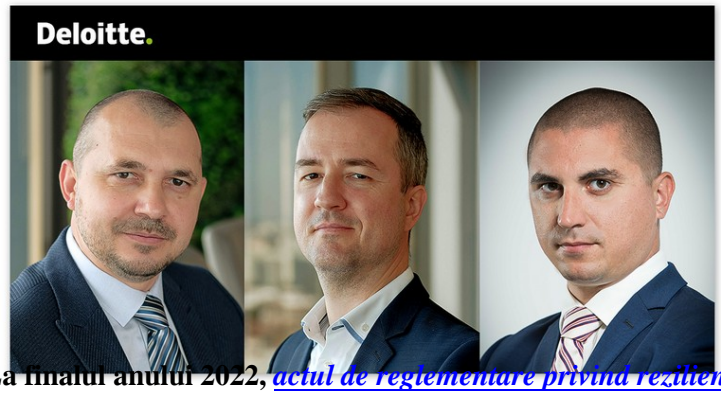
UE a adoptat DORA, un fel de GDPR al siguranței cibernetice pentru organizațiile din sectorul financiar. Ce presupune noul cadru de reglementare pentru echipele de management?



La finalul anului 2022, *actul de reglementare privind rezilienta operationala digitala (DORA)* a fost publicat în monitorul oficial al Uniunii Europene, intrând în vigoare începând cu 16 ianuarie 2023. Complexitatea efectelor DORA asupra domeniului siguranței cibernetice pentru organizațiile din sectorul financiar este comparabila cu ceea ce a însemnat GDPR pentru domeniul protecției datelor personale. DORA creeaza primul cadru legislativ care armonizeaza masurile de securitate cibernetica și de risc pentru toate entitațile din sectorul financiar, nu doar pentru banci, la nivel european.

Cei patru piloni prezentați în DORA

DORA are în vedere **patru piloni** pe care companiile din sectorul financiar trebuie sa îi ia în considerare pentru a înțelege maniera în care practicile lor privind tehnologia informației și comunicațiilor, reziliența operațională și cibernetica, dar și managementul riscurilor rezultate în urma colaborarii cu terți asigura continuitatea funcțiilor lor critice.

Primul pilon presupune crearea unui cadru de management al riscului în jurul unui set de principii și cerințe cheie în vederea **gestionarii riscului privind tehnologia informației și comunicațiilor**.

Al doilea pilon vizeaza modalitatea de **raportare a incidentelor**, entitațile financiare fiind nevoite sa notifice astfel de cazuri în 24 de ore de la producere. În decurs de o luna, organizația compromisa este nevoita sa identifice cauza primara a atacului folosind instrumente de detecție și raspuns implementate cu ajutorul echipelor operaționale care trebuie sa dea dovada de o serie de abilitați speciale în domeniu. Tehnologiile care pot sprijini procesele de detecție și raspuns sunt soluții cu care principalii jucatorii din sistemul bancar sunt cel mai probabil la zi, activând într-un sector deja puternic reglementat.

Testarea rezilienței operaționale reprezinta **al treilea pilon** pe care DORA îl reglementeaza, stabilind standarde la nivelul UE în vederea realizarii acestor exerciții. Companiile care au depașit un anumit prag de maturitate – prag care va fi specificat într-un standard tehnic de reglementare ce nu a fost înca adoptat - trebuie sa efectueze teste de securitate bazate pe informații despre amenințari cibernetice actuale (*Threat-Led Penetration Testing*) la fiecare trei ani, excepție facând cazurile în care aceste dispoziții sunt modificate de autoritațile naționale. În țara noastra, Banca Națională a României a adoptat cadrul TIBER-RO în mai 2022, care se aplica instituțiilor financiare pe care le supravegheaza. Acesta presupune testarea rezilienței cibernetice a companiilor din sectorul financiar la fiecare trei ani, iar cele care în prezent se pregatesc pentru implementarea regulamentului nr. 6/2022 privind cadrul de

desfășurare a testelor de reziliența cibernetica TIBER-RO pot avea încredere ca aceasta activitate le va fi utila în vederea respectarii cerințelor avansate de testare specificate de DORA.

În final, **al patrulea pilon** precizeaza necesitatea adoptarii unei strategii holistice în ceea ce privește gestionarea relației cu terții, care sa permita o monitorizare completa din partea companiei.

Implicații pentru echipele de conducere executiva

Odata cu DORA, un cadru de reglementare mult mai strict decât alte inițiative similare din zona de securitate cibernetica și care va beneficia de o vizibilitate mai mare la nivel european, se observa o schimbare de paradigma în ceea ce privește implementarea cerințelor, membrii echipelor de conducere executiva din sectorul financiar având un rol mult mai specific în acest sens. Astfel, aceștia vor fi nevoiți sa aprobe un set de planuri cheie, cum ar fi strategia de reziliența operațională digitala a companiei și politica acesteia privind terții.

De asemenea, echipele de conducere trebuie sa fie instruite și pregatite astfel încât sa înțeleaga gradul de maturitate a organizației din perspectiva capacității de a face față potențialelor crize cibernetice și întreruperi majore care țin de tehnologia informației și comunicațiilor. Directorii executivi mai trebuie sa știe și în ce masura compania poate asigura continuitatea serviciilor critice în fața acestor provocari. În acest sens, companiile pot opta pentru organizarea periodica a *exercițiilor de simulare a unor potențiale atacuri cibernetice*, care ajuta la exersarea capacității de raspuns la criza din perspectiva comunicarii cu angajații, presa, autoritățile sau din cea juridica.

Un alt aspect de care managementul unei companii trebuie sa țina cont este modalitatea în care DORA va afecta colaborarea cu terții. Astfel, este probabil ca directorii executivi sa fie nevoiți sa regândeasca deciziile strategice în privința partenerilor și sa revizuiasca rolul departamentelor de risc și achiziții.

Pe scurt, DORA va obliga managementul sa devina un actor activ în procesul decizional care asigura reziliența cibernetica a organizației.

Deși direcțiile și conceptele pe care DORA le propune nu sunt noi, ele fiind deja introduse în unele directive și ghiduri de specialitate, implementarea cadrului va aduce în prim plan o serie de provocari pentru directorii executivi din sectorul financiar care, pâna în acest moment, se aflau preponderent pe lista de prioritați a directorilor de securitate a informațiilor (*chief information security officer* - CISO) sau a directorilor de tehnologie (*chief technology officers* - CTO). Companiile trebuie sa aplice prevederile DORA din 17 ianuarie 2025, așadar au la dispoziție o perioada generoasa pentru a se pregati, dar este important sa aiba în vedere ca aceste cerințe nu fac parte dintr-un exercițiu unic de conformare, ci dintr-un proces continuu, care le va ajuta sa ramâna în siguranța într-un peisaj al amenințarilor cibernetice aflat în plina evoluție.