sanāksmē.

PIELIKUMS

Padomes secinājumi par kiberdrošības spēju un spēju veidošanu ES

Eiropas Savienības Padome,

1. ATGĀDINOT savus secinājumus "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" [1];

2. ATGĀDINOT savus secinājumus par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm [2];

3. ATGĀDINOT savus secinājumus par ārējo kiberspēju veidošanu [3];

4. ATKĀRTOTI APSTIPRINOT, ka tīklu un informācijas sistēmu augsta līmeņa drošību var garantēt, pastiprinot dalībvalstu un ES iestāžu, aģentūru un struktūru kiberdrošības spēju un spējas, un ar turpmāku to kibernoturības nostiprināšanu;

5. ATZINĪGI VĒRTĒ progresu, kuru dalībvalstis sasniegušas datordrošības incidentu reaģēšanas vienību (*CSIRT*) stiprināšanā;

6. PAUŽOT GANDARĪJUMU par to, ka dalībvalstis ar aktīvu Komisijas un *ENISA* atbalstu ir izveidojušas *CSIRT* tīklu, kā arī par pastiprināto stratēģiskā līmeņa sadarbību TID sadarbības grupā, kuras sastāvā ir dalībvalstis, Komisija un *ENISA*;

---

1 Dok. 14435/17 (Padomes secinājumi par kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" (2017. gada 20. novembris)).

2 Dok. 10086/18 (Secinājumi par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (2018. gada 26. jūnijs)).

3 Dok. 10496/18 (Padomes secinājumi par nostādnēm ES ārējo kiberspēju veidošanai (2018. gada 26. jūnijs)).

7. UZSVEROT TID sadarbības grupas būtisko lomu to norādījumu sniegšanā, kas vajadzīgi, lai pēc iespējas salāgotu pieeju TID direktīvas [4] transponēšanā visā ES, kā arī attiecīgo kiberdrošības jautājumu risināšanā;

8. ATZĪSTOT pašreizējo atbalstu, kuru Komisija sniedz dalībvalstīm *CSIRT* spēju veidošanai ar Eiropas infrastruktūras savienošanas instrumenta starpniecību;

9. ATZĪSTOT atbalstu, kuru ar Iekšējā drošības fonda un *CEPOL* starpniecību sniedz tiesībaizsardzības iestādēm spēju veidošanai kibernoziedzības apkarošanā;

10. ATZINĪGI VĒRTĒJOT ES kiberaizsardzības politikas satvara atjaunināšanu nolūkā vēl vairāk atbalstīt dalībvalstu kiberaizsardzības spēju pilnveidošanu;

11. PAUŽOT GANDARĪJUMU par progresu, kuru dalībvalstis sasniegušas TID direktīvas īstenošanā;

12. ATZĪMĒJOT, ka kiberdrošība ir sarežģīta, neatkarīga un pastāvīgi mainīga joma, kā dēļ politiskais un tiesiskais regulējums ir jāpielāgo jaunām tehnoloģiskām tendencēm un jaunām tehnoloģijām, piemēram, mākslīgajam intelektam, blokķēdei un kvantu skaitļošanai;

---

[4] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gads 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016.).

13. UZSVEROT, ka kiberdrošības risku mazināšanā būtiska nozīme ir ar kiberdrošību saistītām mācību un izglītības programmām, kā arī informācijai un izpratnes veidošanai par drošības apdraudējumu galalietotājiem;

14. PASVĪTROJOT, ka kiberjomas mācības ir efektīvs līdzeklis, kā izvērtēt un vēl vairāk uzlabot ES un tās dalībvalstu gatavības līmeni reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm;

15. ATKĀRTOTI ATZĪMĒJOT, ka kibertelpai nav robežu, kas nozīmē, ka pārrobežu un starpnozaru perspektīvas un sadarbība ir nelokāms kiberspēju veidošanas darbību un iniciatīvu princips;

16. UZSVEROT, cik svarīga ir publiskā sektora, privātā sektora un akadēmisko aprindu sadarbība, jo īpaši ar kopdarbības projektu starpniecību;

17. UZSVEROT civilmilitāras sadarbības nozīmi, strādājot pie kopīgu mērķu sasniegšanas kiberjomā, lai nodrošinātu konsekventu un efektīvu atbildi uz kiberdraudiem;

18. ATZĪMĒ progresu, kuru grupa dalībvalstu ir sasniegusi kiberdrošības ātrās reaģēšanas vienību izveidē, lai ar savstarpēju palīdzību pastiprinātu brīvprātīgu sadarbību kiberjomā;

19. ATZINĪGI VĒRTĒ Padomē notiekošās diskusijas par Komisijas priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu;

20. VEICINA aktīvu dalību TID sadarbības grupā notiekošajā darbā, jo īpaši attiecībā uz kiberspēju veidošanu;

21. VEICINA TID sadarbības grupā notiekošo darbu attiecībā uz koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm;

22. AICINA dalībvalstis balstīties uz savām nacionālajām kiberdrošības stratēģijām un kiberdrošību integrēt, ņemot vērā nozarei specifiskās prasības;

23. AICINA dalībvalstis pastāvīgi pārraudzīt, novērtēt/izvērtēt to pasākumu ietekmi, kuri pieņemti, lai stiprinātu kibernoturību un sekmētu kiberspēju un spējas valsts līmenī;

24. AICINA dalībvalstis kiberdrošību un digitālo pratību integrēt mācību programmās visos izglītības (sākumskolas, vidusskolas, terciārās izglītības, mūžizglītības) līmeņos, attiecīgā gadījumā pamatojoties uz izveidotajiem un nākotnes amatu profiliem;

25. AICINA dalībvalstis izvērst izpratnes par kiberdrošību veidošanas kampaņas un kiberhigiēnas iniciatīvas, kas paredzētas visplašākajai sabiedrībai un galalietotājiem, orientējoties uz publiskā sektora darbiniekiem;

26. MUDINA dalībvalstis rīkot kiberdrošības mācības valsts līmenī, kā arī rīkot kiberdrošības mācības ES līmenī un/vai šādās mācībās piedalīties, lai testētu stratēģiskos un tehnoloģiskos aspektus un tajos apmācītu, kā arī lai efektīvi un praktiskā līmenī veidotu vajadzīgās prasmes;

27. AICINA dalībvalstis pilnveidot savu *CSIRT* kiberdrošības tehniskās un operatīvās spējas incidentu novēršanas, to ierobežošanas un reaģēšanas uz tiem jomā;

28. AICINA Komisiju un *ENISA* turpināt sniegt savu atbalstu dalībvalstu *CSIRT* tīkla spējas un spēju veidošanai, lai sekmīgāk sadarbotos, dalītos informācijā par incidentiem un efektīvi reaģētu uz plašapmēra pārrobežu incidentiem;

29. AICINA dalībvalstis turpināt palīdzēt tiesībaizsardzības iestādēm specifisku spēju veidošanā sadarbībā ar kompetentajām Eiropas iestādēm, lai efektīvi apkarotu kibernoziedzību ES līmenī;

30. AICINA dalībvalstis palielināt ieguldījumus kiberspēju veidošanā;

31. AICINA Komisiju un *ENISA* īstenot izpratnes par kiberdrošību veidošanas programmas un mācības, kas orientētas uz ES iestādēm, aģentūrām un struktūrām;

32. AICINA ES un tās dalībvalstis brīvprātīgi dalīties informācijā un paraugpraksē, lai dotu ieguldījumu galveno kiberspēju veidošanas vajadzību apzināšanā un darbā pie tām valsts un ES līmenī;

33. AICINA ES un tās dalībvalstis atbalstīt pētniecību kiberdrošības jomā un popularizēt kiberdrošību kā problēmjautājumu citās pētījumu jomās, tādējādi vienā veselumā vienkopus apvienojot dažādas ar kiberdrošību saistītas pētniecības un izstrādes nozares, un sekmēt izcilību kiberdrošības pētniecībā;

34. AICINA ES un tās dalībvalstis attīstīt kiberdrošības jomas pētniecību, kas atspoguļo sabiedrības vajadzības un kas pētniecības rezultātus integrē tirgū;

35. AICINA ES un tās dalībvalstis attiecīgā gadījumā kiberdrošību ņemt vērā IKT jomas iepirkumos.