Oficial ENISA: Cyber Resilience Act va asigura securitatea reala a produselor din Uniunea Europeana

Cyber Resilience Act va asigura principiile de baza ale securitatii cibernetice în Uniunea Europeana (UE), ce vor ajuta ca produsele noastre sa fie sigure, sa fie competitive la scara globala si sa contribuie la depasirea diferitelor cazuri de vulnerabilitati, a declarat, miercuri, la Conferinta de Securitate Cibernetica de la Bucuresti (BCC2025), Apostolos Malatras, seful Departamentului Market Technology and Product Security al Agentiei Uniunii Europene pentru Securitate Cibernetica (ENISA).

"Regulamentul privind securitatea cibernetica (CRA - Cyber Resilience Act, n.r.), pentru cei care nu l-au citit, va încurajez calduros sa o faceti, este o piesa legislativa importanta pe care colegii nostri de la Comisia Europeana au propus-o împreuna cu co-legislatorii. Pentru început, CRA se aplica aproape tuturor. Daca vindeti sau cumparati produse pe piata unica digitala, pe piata unica în sine, toate componentele, toate produsele introduse trebuie sa respecte CRA. Va puteti imagina ca amploarea este uriasa. La început, acest lucru poate parea descurajant. Acesta este sentimentul pe care îl au multi. Lucram împreuna cu toate organismele din statele-membre si, bineînteles, cu actorii privati. Asadar, se depune multa munca acum pentru a veni cu îndrumari practice si implementari tehnice pentru a sprijini oamenii, în special IMM-urile, comunitatea open-source, dar si producatorii care trebuie sa introduca produse pe piata", a mentionat Malatras.

Acesta a adaugat ca termenul de implementare al Cyber Resilience Act, finele anului 2027, nu este chiar atât de departe iar oamenii trebuie sa înteleaga impactul pe care CRA îl va avea asupra lor, nu doar în termeni de conformitate ci si de securitate reala a produselor.

"Se lucreaza mult în cadrul organismelor de standardizare, cu toata lumea implicata activ, pentru a stabili standardele care vor trebui puse în aplicare pentru a asigura conformitatea produselor cu CRA. Cred ca unul dintre motivele pentru care am dorit sa organizam acest eveniment, în parteneriat, este sa începem sa crestem gradul de constientizare pentru toata lumea ca acest lucru nu se va întâmpla peste noapte. Oamenii trebuie sa înceapa sa se pregateasca. Trebuie sa înteleaga impactul pe care CRA îl va avea asupra lor. Dar nu doar în termeni de conformitate, pentru ca de obicei se gândeste la conformitate: exista o reglementare, trebuie sa ma conformez din cauza x, y, z sau pentru ca asa este scris undeva. Nu este vorba doar despre securitatea pe hârtie, iar acesta este mesajul pe care încercam sa îl transmitem. Este vorba despre securitatea reala a produselor. Documentul este acolo pentru a stabili o baza, astfel încât sa putem avea, pe întreaga piata unica, principii de baza ale securitatii cibernetice care vor ajuta ca produsele noastre sa fie sigure, sa fie competitive la scara globala si sa contribuie la depasirea diferitelor cazuri de vulnerabilitati pe care le-am întâlnit", a spus oficialul ENISA.

Potrivit sursei citate, crizele cibernetice se produc din cauza vulnerabilitatilor pe care le au anumite produse.

"În ultimii ani, am discutat mult despre crize cibernetice. Majoritatea acestor lucruri se întâmpla din cauza vulnerabilitatilor si incidentelor care apar în produse. Prin toata aceasta munca pregatitoare, prin aceasta abordare proactiva pentru a ne asigura ca produsele îndeplinesc cerintele minime de securitate, contribuim si la reducerea impactului advers potential. Facem acest lucru împreuna cu autoritatile de securitate cibernetica, cu autoritatile de supraveghere a pietei, cu actorii privati, cu IMM-urile care sunt coloana vertebrala a societatii europene. Cred ca obiectivul este clar: suntem cu totii dedicati lui si, foarte probabil, vom ajunge acolo unde trebuie", a subliniat Apostolos Malatras.

Cyber Resilience Act a fost adoptat de Comisia Europeana în octombrie 2024 si va deveni obligatoriu pentru producatori începând din decembrie 2027. Documentul stabileste un nivel minim de securitate cibernetica pentru

produsele conectate de pe piata europeana.

Producatorii au la dispozitie 36 de luni pentru a-si adapta produsele la noile cerinte, iar începând de la 11 decembrie 2027, toate produsele noi vor trebui sa respecte integral aceste reguli.

Noile reguli asigura: design securizat al produselor, protectie împotriva vulnerabilitatilor si suport pe întreg ciclul de viata al produsului (inclusiv actualizari si patch-uri de securitate). Aceste cerinte sunt aplicabile tuturor produselor digitale vândute în UE, fie ca sunt independente sau integrate în alte sisteme.

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).