Curtea de Conturi Europeana: Organismele UE trebuie sa-si intensifice pregatirea în materie de securitate cibernetica

Organismele UE trebuie sa-si intensifice pregatirea în materie de securitate cibernetica în conditiile în care numarul de atacuri cibernetice îndreptate împotriva organismelor UE este în crestere vertiginoasa, arata un raport publicat de Curtea de Conturi Europeana.

Potrivit sursei citate, nivelul de pregatire al acestora în materie de securitate cibernetica variaza si, per ansamblu, nu este proportional cu amenintarile din ce în ce mai mari si dat fiind ca organismele UE sunt puternic interconectate, un punct slab al unuia le poate expune pe celelalte la amenintari de securitate.

"Aceasta este concluzia unui raport special publicat de Curtea de Conturi Europeana, care examineaza cât de pregatite sunt entitatile din guvernanta UE sa faca fata amenintarilor cibernetice. Auditorii recomanda sa se introduca norme obligatorii în materie de securitate cibernetica si sa se puna mai multe resurse la dispozitia Centrului de raspuns la incidente de securitate cibernetica (CERT-UE). De asemenea, în opinia auditorilor, Comisia Europeana ar trebui sa promoveze un nivel mai mare de cooperare între organismele UE, iar CERT-UE si Agentia Uniunii Europene pentru Securitate Cibernetica ar trebui sa puna un accent mai puternic pe acele organisme care au mai putina experienta în gestionarea securitatii cibernetice", se precizeaza în comunicatul Curtii de Conturi Europene.

Numarul incidentelor semnificative de securitate cibernetica în organismele UE a crescut de peste 10 ori între 2018 si 2021. Telemunca a marit considerabil numarul de puncte potentiale de acces pentru atacatori. Incidentele semnificative sunt cauzate în general de atacuri cibernetice complexe, care implica de regula utilizarea de metode si tehnologii noi, pentru investigarea si redresarea în urma lor fiind uneori nevoie de saptamâni sau chiar de luni întregi.

Potrivit sursei citate, un astfel de exemplu a fost atacul cibernetic asupra Agentiei Europene pentru Medicamente, soldat cu divulgarea unor date sensibile si manipularea acestora cu scopul de a se submina încrederea în vaccinuri.

"Institutiile, organele si agentiile UE sunt tinte atractive pentru potentialii atacatori, în special pentru grupuri capabile sa execute atacuri disimulate extrem de sofisticate în scopuri de spionaj cibernetic sau cu alte intentii criminale. Astfel de atacuri pot avea implicatii politice considerabile, pot afecta reputatia generala a UE si pot submina încrederea în institutiile acesteia. UE trebuie sa-si intensifice eforturile pentru a-si proteja propriile organizatii", a declarat Bettina Jakobsen, membra Curtii care a condus acest audit.

Principala constatare a auditorilor a fost ca institutiile, organele si agentiile UE nu sunt întotdeauna bine protejate împotriva amenintarilor cibernetice. Acestea nu dispun de o abordare consecventa în materie de securitate cibernetica, nu au introdus în toate cazurile controale esentiale si bune practici importante în domeniu si nu ofera sistematic formare cu privire la securitatea cibernetica. Nivelul resurselor alocate pentru securitatea cibernetica variaza considerabil si o serie de organisme ale UE cheltuiesc mult mai putin în acest domeniu decât omologi comparabili. Desi diferentele dintre nivelurile de securitate cibernetica ar putea fi justificate teoretic de profilurile de risc diferite ale fiecarei organizatii si de nivelurile variabile de sensibilitate a datelor gestionate de acestea, auditorii subliniaza faptul ca deficientele în materie de securitate cibernetica ale unui singur organism UE pot expune mai multe alte organizatii la amenintari în domeniu (organismele UE sunt conectate atât între ele, cât si, adesea, cu organizatii publice si private din statele membre).

Centrul de raspuns la incidente de securitate cibernetica si Agentia Uniunii Europene pentru Securitate

Cibernetica (ENISA) sunt cele doua entitati principale ale UE care au misiunea de a acorda sprijin în materie de securitate cibernetica. Din cauza resurselor limitate sau a faptului ca s-a acordat prioritate altor domenii, ele nu au fost însa în masura sa ofere organismelor UE tot sprijinul de care acestea au nevoie.

În opinia auditorilor, schimbul de informatii este de asemenea o problema: de exemplu, nu toate organismele UE raporteaza în timp util cu privire la vulnerabilitati si la incidentele semnificative de securitate cibernetica cu care s-au confruntat si care pot avea un impact asupra altor organisme.

Potrivit comunicatului, institutiile, organele si agentiile UE nu dispun în prezent de un cadru juridic pentru securitatea informatiilor si securitatea cibernetica. Ele nu fac obiectul celui mai cuprinzator act legislativ al UE privind securitatea cibernetica, si anume Directiva NIS din 2016, si nici al noii directive revizuite propuse, Directiva NIS2. De asemenea, nu exista informatii complete cu privire la sumele cheltuite de acestea pentru securitatea cibernetica. Strategia UE privind uniunea securitatii pentru perioada 2020-2025, comunicare publicata de Comisia Europeana în iulie 2020, include norme comune privind securitatea informatiilor si securitatea cibernetica pentru toate organismele UE.

În Strategia de securitate cibernetica a UE pentru deceniul digital, publicata în decembrie 2020, Comisia s-a angajat sa propuna un regulament privind norme comune în materie de securitate cibernetica pentru toate organismele UE. Aceasta strategie propunea totodata un nou temei juridic pentru CERT-UE în vederea consolidarii mandatului si a finantarii acestuia.

Raportul special nr. 05/2022, intitulat "Securitatea cibernetica a institutiilor, organelor si agentiilor UE; Per ansamblu, nivelul de pregatire
nu este proportional cu amenintarile", este disponibil pe site-ul Curtii.

Curtea s-a aplecat asupra provocarilor pentru o politica eficace a UE în domeniul securitatii cibernetice si într-un document de analiza din 2019, se precizeaza în comunicat.