



## Comunicat de presă

Luxemburg, 29 martie 2022

# Organismele UE trebuie să își intensifice pregătirea în materie de securitate cibernetică

Numărul de atacuri ciberneticе îndreptate împotriva organismelor UE este în creștere vertiginoasă. Nivelul de pregătire al acestora în materie de securitate cibernetică variază și, per ansamblu, nu este proporțional cu amenințările din ce în ce mai mari. Dat fiind că organismele UE sunt puternic interconectate, un punct slab al unuia le poate expune pe celelalte la amenințări de securitate. Aceasta este concluzia unui raport special publicat de Curtea de Conturi Europeană, care examinează cât de pregătite sunt entitățile din guvernanta UE să facă față amenințărilor ciberneticе. Auditorii recomandă să se introducă norme obligatorii în materie de securitate cibernetică și să se pună mai multe resurse la dispoziția Centrului de răspuns la incidente de securitate cibernetică (CERT-UE). De asemenea, în opinia auditorilor, Comisia Europeană ar trebui să promoveze un nivel mai mare de cooperare între organismele UE, iar CERT-UE și Agenția Uniunii Europene pentru Securitate Cibernetică ar trebui să pună un accent mai puternic pe acele organisme care au mai puțină experiență în gestionarea securității ciberneticе.

Numărul incidentelor semnificative de securitate cibernetică în organismele UE a crescut de peste zece ori între 2018 și 2021; teledemonstrarea a mărit considerabil numărul de puncte potențiale de acces pentru atacatori. Incidentele semnificative sunt cauzate în general de atacuri ciberneticе complexe, care implică de regulă utilizarea de metode și tehnologii noi, pentru investigarea și redresarea în urma lor fiind uneori nevoie de săptămâni sau chiar de luni întregi. Un astfel de exemplu a fost atacul cibernetic asupra Agenției Europene pentru Medicamente, soldat cu divulgarea unor date sensibile și manipularea acestora cu scopul de a se submina încrederea în vaccinuri.

*„Instituțiile, organele și agențiile UE sunt ținte atractive pentru potențialii atacatori, în special pentru grupuri capabile să execute atacuri disimulate extrem de sofisticate în scopuri de spionaj cibernetic sau cu alte intenții criminale”, a declarat doamna Bettina Jakobsen, membra Curții care a condus acest audit. „Astfel de atacuri pot avea implicații politice considerabile, pot afecta reputația generală a UE și pot submina încrederea în instituțiile acesteia. UE trebuie să își intensifice eforturile pentru a-și proteja propriile organizații.”*

Scopul acestui comunicat de presă este să prezinte mesajele principale ale raportului special adoptat de Curtea de Conturi Europeană. Textul integral al raportului este disponibil la adresa [eca.europa.eu](https://eca.europa.eu).

## ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: [press@eca.europa.eu](mailto:press@eca.europa.eu) @EUAuditors [eca.europa.eu](https://eca.europa.eu)

Principala constatare a auditorilor a fost că instituțiile, organele și agențiile UE nu sunt întotdeauna bine protejate împotriva amenințărilor cibernetice. Acestea nu dispun de o abordare consecventă în materie de securitate cibernetică, nu au introdus în toate cazurile controale esențiale și bune practici importante în domeniu și nu oferă sistematic formare cu privire la securitatea cibernetică. Nivelul resurselor alocate pentru securitatea cibernetică variază considerabil și o serie de organisme ale UE cheltuiesc mult mai puțin în acest domeniu decât omologii comparabili. Deși diferențele dintre nivelurile de securitate cibernetică ar putea fi justificate teoretic de profilurile de risc diferite ale fiecărei organizații și de nivelurile variabile de sensibilitate a datelor gestionate de acestea, auditorii subliniază faptul că deficiențele în materie de securitate cibernetică ale unui singur organism UE pot expune mai multe alte organizații la amenințări în domeniu (organismele UE sunt conectate atât între ele, cât și, adesea, cu organizații publice și private din statele membre).

Centrul de răspuns la incidente de securitate cibernetică și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sunt cele două entități principale ale UE care au misiunea de a acorda sprijin în materie de securitate cibernetică. Din cauza resurselor limitate sau a faptului că s-a acordat prioritate altor domenii, ele nu au fost însă în măsură să ofere organismelor UE tot sprijinul de care acestea au nevoie. În opinia auditorilor, schimbul de informații este de asemenea o problemă: de exemplu, nu toate organismele UE raportează în timp util cu privire la vulnerabilități și la incidentele semnificative de securitate cibernetică cu care s-au confruntat și care pot avea un impact asupra altor organisme.

### Informații de fond

Instituțiile, organele și agențiile UE nu dispun în prezent de un cadru juridic pentru securitatea informațiilor și securitatea cibernetică. Ele nu fac obiectul celui mai cuprinzător act legislativ al UE privind securitatea cibernetică, și anume Directiva NIS din 2016, și nici al noii directive revizuite propuse, Directiva NIS2. De asemenea, nu există informații complete cu privire la sumele cheltuite de acestea pentru securitatea cibernetică. Strategia UE privind uniunea securității pentru perioada 2020-2025, comunicare publicată de Comisia Europeană în iulie 2020, include norme comune privind securitatea informațiilor și securitatea cibernetică pentru toate organismele UE. În Strategia de securitate cibernetică a UE pentru deceniul digital, publicată în decembrie 2020, Comisia s-a angajat să propună un regulament privind norme comune în materie de securitate cibernetică pentru toate organismele UE. Această strategie propunea totodată un nou temei juridic pentru CERT-UE în vederea consolidării mandatului și a finanțării acestuia.

Raportul special nr. 05/2022, intitulat „*Securitatea cibernetică a instituțiilor, organelor și agențiilor UE – Per ansamblu, nivelul de pregătire nu este proporțional cu amenințările*”, este disponibil pe [site-ul Curții](#). Curtea s-a aplecat asupra provocărilor pentru o politică eficientă a UE în domeniul securității cibernetice și într-un [document de analiză](#) din 2019.

### Date de contact pentru presă

Serviciul de presă al Curții: [press@eca.europa.eu](mailto:press@eca.europa.eu)

- Claudia Spiti: [claudia.spiti@eca.europa.eu](mailto:claudia.spiti@eca.europa.eu) - M: (+352) 691 553 547
- Vincent Bourgeais: [vincent.bourgeais@eca.europa.eu](mailto:vincent.bourgeais@eca.europa.eu) - M: (+352) 691 551 502
- Damijan Fišer: [damijan.fiser@eca.europa.eu](mailto:damijan.fiser@eca.europa.eu) - M: (+352) 621 552 224