# Oficial DG Connect: Nu am avut înca o criza specifica pentru securitatea cibernetica la nivelul UE

**Exista diverse mecanisme la nivelul Uniunii Europene pentru escaladarea unui eveniment sau incident într-o criza europeana, însa nu am avut înca o criza specifica pentru securitatea cibernetica, a declarat, marti, la Conferinta de Securitate Cibernetica de la Bucuresti (BCC2025), Christian D'Cunha, seful Departamentui Grupul Operativ pentru Criza Cibernetica al DG Connect, Comisia Europeana (CE).**

"Exista diverse mecanisme la nivelul Uniunii Europene pentru escaladarea unui eveniment sau incident într-o criza europeana. Totul a început, cred, la începutul anilor 2000, cu atacurile teroriste, când a fost activat ceea ce se numeste Mecanismul Integrat de Raspuns la Crize Politice, utilizat de mai multe ori de atunci pentru o varietate de evenimente, inclusiv eruptii vulcanice în Islanda, crize de migratie si cutremure în Turcia si Siria. Nu am avut înca o criza specifica pentru securitatea cibernetica, dar cu siguranta componenta cibernetica a fost semnificativa în mai multe activari ale acestui Mecanism, în special pentru Ucraina. Este momentul în care, la nivel politic, liderii decid ca este vorba despre o situatie care necesita un raspuns coordonat al tuturor ramurilor relevante ale statelor-membre pentru a o gestiona o situatie de criza (...) Domeniul cibernetic se încadreaza în categoria unora dintre amenintarile serioase cu care ne confruntam în mediul geopolitic actual, în evolutie si în dinamica", a spus D'Cunha.

Expertul în securitate cibernetica a amintit de beneficiile Directivei NIS2, dar si despre reteaua EU-CyCLONe, formata din autoritatile de gestionare a crizelor cibernetice din Uniunea Europeana (UE).

"În ceea ce priveste securitatea cibernetica, avem Directiva NIS2, care defineste ce înseamna un incident de amploare si, daca te uiti la preambul, se explica faptul ca acesta este un incident de securitate cibernetica care are potentialul de a escalada într-o criza completa. Nu defineste ce este o criza, dar stii când esti într-o criza, nu trebuie sa o definesti. Avem mecanisme pentru a gestiona astfel de situatii, iar cel mai important mecanism prevazut de Directiva NIS2 este înfiintarea oficiala a retelei EU-CyCLONe, formata din autoritatile de gestionare a crizelor cibernetice din UE. (...) Exista si un nivel inferior de incidente, care sunt de asemenea descrise în Directiva NIS2, unde exista un impact semnificativ asupra sectoarelor critice. Directiva NIS2 spune ca un incident de amploare poate aparea nu neaparat pentru ca un stat-membru cere ajutor, ci pentru ca exista un incident semnificativ care afecteaza doua sau mai multe state-membre. Cu alte cuvinte, este o situatie transfrontaliera. CyCLONe, împreuna cu alte retele si organisme relevante, ar trebui sa dezvolte o taxonomie pentru a determina severitatea incidentelor. Acest lucru ar ajuta statele-membre sa evalueze când o situatie nationala ar trebui adusa la masa discutiilor ca fiind o situatie europeana", a explicat reprezentantul DG Connect.

Directoratul National de Securitate Cibernetica (DNSC), cu sprijinul Centrului National de Coordonare al României (NCC-RO) si al Asociatiei Nationale pentru Securitatea Sistemelor Informatice (ANSSI), organizeaza, în perioada 6 - 9 octombrie, editia 2025 a Conferintei de Securitate Cibernetica de la Bucuresti (BCC2025).