Dinu (DNSC): Piata românească de securitate cibernetica, estimata la circa 200 de milioane de euro, este insuficienta

Piata românească de securitate cibernetica, estimata undeva la vreo 200 de milioane de euro, în momentul de fata, este insuficienta din punctul meu de vedere, a declarat, luni, adjunctul directorului Directoratului National pentru Securitate Cibernetica (DNSC), Gabriel Dinu.

"Piata românească de securitate cibernetica, estimata undeva pe la vreo 200 de milioane de euro, în momentul de fata, daca ma întrebati pe mine, este insuficienta. Securitatea cibernetica costa si una dintre modalitatile în care împingem societatea înainte, ca ne place sau nu ne place, trebuie sa fie reglementarea. Trebuie cumva sa uniformizam regulile în ceea ce priveste securitatea cibernetica pentru a atinge un nivel minim de securitate. Din punctul meu de vedere, sunt si beneficii din respectarea reglementarilor, nu sunt doar costuri (...)", a afirmat Dinu la conferinta Cybersecurity Forum

Potrivit acestuia, în ceea ce priveste reglementarea, autoritatile lucreaza pentru implementarea Directivei NIS2 iar la sfârsitul acestui proces peste 5.000 de organizatii vor trebui sa aplice reguli ce tin de securitate cibernetica.

"Am avut Directiva NIS1 care a introdus o serie de organizatii din România în ceea ce priveste obligatiile de securitate cibernetica, pentru a încerca sa creeze un nivel minim de securitate cibernetica, cu mai mult sau mai putin succes. Am avut câtiva ani în care am pilotat aceasta reglementare în România. Am trecut deja la etapa urmatoare si suntem în curs de aplicare a Directivei NIS2. Ne asteptam, la sfârsitul acestui proces, sa vorbim de peste 5.000 de organizatii (înscrise, n.r.), poate chiar spre 10.000 în functie de anumite cifre, care vor trebui sa aplice reguli ce tin de securitate cibernetica pentru a atinge un nivel minim de securitate la nivel de organizatie", a mentionat sursa citata.

Potrivit specialistului, Directiva NIS2 este o reglementare esentiala, cu caracter orizontal, care are rolul sa dezvolte instinctele societatii de aparare în domeniul securitatii cibernetice si sa creeze un minim de confort si de securitate prin aplicarea obligatiilor pe care le prevede.

"Sunt câtiva pasi importanti care s-au facut în Directiva NIS, cum ar fi implementarea obligatiei sau a responsabilitatii la nivelul managementului organizatiilor pentru a implementa cerintele de securitate cibernetica, ceea ce eu consider ca este esential daca dorim într-adevar sa generam o schimbare în organizatii. De asemenea, obligatia de raportare a incidentelor de securitate cibernetica, care acum se adreseaza unei arii mult mai largi din societate. Alaturi de atributiile pe care DNSC le are, poate sa creasca si capacitatea de raspuns la incidente de securitate cibernetica în societatea românească si, de asemenea, sa avem o imagine mai clara cu privire la impactul real al incidentelor de securitate cibernetica în societate. Probabil ca înca mai exista destule entitati care nu au acest exercitiu de transparenta în ceea ce priveste confruntarea cu astfel de probleme. O alta componenta relevanta este cea legata de implementarea unor minime reguli pentru cresterea rezilientei organizatiilor în domeniul securitatii cibernetice: gestionarea lantului de aprovizionare, implementarea unor capabilitati minime în ceea ce priveste raspunsul la crize cibernetice. Avem un cadru european de cooperare în acest sens, avem linii de finantare la nivel european pe care organizatiile ar trebui sa le exploateze pentru a-si creste nivelul de rezilienta si de securitate cibernetica", a explicat oficialul DNSC.

Acesta a mentionat, totodata, ca una dintre cele mai relevante reglementari care se completeaza foarte bine cu Directiva NIS2 este Regulamentul EU Cyber Resilience Act, care va obliga producatorii de software sau hardware sa aiba o abordare de tip "secure by design", respectiv sa securizeze aceste produse înca de la momentul în care ele sunt dezvoltate.

"Exista si se lucreaza în momentul de fata la un set de standarde de securitate cibernetica pentru multe categorii de produse care fac obiectul acestui act normativ. Din punctul meu de vedere, respectarea obligatiilor acestui act normativ este pentru producatorii din România o oportunitate pentru a avea mai mult succes în a accesa piata europeana. În momentul în care vor avea marcajul CE, în perioada urmatoare pe echipamentele si pe software-ul care va fi produs, bineînteles, nivelul de încredere fata de aceste produse va fi unul mai ridicat", a subliniat Gabriel Dinu.

Financial Intelligence a organizat, luni, evenimentul de specialitate Cybersecurity Forum, în cadrul caruia au fost dezbatute teme precum protectia în fata criminalitatii cibernetice, cyberintelligence, tentative de frauda prin Deep-Fake si Vishing.