



RĂSPUNSURILE COMISIEI EUROPENE

LA RAPORTUL SPECIAL AL CURȚII DE CONTURI EUROPENE

intitulat „Detectarea incidentelor de securitate
cibernetică și răspunsul la acestea”

Cuprins

I. RĂSPUNSURILE COMISIEI PE SCURT.....	2
II. RĂSPUNSURI LA RECOMANDĂRI.....	4
Recomandarea 1 – Să se consolideze schimbul de informații între statele membre.....	4
Recomandarea 2 – Să se raționalizeze capacitățile UE de conștientizare a situației în materie de securitate cibernetică și să se optimizeze diseminarea informațiilor	4
Recomandarea 3 – Să se integreze sistemul european de alertă în materie de securitate cibernetică în peisajul securității cibernetică din UE	5
Recomandarea 4 – Să se asigure o evaluare solidă privind proprietatea și controlul entităților care primesc finanțare din partea UE în cadrul programului „Europa digitală”	5
Recomandarea 5 – Să se consolideze cadrul de monitorizare a performanței aferent componentei de securitate cibernetică a programului „Europa digitală”	6

În conformitate cu articolul 265 din [Regulamentul financiar](#), prezentul document cuprinde răspunsurile Comisiei Europene la observațiile dintr-un raport special al Curții de Conturi Europene și urmează să fie publicat concomitent cu raportul special.

I. RĂSPUNSURILE COMISIEI PE SCURT

Comisia salută interesul susținut al Curții de Conturi Europene (CCE) față de securitatea cibernetică și, îndeosebi în prezentul raport special, față de detectarea incidentelor de securitate cibernetică și răspunsul la acestea, precum și față de practicile sale de gestionare a programelor.

În ceea ce privește cadrul UE pentru incidentele semnificative și de mare amploare, Comisia reamintește faptul că acesta este relativ nou și s-a bazat în mare parte pe cooperarea voluntară și pe schimbul de informații dintre entitățile UE și statele membre, reflectând echilibrul dintre competențele UE și cele naționale în ceea ce privește securitatea. Abia odată cu adoptarea Directivei (UE) 2022/2555¹ a fost definit conceptul de incidente de mare amploare în dreptul UE și a fost creată Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetică (EU-CyCLONe) pentru a sprijini gestionarea coordonată a incidentelor și a crizelor de securitate cibernetică de mare amploare la nivel operațional și pentru a asigura schimbul periodic de informații relevante între statele membre și instituțiile, organele, oficiile și agențiile UE. Cu toate acestea, după cum se menționează în raport², acest cadru a devenit din ce în ce mai important, având în vedere digitalizarea rapidă a infrastructurii critice și volatilitatea geopolitică, în special odată cu escaladarea situației amenințărilor cibernetică. Recomandarea Consiliului privind un plan de acțiune al UE pentru gestionarea crizelor cibernetică, adoptată în iunie 2025 („Planul de acțiune privind securitatea cibernetică”)³, descrie cadrul, precum și rolurile și responsabilitățile distincte ale diferitelor părți interesate. Planul de acțiune privind securitatea cibernetică recomandă acțiuni de îmbunătățire a funcționării practice a acestui cadru, cum ar fi convenirea asupra unei taxonomii comune aliniate a nivelurilor de gravitate a incidentelor și îndemnarea rețelei echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) și a EU-CyCLONe să convină fără întârziere, astfel cum se prevede în Directiva (UE) 2022/2555, asupra modalităților procedurale în caz de incidente de securitate cibernetică de mare amploare potențiale sau aflate în curs. În prezent, Comisia colaborează cu alte entități relevante ale UE și cu statele membre pentru punerea în aplicare a recomandării Consiliului.

Statele membre au fost obligate să transpună Directiva (UE) 2022/2555 până în octombrie 2024, iar Comisia continuă să ia decizii de constatare a neîndeplinirii obligațiilor în ceea ce privește statele membre care nu au comunicat măsurile luate pentru transpunerea directivei în legislația națională. Regulamentul privind solidaritatea cibernetică a fost adoptat în 2025, iar instrumentele pe care le creează, cum ar fi rezerva pentru securitate cibernetică și centrele cibernetică, vor necesita timp pentru a fi pe deplin operaționale. Comisia recunoaște necesitatea unui rol sporit al Agenției Europene pentru Securitate Cibernetică (ENISA) în ceea ce privește contribuția la pregătirea și răspunsul la nivelul UE în cazul unor incidente de mare amploare, inclusiv prin emiterea de alerte timpurii și prin furnizarea de sprijin pentru răspunsul la incidente și pentru revizuire. În consecință, aceasta este o componentă importantă a propunerii Comisiei de revizuire a Regulamentului privind securitatea cibernetică⁴. Prin urmare, este extrem de urgent ca statele membre să pună în aplicare pe deplin normele existente și ca pachetul de noi măsuri să fie adoptat de Parlament și de Consiliu cât mai curând posibil.

¹ JO L 333, 27.12.2022, p. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>.

² Raportul special, punctele 01-05.

³ JO C, C/2025/3445, 20.6.2025, ELI: <http://data.europa.eu/eli/C/2025/3445/oj>.

⁴ COM(2026) 11 final.

Comisia este de acord cu constatarea CCE⁵, bazată pe raportarea ENISA cu privire la peisajul amenințărilor, potrivit căreia incidentele semnificative, în special cele de natură transfrontalieră, rămân subraportate, iar valoarea potențială a mecanismelor de cooperare care există în cadrul UE nu a fost încă fructificată. În același timp, Comisia reamintește că cooperarea în materie de securitate cibernetică depinde de încredere și că nu există nicio obligație în temeiul normelor UE aplicabile pentru schimbul de informații între entitățile UE și statele membre. Rețeaua CSIRT, creată prin prima Directivă privind securitatea rețelilor și a sistemelor informatice (NIS)⁶, și EU-CyCLONe ar trebui încurajate să promoveze o cultură a schimbului de informații în cadrul celor două rețele și între acestea. Totuși, securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru, care nu poate fi obligat să furnizeze informații a căror divulgare ar fi contrară intereselor sale esențiale de securitate națională, siguranță publică sau apărare.

Deși este de acord cu recomandarea 2: „Să se raționalizeze capacitățile UE de conștientizare a situației în materie de securitate cibernetică și să se optimizeze diseminarea informațiilor”, Comisia recunoaște necesitatea unor anumite elemente de context: astfel cum se prevede în Planul de acțiune privind securitatea cibernetică, diferite părți interesate de la nivelul UE au roluri distincte în gestionarea incidentelor semnificative și de mare amploare. Comisia, în calitatea sa de instituție cu responsabilități politice și operaționale în ceea ce privește pregătirea pentru situații de criză și răspunsul la acestea, inclusiv în cazul unor incidente de securitate cibernetică de mare amploare potențiale și aflate în curs, a investit în mod corespunzător în dezvoltarea unui Centru de conștientizare a situației în materie de securitate cibernetică în cadrul unuia dintre departamentele sale, cu sprijinul unor servicii personalizate furnizate de un prestator extern de servicii contractat pentru o perioadă limitată. Comisia recunoaște necesitatea de a explora noi sinergii și de a spori eficiența colaborării cu ENISA, subliniind, în același timp, că responsabilitățile serviciilor Comisiei însărcinate cu aceste problematice, împreună cu contractul de servicii externe pentru Centrul de conștientizare a situației în materie de securitate cibernetică, sunt chestiuni distincte. Nu există nicio suprapunere între rolul Comisiei și cel al ENISA, deoarece acestea desfășoară activități în concordanță cu mandatele lor⁷. Mai mult, există structuri care asigură fluxul de informații între departamentele Comisiei și între entitățile relevante ale UE, inclusiv ENISA, în cazul unui incident semnificativ sau de mare amploare.

În ceea ce privește rezerva pentru securitate cibernetică⁸, Comisia reamintește că obiectivul subiacent este ca, în cazul unor incidente de securitate cibernetică semnificative sau de mare amploare, toate statele membre, instituțiile, organele, oficiile și agențiile UE, precum și anumite țări terțe asociate la programul Europa digitală să aibă un instrument care să fie disponibil 24 de ore pe zi, 7 zile din 7. Cu toate acestea, ar trebui subliniat faptul că este practic imposibil să se prevadă câte incidente de securitate cibernetică de o asemenea amploare vor avea loc.

În ceea ce privește Centrul european de competențe în materie de securitate cibernetică (ECCC)⁹, Comisia recunoaște faptul că a fost nevoie de timp pentru instituirea Comunității de competențe în materie de securitate cibernetică și a Grupului consultativ strategic. Totuși, ar trebui să se țină seama de faptul că, de atunci, Rețeaua de centre naționale de coordonare funcționează ca un intermediar și ca o legătură directă cu comunitățile de părți interesate din statele membre în scopul colectării de informații și al pregătirii programelor de lucru.

Comisia ia act în mod corespunzător de toate constatările raportului și le va analiza cu atenție în viitor.

⁵ Raportul special, punctul 35.

⁶ JO L 194, 19.7.2016, p. 1, ELI: <http://data.europa.eu/eli/dir/2016/1148/oj>.

⁷ Raportul special, pagina de titlu 19, punctele 11 și 48.

⁸ Raportul special, punctele 52-61.

⁹ A se vedea raportul, secțiunile 17 și 77-81.

II. RĂSPUNSURI LA RECOMANDĂRI

Recomandarea 1 – Să se consolideze schimbul de informații între statele membre

Pentru a îmbunătăți detectarea incidentelor de securitate cibernetică și răspunsul la acestea, Comisia, cu sprijinul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), ar trebui:

(a) să propună Grupului de cooperare în materie de securitate a rețelelor și a informațiilor să efectueze o analiză detaliată a restricțiilor de securitate națională care limitează schimbul de informații și care afectează reziliența cibernetică a UE și să identifice soluții juridice și tehnice pentru a îmbunătăți schimbul de informații, cu respectarea, în același timp, a limitelor impuse de securitatea națională;

(b) fără a aduce atingere deciziilor colegiuitorilor, să se asigure, în colaborare cu statele membre, că punctul unic de contact pentru raportarea incidentelor propus de Regulamentul omnibus în domeniul digital poate detecta potențialele incidente transfrontaliere;

(c) să depună eforturi pentru găsirea unor soluții care să permită raportarea în timp real a incidentelor către ENISA.

(Data-țintă pentru punerea în aplicare a recomandării: 2027 pentru (a) și (b) și 2028 pentru (c))

Comisia **acceptă** recomandarea 1 literele (a), (b) și (c).

Recomandarea 2 – Să se raționalizeze capacitățile UE de conștientizare a situației în materie de securitate cibernetică și să se optimizeze diseminarea informațiilor

Pentru a îmbunătăți eficiența, Comisia ar trebui ca, în colaborare cu ENISA, să evalueze fezabilitatea achiziției și analizei comune de informații necesare pentru conștientizarea situației. Ea ar trebui, de asemenea, să pună aceste informații și rapoartele conexe privind amenințările cibernetică la dispoziția tuturor serviciilor și agențiilor relevante ale UE.

(Data-țintă pentru punerea în aplicare a recomandării: 2027)

Comisia **acceptă** recomandarea 2.

Comisia sprijină această recomandare. Aceasta este în concordanță cu Recomandarea Consiliului privind un plan de acțiune al UE pentru gestionarea crizelor cibernetică și cu Propunerea Comisiei de regulament de instituire a unui regulament al UE privind securitatea cibernetică, care prevede o colaborare între entitățile relevante ale UE, inclusiv între Comisie și ENISA, pentru a crea registre de date operative privind amenințările cibernetică și recunoaște necesitatea unei raționalizări suplimentare, maximizând, în același timp, buna gestiune financiară.

Comisia acceptă această recomandare fără a aduce atingere dispozițiilor și domeniului de aplicare al Regulamentului (UE, Euratom) 2023/2841¹⁰ și statutului independent al CERT-UE, care, în ceea ce privește aspectele operaționale, rămâne sub autoritatea Consiliului interinstituțional pentru securitate cibernetică.

Recomandarea 3 – Să se integreze sistemul european de alertă în materie de securitate cibernetică în peisajul securității cibernetice din UE

Comisia, împreună cu ENISA și cu statele membre, ar trebui să se asigure că sunt instituite acorduri de cooperare și standarde de interoperabilitate pentru a facilita schimbul de informații între centrele transfrontaliere care fac parte din sistemul european de alertă în materie de securitate cibernetică, rețeaua CSIRT și EU-CyCLONe.

(Data-țintă pentru punerea în aplicare a recomandării: 2028)

Comisia **acceptă** recomandarea 3.

Recomandarea 4 – Să se asigure o evaluare solidă privind proprietatea și controlul entităților care primesc finanțare din partea UE în cadrul programului „Europa digitală”

Centrul european de competențe în materie de securitate cibernetică ar trebui:

- (a)** *să obțină o asigurare rezonabilă că beneficiarii responsabili cu furnizarea de sprijin financiar părților terțe dispun de capacitatea administrativă și tehnică necesară pentru a efectua evaluări adecvate ale proprietății și ale controlului, pe baza metodologiei existente aflate la dispoziția beneficiarilor care implementează sprijinul financiar acordat părților terțe, precum și*
- (b)** *să verifice, pe baza unor eșantioane, dacă numai entitățile eligibile au primit finanțare din partea UE.*

(Data-țintă pentru punerea în aplicare a recomandării: 2026 pentru (a) și 2027 pentru (b))

Comisia ia act de faptul că recomandarea se adresează ECCC.

¹⁰ JO L, 2023/2841, 18.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2841/oj>.

Recomandarea 5 – Să se consolideze cadrul de monitorizare a performanței aferent componentei de securitate cibernetică a programului „Europa digitală”

Pentru a permite o monitorizare adecvată a progreselor și a performanței, Centrul european de competențe în materie de securitate cibernetică ar trebui:

- a) să se asigure, înainte de semnarea unui grant, că toate proiectele au definit jaloane, livrabile și indicatori de performanță care respectă instrucțiunile furnizate în formularul de cerere;**
- b) să conceapă și să pună în aplicare un sistem solid de colectare, trasabilitate, verificare și agregare a datelor pentru indicatorii de performanță ai componentei de securitate cibernetică a programului „Europa digitală”, urmărind să se asigure că indicatorii reflectă cu acuratețe rezultatele obținute.**

(Data-țintă pentru punerea în aplicare a recomandării: 2027)

Comisia ia act de faptul că recomandarea se adresează ECCC.