Directiva NIS 2 reprezinta o necesitate în contextul cibernetic actual, nu doar o obligatie legala (analiza)

Transpunerea Directivei NIS 2 (Network and Information Security) în legislatia românească prin OUG 155/2024 marcheaza un moment definitoriu în eforturile locale de consolidare a rezilientei în fata amenintarilor cibernetice din ce în ce mai complexe, releva o analiza Deloitte România.

"Acest pas legislativ, parcurs pe fondul unui context geopolitic cu multe provocari si al unui peisaj al amenintarilor cibernetice în crestere, urmareste sa îmbunatateasca modul proactiv de gestionare a riscurilor, sa asigure continuitate operationala si sa pozitioneze România pe un loc fruntas în materie de securitate cibernetica", sustin autorii analizei, Raluca Anton, Cyber Strategy Senior Manager, si Octavian Popa, Cyber Strategy Manager de la Deloitte România.

Potrivit acestora, securitatea cibernetica a devenit un pilon fundamental al economiei si al stabilitatii functionale a serviciilor esentiale, România înregistrând deja progrese notabile în acest domeniu prin adoptarea de legislatie specifica, precum transpunerea primei versiuni a Directivei NIS prin Legea 362/2018, înfiintarea Directoratului National de Securitate Cibernetica prin OUG 104/2021 sau adoptarea Strategiei Nationale de Securitate Cibernetica a României prin HG 1321/2021, toate sub cupola Legii 58/2023 privind securitate si apararea cibernetica a României.

Cu toate acestea, ritmul accelerat al procesului de transformare digitala si complexitatea tot mai mare a atacurilor cibernetice au evidentiat necesitatea unui cadru extins si actualizat. Directiva NIS 2, în esenta, abordeaza vulnerabilitatile infrastructurilor critice si armonizeaza standardele de securitate cibernetica la nivelul Uniunii Europene, construind pe baza reglementarilor anterioare si remediind lacunele din gestionarea riscurilor si modul de raspuns la incidente, conform analizei.

"Directiva NIS 2 impune politici stricte pentru identificarea, atenuarea si gestionarea riscurilor de securitate cibernetica, organizatiile fiind obligate sa efectueze evaluari regulate ale riscurilor pentru potentialele vulnerabilitati, sa implementeze masuri adecvate pentru a aborda toata aceasta gama de riscuri de natura cibernetica si sa ramâna vigilente prin sisteme de monitorizare proactiva. Accentul pus pe managementul riscului se extinde dincolo de procedurile interne, incluzând si securitatea lanturilor de aprovizionare, vizând astfel vulnerabilitatile furnizorilor terti de servicii", se mentioneaza în analiza citata.

Existenta unui cadru robust pentru raportarea incidentelor de securitate cibernetica este un element central al Directivei NIS 2, considera specialistii Deloitte. Entitatile sunt obligate sa raporteze, fara întârzieri nejustificate, orice eveniment care are un impact semnificativ asupra prestarii serviciilor echipei de raspuns la incidente de securitate cibernetica la nivel national, fiind astfel asigurata o partajare rapida a informatiilor si o gestionare mai eficienta a incidentelor.

"Spre deosebire de Directiva NIS 1, pentru a carei implementare erau responsabili în principal reprezentantii desemnati din organizatie, NIS 2 transfera aceasta responsabilitatea catre echipa de top management. Echipa de conducere are acum obligatia de a aproba si de a supraveghea masurile de gestionare a riscurilor, dar si de a se asigura ca sunt alocate resurse adecvate pentru componenta de securitate cibernetica. De asemenea, membrii echipei de conducere trebuie sa participe la instruiri periodice în domeniul securitatii cibernetice, cum ar fi exercitii de simulare a crizelor de natura cibernetica, asigurându-se ca detin cunostintele necesare pentru a supraveghea eficient procesul de management al riscurilor", se mai spune în analiza Deloitte.

Ca urmare a implementarii noii directive, organizatiile sunt obligate sa adopte masuri stricte în ceea ce priveste dezvoltarea si implementarea planurilor de continuitate a afacerii în cazul unui incident major de securitate cibernetica, accentul fiind pus pe pregatirea si asigurarea continuitatii serviciilor esentiale.

Mai mult, noua directiva extinde domeniul de aplicabilitate prin includerea a 11 noi sectoare critice, printre care se numara energie, transporturi, sanatate, infrastructura digitala si financiar-bancar. Sectoarele precum serviciile postale, managementul deseurilor, productia chimica, cercetarea si productia, prelucrarea si distributia de alimente sunt integrate în reglementarea europeana, reflectând cresterea nivelului de constientizare în materie de amenintari de securitate cibernetica la adresa diverselor industrii ce sustin functionarea societatii.

"Prin accentul pus pe gestionarea riscurilor, transferul responsabilitatii privind supravegherea procesului de management al riscului catre echipa de top management, prevederile stricte de raportare a incidentelor, inclusiv cele care vizeaza lanturile de aprovizionare, transpunerea Directivei NIS 2 la nivel local impune o schimbare majora catre un model proactiv în materie de securitate cibernetica care reprezinta mai mult decât o obligatie legala. Pentru organizatii, masurile impuse de aceasta directiva, respectiv de textul legislativ transpus la nivel national, reprezinta o oportunitate în vederea gestionarii eficiente a riscurilor de natura cibernetica si a asigurarii continuitatii operatiunilor", încheie specialistii Deloitte analiza despre legislatia privind amenintarilor cibernetice.