Europeiska unionens råd

Bryssel den 20 mars 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	

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	19 mars 2019
till:	Delegationerna
Föreg. dok. nr:	6866/19
Ärende:	Rådets slutsatser om uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU

För delegationerna bifogas rådets slutsatser om uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU som antogs av allmänna rådet den 19 mars 2019.

BILAGA

Rådets slutsatser om uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU

Europeiska unionens råd

1. SOM ERINRAR OM sina slutsatser om resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU[1],

2. SOM ERINRAR om sina slutsatser om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser[2],

3. SOM ERINRAR om sina slutsatser om extern kapacitetsuppbyggnad på cyberområdet[3],

4. SOM UPPREPAR att en hög nivå på säkerhet i nätverks- och informationssystem kan tillhandahållas genom en förbättring av medlemsstaternas samt EU-institutionernas, EU-organens och EU-byråernas kapacitet och förmågor på cybersäkerhetsområdet och en därpå följande förstärkning av deras cyberresiliens,

5. SOM VÄLKOMNAR medlemsstaternas framsteg med stärkandet av it-incidentcentrumen (CSIRT),

6. SOM LOVORDAR medlemsstaternas inrättande, med aktivt stöd från kommissionen och Enisa, av CSIRT-nätverket samt det stärkta samarbetet på strategisk nivå genom samarbetsgruppen för nät- och informationssäkerhet, som består av medlemsstaterna, kommissionen och Enisa,

---

1 Dok. 14435/17 (Rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet – Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU av den 20 november 2017).

2 Dok. 10086/18 (Rådets slutsatser om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser av den 26 juni 2018).

3 Dok. 10496/18 (Rådets slutsatser om EU-riktlinjer för extern kapacitetsuppbyggnad på cyberområdet av den 26 juni 2018).

7. SOM UNDERSTRYKER den nyckelroll som samarbetsgruppen för nät- och informationssäkerhet har när det gäller tillhandahållande av nödvändig vägledning i syfte att skapa så stor enhetlighet som möjligt i införlivandet av NIS-direktivet [4] i hela EU samt när det gäller hanteringen av relevanta cybersäkerhetsfrågor,

8. SOM ERKÄNNER det stöd för kapacitetsuppbyggnad avseende CSIRT som kommissionen ger medlemsstaterna genom Fonden för ett sammanlänkat Europa,

9. SOM ERKÄNNER stödet till de brottsbekämpande myndigheterna avseende kapacitetsuppbyggnad för bekämpning av it-brottslighet genom Fonden för inre säkerhet och Cepol,

10. SOM VÄLKOMNAR uppdateringen av ramen för EU:s politik för it-försvar för att ytterligare understödja utvecklingen av medlemsstaternas it-försvarsförmågor,

11. SOM LOVORDAR de framsteg som gjorts i medlemsstaternas genomförande av NIS-direktivet,

12. SOM KONSTATERAR att cybersäkerhet är ett komplicerat och föränderligt område som är beroende av utvecklingen inom andra områden och kräver att den politiska och rättsliga ramen anpassas till nya tekniktrender och ny teknik som artificiell intelligens, blockkedjeteknik och kvantdatorteknik,

---

[4] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016).

13. SOM UNDERSTRYKER att cybersäkerhetsrelaterade utbildningsprogram samt information och medvetandehöjande kampanjer om säkerhetshot för slutanvändare är avgörande för att minska cybersäkerhetsriskerna,

14. SOM UNDERSTRYKER att cyberövningar är effektiva verktyg för att bedöma och ytterligare förbättra EU:s och medlemsstaternas beredskapsnivå när det gäller motverkande av storskaliga cyberincidenter och cyberkriser,

15. SOM UPPREPAR att cyberrymden inte har några gränser, vilket innebär att gränsöverskridande och tvärsektoriella synsätt och samarbeten är en orubblig princip för verksamhet och initiativ för kapacitetsuppbyggnad på cyberområdet,

16. SOM BETONAR vikten av samarbete mellan den offentliga sektorn, den privata sektorn och den akademiska världen, i synnerhet genom samverkansprojekt,

17. SOM BETONAR vikten av civil-militär samverkan med gemensamma mål på it-området, för att säkerställa en samstämmig och effektiv respons vid cyberhot,

18. SOM NOTERAR de framsteg som en grupp medlemsstater har uppnått med utvecklandet av cybersnabbinsatsteam för att fördjupa det frivilliga samarbetet på it-området genom ömsesidigt bistånd,

19. VÄLKOMNAR de pågående diskussionerna i rådet om kommissionens förslag till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum,

20. UPPMUNTRAR aktivt deltagande i samarbetsgruppens pågående arbete, i synnerhet det med kapacitetsuppbyggnad på cyberområdet,

21. UPPMUNTRAR samarbetsgruppens pågående arbete med EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser,

22. UPPMANAR medlemsstaterna att bygga vidare på sina nationella strategier för cybersäkerhet och integrera cybersäkerheten med beaktande av sektorsspecifika krav,

23. UPPMANAR medlemsstaterna att kontinuerligt övervaka samt utvärdera/bedöma effekten av de åtgärder som vidtagits för att stärka cyberresiliensen och förbättra cyberförmågorna och cyberkapaciteterna på nationell nivå,

24. UPPMANAR medlemsstaterna att integrera cybersäkerhet och digital kompetens i utbildningsplanerna på alla nivåer (primär utbildning, sekundärutbildning, tertiär utbildning, livslångt lärande) baserat på etablerade och framtida arbetsprofiler när så är lämpligt,

25. UPPMANAR medlemsstaterna att genomföra initiativ för att öka medvetenheten vad gäller cybersäkerhet samt initiativ för it-hygien för allmänheten och för slutanvändare, med inriktning mot offentliganställda,

26. UPPMUNTRAR medlemsstaterna att genomföra cybersäkerhetsövningar på nationell nivå samt genomföra och/eller delta i cybersäkerhetsövningar på EU-nivå för att testa strategiska och tekniska aspekter, utbilda om dessa samt effektivt och praktiskt utveckla de nödvändiga färdigheterna,

27. UPPMANAR medlemsstaterna att ytterligare utveckla de tekniska och operativa cybersäkerhetsförmågorna hos sina CSIRT:er vad gäller förebyggande, begränsning och hantering av incidenter,

28. UPPMANAR kommissionen och Enisa att fortsätta stödja medlemsstaternas utveckling av CSIRT-nätverkets kapacitet och förmåga, så att medlemsstaterna bättre kan samarbeta, utbyta information om incidenter och effektivt hantera storskaliga gränsöverskridande incidenter,

29. UPPMANAR medlemsstaterna att fortsätta att hjälpa de brottsbekämpande myndigheterna att i samordning med de behöriga europeiska myndigheterna utveckla särskild kompetens för att effektivt bekämpa it-brottslighet på EU-nivå,

30. UPPMANAR medlemsstaterna att öka investeringarna i kapacitetsuppbyggnad på cyberområdet,

31. UPPMANAR kommissionen och Enisa att genomföra informationsprogram om cybersäkerhet samt utbildning för anställda vid EU:s institutioner, organ och byråer,

32. UPPMANAR EU och dess medlemsstater att frivilligt dela information och bästa praxis för att bidra till att kartlägga och möta de största behoven av kapacitetsuppbyggnad på cyberområdet på nationell nivå och EU-nivå,

33. UPPMANAR EU och dess medlemsstater att stödja forskning om cybersäkerhet och främja att cybersäkerhet tas upp inom andra forskningsområden, föra samman olika delområden av cybersäkerhetsrelaterad forskning och utveckling till en integrerad helhet samt främja spetskompetens inom cybersäkerhetsforskningen,

34. UPPMANAR EU och dess medlemsstater att utveckla cybersäkerhetsforskningen så att den återspeglar samhällets behov och så att forskningsresultaten integreras på marknaden,

35. UPPMANAR EU och dess medlemsstater att på lämplig sätt beakta cybersäkerhet vid IKT-upphandling.