Consiglio
dell'Unione europea

Bruxelles, 21 giugno 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	21 giugno 2022
Destinatario:	Delegazioni
n. doc. prec.:	9716/22
Oggetto:	Conclusioni del Consiglio sulla relazione speciale n. 05/2022 della Corte dei conti europea dal titolo "Cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE: il livello complessivo di preparazione non è commisurato alle minacce" - Conclusioni del Consiglio approvate dal Consiglio nella sessione del 21 giugno 2022

Si allegano per le delegazioni le conclusioni del Consiglio in oggetto, approvate dal Consiglio nella sessione del 21 giugno 2022.

ALLEGATO

CONCLUSIONI DEL CONSIGLIO

sulla relazione speciale n. 05/2022 della Corte dei conti europea dal titolo "Cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE: il livello complessivo di preparazione non è commisurato alle minacce"

IL CONSIGLIO DELL'UNIONE EUROPEA,

RAMMENTANDO le sue conclusioni sul miglioramento dell'esame delle relazioni speciali elaborate dalla Corte dei conti nel quadro della procedura di scarico[1],

1. PRENDE ATTO della relazione speciale n. 05/2022 della Corte dei conti europea dal titolo "Cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE: il livello complessivo di preparazione non è commisurato alle minacce"[2].

2. SOTTOLINEA l'importanza e l'urgenza di rafforzare il livello di cibersicurezza all'interno delle istituzioni, degli organi e delle agenzie dell'UE, alla luce della recente intensificazione della trasformazione digitale presso le istituzioni, delle informazioni sensibili da esse trattate, del numero e della gravità sempre maggiori degli attacchi contro le istituzioni, gli organi e le agenzie dell'UE e del livello di minaccia che li riguarda.

3. RICHIAMA le conclusioni del Consiglio europeo del 20 giugno 2019[3], nelle quali il Consiglio europeo ha invitato le istituzioni dell'UE, insieme agli Stati membri, a lavorare a misure per aumentare la resilienza e migliorare la cultura della sicurezza dell'UE contro le minacce informatiche e ibride provenienti dall'esterno dell'UE, nonché per meglio proteggere da qualsiasi attività dolosa le reti di informazione e di comunicazione dell'UE e i suoi processi decisionali.

---

1 Doc. 7515/00 + COR 1.
2 Doc. 8040/22.
3 Doc. EUCO 9/19.

4. RAMMENTA le sue conclusioni del 10 dicembre 2019 sugli sforzi complementari per rafforzare la resilienza e contrastare le minacce ibride[4], nelle quali ha chiesto alle istituzioni, agli organi e alle agenzie dell'UE, con il sostegno dagli Stati membri, di assicurare la capacità dell'Unione di proteggere la propria integrità e di rafforzare la sicurezza delle reti di informazione e comunicazione e dei processi decisionali dell'UE rispetto alle attività dolose di ogni genere, partendo da una valutazione completa delle minacce. A questo fine, nelle conclusioni si affermava che occorre che le istituzioni, gli organi e le agenzie, con il sostegno degli Stati membri, elaborino e mettano in pratica un insieme completo di misure destinate a garantirne la sicurezza, conformemente al mandato del Consiglio europeo di giugno 2019[5].

5. RICORDA le sue conclusioni del 22 marzo 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale[6], nelle quali ha sottolineato che la cibersicurezza è fondamentale per il funzionamento della pubblica amministrazione e delle istituzioni a livello sia nazionale che dell'UE, nonché per la nostra società e per l'economia nel suo complesso.

6. RICHIAMA le sue conclusioni del 23 maggio 2022 sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica[7], nelle quali le istituzioni, gli organi e le agenzie dell'UE sono stati incoraggiati a partecipare a una mappatura degli strumenti esistenti per la comunicazione sicura nel settore informatico, da discutere in seno ai pertinenti organi del Consiglio e con i pertinenti gruppi di cooperazione, quali la rete degli CSIRT e la rete EU-CyCLONe.

7. SOTTOLINEA la necessità di affrontare il rischio sistemico esistente nell'interconnessione tra le istituzioni, gli organi e le agenzie dell'UE, nonché tra questi ultimi e le istituzioni degli Stati membri, nonostante la loro indipendenza istituzionale e la loro autonomia amministrativa.

---

4 Doc. 14972/19.
5 Doc. EUCO 9/19.
6 Doc. 6722/21.
7 Doc. 9364/22.

8. PRENDE ATTO delle osservazioni contenute nella relazione speciale, vale a dire che le istituzioni, gli organi e le agenzie dell'UE non hanno raggiunto un livello di preparazione in materia di cibersicurezza commisurato alle minacce e hanno livelli di maturità diversi in materia di cibersicurezza. RICONOSCE che il livello di preparazione in materia di cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE, nonché le sinergie tra di essi, dovrebbero essere migliorati.

9. INCORAGGIA pertanto vivamente le istituzioni, gli organi e le agenzie dell'UE a proseguire l'attuazione di misure di gestione dei rischi informatici che garantiscano un livello commisurato di cibersicurezza, come previsto dalla proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, al fine di migliorare il loro livello di preparazione.

10. INVITA le istituzioni, gli organi e le agenzie dell'UE a intensificare sia i loro sforzi per proteggersi dalle minacce informatiche sia la loro cooperazione per la definizione di norme e specifiche coerenti, in particolare per appalti pubblici, progetti e servizi connessi alla cibersicurezza, e a migliorare l'interoperabilità dei loro sistemi informatici, anche al fine di garantire la comunicazione sicura di contenuti non classificati.

11. INVITA l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee (CERT-UE), nell'ambito delle loro competenze, a intensificare la loro cooperazione a sostegno delle istituzioni, degli organi e delle agenzie dell'UE nei loro sforzi in materia di cibersicurezza, in particolare per quanto riguarda lo sviluppo di capacità per le istituzioni, gli organi e le agenzie dell'UE che hanno un livello inferiore di maturità in materia di cibersicurezza.

12. PRENDE ATTO delle conclusioni e raccomandazioni della relazione speciale e RICONOSCE che il livello di preparazione in materia di cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE, nonché le sinergie tra di essi, dovrebbero essere notevolmente migliorati. Le istituzioni, gli organi e le agenzie dell'UE dovrebbero disporre di un quadro completo di gestione dei rischi per la cibersicurezza, effettuare valutazioni e audit periodici dei rischi, sulla base di una metodologia comune o ben nota e di norme internazionali, e rendere sistematici programmi di sensibilizzazione e formazione in materia di cibersicurezza destinati al personale.

13. SOTTOLINEA inoltre che le istituzioni, gli organi e le agenzie dell'UE dovrebbero stanziare un bilancio sufficiente per garantire l'attuazione di misure di protezione contro le minacce informatiche, nel rispetto del quadro finanziario pluriennale, e PRENDE ATTO della raccomandazione della relazione speciale secondo cui dovrebbe essere nominato un organo rappresentativo di tutte le istituzioni, gli organi e le agenzie dell'UE e dotato di uno specifico mandato e di specifici mezzi per monitorare la conformità alle norme comuni di cibersicurezza.

14. RICONOSCE che la CERT-UE dovrebbe essere informata senza indugio degli incidenti significativi di cibersicurezza in seno alle istituzioni, agli organi e alle agenzie dell'UE e, a tal fine, dovrebbe essere dotata di risorse adeguate, prevedibili e adattate all'attuale livello di minaccia e alle esigenze delle istituzioni, degli organi e delle agenzie dell'UE, in particolare in termini di personale, attrezzature tecniche e infrastrutture.

15. OSSERVA che la cooperazione e lo scambio di informazioni sulla cibersicurezza, nonché l'interoperabilità di canali di comunicazione sicuri tra le istituzioni, gli organi e le agenzie dell'UE, dovrebbero essere rafforzati e resi sistematici. CHIEDE che tale cooperazione e tale scambio di informazioni includano anche le autorità pubbliche responsabili della cibersicurezza negli Stati membri.

16. PRENDE ATTO delle risposte della Commissione, della CERT-UE e dell'ENISA che accompagnano la relazione speciale.

17. INVITA la Commissione a tenere conto delle raccomandazioni della relazione speciale e a essere ambiziosa nell'elaborazione delle politiche in materia di cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE, nonché a sostenere maggiori sinergie tra di essi.