Consiliul
Uniunii Europene

**Bruxelles, 21 iunie 2022**
**(OR. en)**

**10504/22**

**CYBER 232**
**TELECOM 288**
**CSC 286**
**CSCI 96**
**FIN 689**

**REZULTATUL LUCRĂRILOR**

| | |
|---|---|
| Sursă: | Secretariatul General al Consiliului |
| Data: | 21 iunie 2022 |
| Destinatar: | Delegațiile |
| Nr. doc. ant.: | 9716/22 |
| Subiect: | Concluziile Consiliului privind Raportul special nr. 5/2022 al Curții de Conturi Europene intitulat „Securitatea cibernetică a instituțiilor, organelor și agențiilor UE: per ansamblu, nivelul de pregătire nu este proporțional cu amenințările”<br>- Concluziile Consiliului aprobate de Consiliu în cadrul reuniunii sale din 21 iunie 2022 |

În anexă, se pune la dispoziția delegațiilor textul concluziilor Consiliului sus-menționate, astfel cum au fost aprobate de Consiliu în cadrul reuniunii sale din 21 iunie 2022.

**ANEXĂ**

**CONCLUZIILE CONSILIULUI**

**privind Raportul special nr. 5/2022 al Curții de Conturi Europene**
**intitulat**
**„Securitatea cibernetică a instituțiilor, organelor și agențiilor UE: per ansamblu, nivelul de pregătire nu este proporțional cu amenințările”**

CONSILIUL UNIUNII EUROPENE,

REAMINTIND concluziile sale privind îmbunătățirea examinării rapoartelor speciale întocmite de Curtea de Conturi în contextul procedurii de descărcare de gestiune[1];

1. IA ACT de Raportul special nr. 5/2022 al Curții de Conturi Europene intitulat „Securitatea cibernetică a instituțiilor, organelor și agențiilor UE: per ansamblu, nivelul de pregătire nu este proporțional cu amenințările”[2].

2. SUBLINIAZĂ importanța și urgența consolidării nivelului de securitate cibernetică în cadrul instituțiilor, organelor și agențiilor UE, având în vedere intensificarea recentă a transformării digitale în cadrul instituțiilor, informațiile sensibile pe care le prelucrează, creșterea continuă a numărului și a gravității atacurilor asupra instituțiilor, organelor și agențiilor UE, precum și nivelul de amenințare la adresa acestora.

3. REAMINTEȘTE concluziile Consiliului European din 20 iunie 2019[3], în care Consiliul European a invitat instituțiile UE, împreună cu statele membre, să lucreze la elaborarea unor măsuri pentru a spori reziliența și a îmbunătăți cultura securității UE în fața amenințărilor cibernetice și a amenințărilor hibride din afara UE și pentru a proteja mai bine rețelele de informații și comunicații ale UE, precum și procesele decizionale ale acesteia, de acte răuvoitoare de orice tip.

---

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

4. REAMINTEȘTE concluziile sale din 10 decembrie 2019 privind eforturi complementare de sporire a rezilienței și de contracarare a amenințărilor hibride[4], în care a solicitat instituțiilor, organelor și agențiilor UE, sprijinite de statele membre, să asigure capacitatea Uniunii de a-și proteja integritatea și de a spori securitatea rețelelor de informare și comunicare și a proceselor decizionale ale UE împotriva activităților răuvoitoare de toate tipurile, pe baza unei evaluări cuprinzătoare a amenințărilor. În acest scop, s-a indicat în concluzii, instituțiile, organele și agențiile, sprijinite de statele membre, ar trebui să elaboreze și să pună în aplicare un set cuprinzător de măsuri care să asigure securitatea acestora, în conformitate cu mandatul Consiliului European din iunie 2019[5].

5. REAMINTEȘTE concluziile sale din 22 martie 2021 privind Strategia de securitate cibernetică a UE pentru deceniul digital[6], în care a subliniat că securitatea cibernetică este vitală pentru funcționarea instituțiilor și administrației publice, atât la nivel național, cât și la nivelul UE, precum și pentru societatea noastră și pentru economie în ansamblu.

6. REAMINTEȘTE concluziile sale din 23 mai 2022 privind dezvoltarea poziției cibernetice a Uniunii Europene[7], în care instituțiile, organele și agențiile UE au fost încurajate să participe la cartografierea instrumentelor existente pentru comunicații securizate în domeniul cibernetic, care urmează să fie discutată în cadrul organismelor relevante ale Consiliului și cu grupurile de cooperare relevante, cum ar fi rețeaua CSIRT și CyCLONe UE.

7. SUBLINIAZĂ necesitatea de a aborda riscul sistemic care există în interconexiunea dintre instituțiile, organele și agențiile UE, precum și dintre acestea și instituțiile statelor membre, în pofida independenței lor instituționale și a autonomiei lor administrative.

---

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

8. IA ACT de observațiile raportului special, și anume că instituțiile, organele și agențiile UE nu au atins un nivel de pregătire cibernetică proporțional cu amenințările și au niveluri diferite de maturitate a securității cibernetice. RECUNOAȘTE că nivelul de pregătire în materie de securitate cibernetică al instituțiilor, organelor și agențiilor UE, precum și sinergiile dintre acestea ar trebui îmbunătățite.

9. Prin urmare, ÎNCURAJEAZĂ ferm instituțiile, organele și agențiile UE să continue punerea în aplicare a măsurilor de gestionare a riscurilor cibernetice care să asigure un nivel proporțional de securitate cibernetică, astfel cum se prevede în propunerea de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148, în vederea îmbunătățirii nivelului lor de pregătire.

10. INVITĂ instituțiile, organele și agențiile UE să își intensifice eforturile atât pentru a se proteja împotriva amenințărilor cibernetice și a proteja cooperarea în vederea stabilirii unor standarde și specificații coerente, în special pentru achizițiile publice, proiectele și serviciile legate de securitatea cibernetică, cât și pentru a îmbunătăți interoperabilitatea sistemelor lor informatice, inclusiv în vederea asigurării comunicării securizate a conținutului neclasificat.

11. INVITĂ Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE), în cadrul competențelor lor, să își intensifice cooperarea în ceea ce privește sprijinirea instituțiilor, organelor și agențiilor UE în eforturile lor în materie de securitate cibernetică, în special în ceea ce privește consolidarea capacităților pentru instituțiile, organele și agențiile UE care au un nivel mai scăzut de maturitate a securității cibernetice.

12. IA ACT de concluziile și recomandările raportului special și RECUNOAȘTE că nivelul de pregătire în materie de securitate cibernetică al instituțiilor, organelor și agențiilor UE, precum și sinergiile dintre acestea ar trebui îmbunătățite substanțial. Instituțiile, organele și agențiile UE ar trebui să dispună de un cadru cuprinzător de gestionare a riscurilor pentru securitatea cibernetică, să efectueze evaluări și audituri periodice ale riscurilor, bazate pe o metodologie comună sau bine cunoscută și pe standarde internaționale, și să sistematizeze programe de sensibilizare și de formare în materie de securitate cibernetică pentru personal.

13. SUBLINIAZĂ, de asemenea, că instituțiile, organele și agențiile UE ar trebui să aloce un buget suficient pentru a asigura punerea în aplicare a măsurilor de protecție împotriva amenințărilor cibernetice, respectând în același timp cadrul financiar multianual, și IA ACT de recomandarea raportului special potrivit căreia ar trebui numit un organism reprezentativ al tuturor instituțiilor, organelor și agențiilor UE, căruia să i se acorde mandatul și mijloacele adecvate pentru a monitoriza respectarea normelor comune privind securitatea cibernetică.

14. RECUNOAȘTE că CERT-UE ar trebui să fie informat fără întârziere cu privire la incidentele semnificative de securitate cibernetică din cadrul instituțiilor, organelor și agențiilor UE și, în acest scop, ar trebui să dispună de resurse adecvate, previzibile și adaptate nivelului actual de amenințare și nevoilor instituțiilor, organelor și agențiilor UE, în special în ceea ce privește personalul, echipamentele tehnice și infrastructura.

15. IA ACT de faptul că cooperarea și schimbul de informații privind securitatea cibernetică, precum și interoperabilitatea canalelor de comunicare securizate între instituțiile, organele și agențiile UE ar trebui consolidate și sistematizate. SOLICITĂ ca această cooperare și acest schimb de informații să includă și autoritățile publice responsabile cu securitatea cibernetică din statele membre.

16. IA ACT de răspunsurile Comisiei, CERT-UE și ENISA care însoțesc raportul special.

17. INVITĂ Comisia să țină seama de recomandările raportului special și să fie ambițioasă atunci când elaborează politicile în materie de securitate cibernetică ale instituțiilor, organelor și agențiilor UE și să pledeze pentru mai multe sinergii între acestea.