Rådet for
Den Europæiske Union

Bruxelles, den 20. marts 2019
(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	

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	19. marts 2019
til:	delegationerne
Tidl. dok. nr.:	6866/19
Vedr.:	Rådets konklusioner om opbygning af cybersikkerhedskapacitet i EU

Vedlagt følger til delegationerne Rådets konklusioner om opbygning af cybersikkerhedskapacitet i EU, der blev vedtaget af Rådet (almindelige anliggender) den 19. marts 2019.

BILAG

Rådets konklusioner om opbygning af cybersikkerhedskapacitet i EU

Rådet for Den Europæiske Union,

1. SOM MINDER OM sine konklusioner om modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU[1];

2. SOM MINDER OM sine konklusioner om en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og - kriser[2];

3. SOM MINDER OM sine konklusioner om opbygning af ekstern cyberkapacitet[3];

4. SOM GENTAGER, at et højt sikkerhedsniveau for net- og informationssystemer kan tilvejebringes ved at forstærke medlemsstaternes og EU-institutionernes, -agenturernes og -organernes cybersikkerhedskapacitet og efterfølgende styrke deres cybermodstandskraft;

5. SOM SER MED TILFREDSHED PÅ de fremskridt, som medlemsstaterne har gjort i forbindelse med styrkelse af enhederne, der håndterer IT-sikkerhedshændelser (CSIRT'erne);

6. SOM BIFALDER medlemsstaternes oprettelse af CSIRT-netværket med aktiv støtte fra Kommissionen og ENISA tillige med det intensiverede samarbejde på strategisk plan gennem NIS-samarbejdsgruppen bestående af medlemsstaterne, Kommissionen og ENISA;

---

1 14435/17 (Rådets konklusioner om den fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU af 20. november 2017).

2 10086/18 (Rådets konklusioner om en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og - kriser af 26. juni 2018).

3 10496/18 (Rådets konklusioner om EU's retningslinjer for opbygning af ekstern cyberkapacitet af 26. juni 2018).

7. SOM UNDERSTREGER NIS-samarbejdsgruppens centrale rolle med hensyn til at yde den nødvendige rådgivning med henblik på i så høj grad som muligt at tilpasse tilgangen i forbindelse med gennemførelsen af NIS-direktivet[4] i hele EU og tackle de relevante cybersikkerhedsspørgsmål;

8. SOM ANERKENDER den eksisterende støtte fra Kommissionen til medlemsstaterne med henblik på kapacitetsopbygning af CSIRT'er gennem Connecting Europe-faciliteten;

9. SOM ANERKENDER støtten til de retshåndhævende myndigheder med henblik på kapacitetsopbygning i forbindelse med bekæmpelse af cyberkriminalitet gennem Fonden for Intern Sikkerhed og Cepol;

10. SOM SER MED TILFREDSHED PÅ ajourføringen af rammen for EU's cyberforsvarspolitik for yderligere at støtte udviklingen af EU-medlemsstaternes cyberforsvarskapaciteter;

11. SOM BIFALDER de fremskridt, der er gjort med hensyn til medlemsstaternes gennemførelse af NIS-direktivet;

12. SOM NOTERER SIG, at cybersikkerhed er et komplekst, indbyrdes afhængigt og konstant foranderligt område, der kræver tilpasning af de politiske og juridiske rammer til nye teknologiske tendenser og fremspirende teknologier, såsom kunstig intelligens, blockchain og kvantedatabehandling;

---

[4] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016).

13. SOM FREMHÆVER, at cybersikkerhedsrelaterede uddannelsesprogrammer samt oplysninger til og bevidstgørelse af slutbrugerne om sikkerhedstrusler er afgørende for at mindske cybersikkerhedsrisici;

14. SOM UNDERSTREGER, at cyberøvelser er effektive redskaber til vurdering og yderligere forbedring af EU's og dets medlemsstaters beredskab med hensyn til at imødegå væsentlige cybersikkerhedshændelser og -kriser;

15. SOM GENTAGER, at cyberspace ikke har nogen grænser, hvilket betyder, at perspektiver og samarbejde på tværs af grænser og sektorer er et uundgåeligt princip i forbindelse med cyberkapacitetsopbyggende aktiviteter og initiativer;

16. SOM UNDERSTREGER betydningen af samarbejde mellem den offentlige sektor, den private sektor og den akademiske verden, navnlig gennem samarbejdsprojekter;

17. SOM LÆGGER VÆGT PÅ vigtigheden af civil-militært samarbejde, der forfølger fælles mål på cyberområdet for at sikre en konsekvent og effektiv reaktion på cybertrusler;

18. SOM NOTERER SIG de fremskridt, der er gjort af en gruppe af medlemsstater med henblik på at udvikle cyberberedskabshold for at uddybe det frivillige samarbejde på cyberområdet gennem gensidig bistand;

19. SER MED TILFREDSHED PÅ de igangværende drøftelser i Rådet om Kommissionens forslag til Europa-Parlamentet og Rådets forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre;

20. OPFORDRER TIL aktiv deltagelse i det igangværende arbejde i NIS-samarbejdsgruppen, navnlig hvad angår cyberkapacitetsopbygning;

21. TILSKYNDER det igangværende arbejde i NIS-samarbejdsgruppen vedrørende en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og - kriser;

22. OPFORDRER medlemsstaterne TIL at tage udgangspunkt i deres nationale cybersikkerhedsstrategier og integrere cybersikkerhed under hensyntagen til sektorspecifikke krav;

23. OPFORDRER medlemsstaterne TIL at gennemføre fortsat overvågning og evaluering/vurdering af indvirkningen af foranstaltninger, der træffes for at styrke cybermodstandskraften og øge cyberkapaciteterne på nationalt plan;

24. OPFORDRER medlemsstaterne TIL at integrere cybersikkerhed og digital kunnen i studieplanerne på alle uddannelsesniveauer (primært, sekundært, tertiært og livslang læring) i relevant omfang baseret på fastlagte og fremtidige jobprofiler;

25. OPFORDRER medlemsstaterne til at gennemføre initiativer inden for cybersikkerhedsbevidstgørelse og cyberhygiejne for offentligheden og slutbrugerne rettet mod ansatte i den offentlige sektor;

26. TILSKYNDER medlemsstaterne TIL at afholde cybersikkerhedsøvelser på nationalt plan og til at afholde og/eller deltage i cybersikkerhedsøvelser på EU-plan med henblik på test og uddannelse i strategiske og teknologiske aspekter og for effektivt og på et praktisk plan at udvikle de nødvendige kompetencer;

27. OPFORDRER medlemsstaterne TIL at videreudvikle deres CSIRT'ers cybersikkerhedstekniske og -operationelle kapaciteter inden for forebyggelse og afhjælpning af hændelser og hændelsesberedskab;

28. OPFORDRER Kommissionen og ENISA TIL fortsat at støtte medlemsstaternes udvikling af kapacitet i CSIRT-netværket med henblik på bedre samarbejde, udveksling af oplysninger om hændelser og effektiv reaktion på væsentlige grænseoverskridende hændelser;

29. OPFORDRER medlemsstaterne TIL fortsat at hjælpe de retshåndhævende myndigheder med at udvikle specifikke kompetencer koordineret med de kompetente europæiske myndigheder med henblik på effektivt at bekæmpe cyberkriminalitet på EU-plan;

30. TILSKYNDER medlemsstaterne TIL at øge investeringerne i cyberkapacitetsopbygning;

31. OPFORDRER Kommissionen og ENISA TIL at gennemføre programmer og uddannelse inden for cybersikkerhedsbevidstgørelse rettet mod ansatte i EU-institutioner, -agenturer og -organer;

32. OPFORDRER EU og dets medlemsstater TIL på frivillig basis at udveksle oplysninger og god praksis med henblik på at bidrage til at fastsætte og tackle de vigtigste cyberkapacitetsopbygningsbehov nationalt og på EU-plan;

33. OPFORDRER EU og dets medlemsstater TIL at støtte cybersikkerhedsforskning og fremme cybersikkerhed som et spørgsmål på andre undersøgelsesområder og forene forskellige cybersikkerhedsrelaterede forsknings- og udviklingsområder til en integrerende helhed og fremme topkvalitet inden for cybersikkerhedsforskning;

34. OPFORDRER EU og dets medlemsstater TIL at udvikle cybersikkerhedsforskning, der afspejler de samfundsmæssige behov og integrere forskningsresultaterne i markedet;

35. OPFORDRER EU og dets medlemsstater TIL i det nødvendige omfang at tage hensyn til cybersikkerhed i forbindelse med offentlige IKT-udbud.