Consiglio
dell'Unione europea

Bruxelles, 20 marzo 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	

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	19 marzo 2019
Destinatario:	delegazioni
n. doc. prec.:	6866/19
Oggetto:	Conclusioni del Consiglio sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE

Si allegano per le delegazioni le conclusioni del Consiglio sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE adottate dal Consiglio "Affari generali" tenutosi il 19 marzo 2019.

ALLEGATO

Conclusioni del Consiglio sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE

Il Consiglio dell'Unione europea,

1. RAMMENTANDO le sue conclusioni "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE"[1];

2. RAMMENTANDO le sue conclusioni relative alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala[2];

3. RAMMENTANDO le sue conclusioni sullo sviluppo delle capacità informatiche esterne[3];

4. RIBADENDO che un livello elevato di sicurezza delle reti e dei sistemi informativi può essere garantita rafforzando le capacità e le competenze in materia di cibersicurezza degli Stati membri e delle istituzioni, delle agenzie e degli organi dell'UE, nonché mediante il conseguente potenziamento della loro ciberresilienza;

5. ACCOGLIENDO CON FAVORE i progressi realizzati dagli Stati membri nel rafforzamento dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT);

6. ELOGIANDO la creazione della rete dei CSIRT da parte degli Stati membri con il sostegno attivo della Commissione e dell'ENISA, nonché la cooperazione rafforzata a livello strategico attraverso il gruppo di cooperazione NIS, composto dagli Stati membri, dalla Commissione e dall'ENISA;

---

1 doc. 14435/17 (Conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, del 20 novembre 2017).

2 doc. 10086/18 (Conclusioni relative alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala, del 26 giugno 2018).

3 doc. 10496/18 (Conclusioni del Consiglio sugli orientamenti dell'UE per lo sviluppo delle capacità informatiche esterne, del 26 giugno 2018).

7. SOTTOLINEANDO il ruolo fondamentale del gruppo di cooperazione NIS nel fornire gli orientamenti necessari al fine di allineare quanto più possibile le modalità di recepimento della direttiva NIS[4] in tutta l'UE, nonché nel far fronte alle pertinenti questioni riguardanti la cibersicurezza;

8. RICONOSCENDO l'attuale sostegno fornito dalla Commissione agli Stati membri per lo sviluppo di capacità ad opera dei CSIRT attraverso il meccanismo per collegare l'Europa;

9. RICONOSCENDO il sostegno fornito alle autorità di contrasto per lo sviluppo di capacità nella lotta contro la criminalità informatica tramite il Fondo sicurezza interna e CEPOL;

10. ACCOGLIENDO CON FAVORE l'aggiornamento del quadro strategico UE in materia di ciberdifesa volto a intensificare il sostegno allo sviluppo delle competenze in materia di ciberdifesa degli Stati membri;

11. ELOGIANDO i progressi compiuti nell'attuazione della direttiva NIS da parte degli Stati membri;

12. RILEVANDO che la cibersicurezza è un settore complesso, interdipendente e in continua evoluzione, che richiede l'adattamento del quadro politico e giuridico alle nuove tendenze tecnologiche e alle tecnologie emergenti tra cui l'intelligenza artificiale, la tecnologia blockchain e l'informatica quantistica;

---

4 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016).

13. SOTTOLINEANDO che i programmi di formazione e istruzione in materia di cibersicurezza, nonché l'informazione e la sensibilizzazione sulle minacce alla sicurezza per gli utenti finali sono fondamentali per ridurre i rischi per la cibersicurezza;

14. SOTTOLINEANDO che le esercitazioni informatiche sono strumenti efficaci per valutare e migliorare ulteriormente il livello di preparazione dell'UE e dei suoi Stati membri per contrastare gli incidenti e le crisi di cibersicurezza su vasta scala;

15. RIBADENDO che il ciberspazio non ha frontiere, vale a dire che le prospettive e la cooperazione transfrontaliere e intersettoriali sono elementi essenziali delle attività e delle iniziative di sviluppo di capacità informatiche;

16. SOTTOLINEANDO l'importanza della cooperazione tra il settore pubblico, il settore privato e il mondo accademico, in particolare attraverso progetti collaborativi;

17. SOTTOLINEANDO l'importanza della cooperazione civile-militare per la realizzazione di obiettivi comuni in materia di cibersicurezza, al fine di garantire una risposta coerente ed efficace alle minacce informatiche;

18. PRENDE ATTO dei progressi compiuti da una serie di Stati membri nella creazione di gruppi di risposta rapida agli incidenti informatici al fine di approfondire la cooperazione volontaria in materia di cibersicurezza mediante la mutua assistenza;

19. ACCOGLIE CON FAVORE le discussioni in corso in sede di Consiglio sulla proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento, presentata dalla Commissione;

20. INCORAGGIA la partecipazione attiva ai lavori in corso del gruppo di cooperazione NIS, in particolare per quanto riguarda lo sviluppo di capacità informatiche;

21. INCORAGGIA i lavori in corso in sede di gruppo di cooperazione NIS relativi alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala;

22. INVITA gli Stati membri a basarsi sulle proprie strategie nazionali in materia di cibersicurezza e a integrare la cibersicurezza, tenendo conto dei requisiti settoriali specifici;

23. INVITA gli Stati membri a eseguire un monitoraggio continuo, nonché valutazioni dell'impatto delle misure adottate per rafforzare la ciberresilienza e migliorare le capacità e le competenze in materia di cibersicurezza a livello nazionale;

24. INVITA gli Stati membri a integrare la cibersicurezza e l'alfabetizzazione digitale nei programmi di studio a tutti i livelli di istruzione (primaria, secondaria, terziaria, apprendimento permanente) basandosi, se del caso, su profili professionali esistenti e futuri;

25. INVITA gli Stati membri a realizzare iniziative di sensibilizzazione in materia di cibersicurezza e di igiene informatica per i cittadini e gli utenti finali, in particolare i dipendenti del settore pubblico;

26. INCORAGGIA gli Stati membri a realizzare esercitazioni di cibersicurezza a livello nazionale, nonché a realizzare e/o partecipare a esercitazioni di cibersicurezza a livello di UE, al fine di effettuare prove e addestramenti sugli aspetti strategici e tecnologici, nonché sviluppare le competenze necessarie in modo efficace e a livello pratico;

27. INVITA gli Stati membri a sviluppare ulteriormente le competenze tecniche e operative in materia di cibersicurezza dei loro CSIRT nella prevenzione, mitigazione e risposta in caso di incidenti;

28. INVITA la Commissione e l'ENISA e a continuare a sostenere gli Stati membri nello sviluppare le capacità e le competenze della rete dei CSIRT, in modo da migliorare la cooperazione e lo scambio di informazioni sugli incidenti e rispondere efficacemente agli incidenti transfrontalieri su vasta scala;

29. INVITA gli Stati membri a continuare ad assistere le autorità di contrasto nello sviluppare competenze specifiche, in coordinamento con le autorità europee competenti, al fine di lottare efficacemente contro la criminalità informatica a livello dell'UE;

30. INVITA gli Stati membri ad aumentare gli investimenti nello sviluppo di capacità informatiche;

31. INVITA la Commissione e l'ENISA ad attuare programmi di sensibilizzazione e di formazione in materia di cibersicurezza destinati ai dipendenti delle istituzioni, agenzie e organismi dell'UE;

32. INVITA l'UE e i suoi Stati membri a condividere informazioni e migliori pratiche su base volontaria al fine di contribuire a individuare e affrontare le principali esigenze di sviluppo di capacità informatica a livello nazionale e dell'UE;

33. INVITA l'UE e i suoi Stati membri a sostenere la ricerca in materia di cibersicurezza e a promuovere quest'ultima in altri ambiti di studio, riunendo vari settori di ricerca e sviluppo correlati alla cibersicurezza in un insieme integrato, nonché a promuovere l'eccellenza nella ricerca in materia di cibersicurezza;

34. INVITA l'UE e i suoi Stati membri a incrementare la ricerca in materia di cibersicurezza rispecchiando le esigenze della società e integrando nel mercato i risultati di tale ricerca;

35. INVITA l'UE e i suoi Stati membri a tenere conto della cibersicurezza nelle gare d'appalto per le TIC, ove opportuno.