Studiu Deloitte: organizațiile din domeniul serviciilor financiare încep sa înregistreze progrese în implementarea noului regulament UE privind reziliența operațională digitala, DORA

Organizațiile active în industria serviciilor financiare încep sa înregistreze progrese semnificative în implementarea modificarilor menite sa asigure conformarea cu noul regulament UE Legea privind reziliența operațională digitala (*Digital Operational Resilience Act* - DORA), în contextul în care o treime dintre acestea (29%) au început sa se pregateasca încă din 2022 și, dintre acestea, 29% au finalizat deja, până în februarie 2023, 75% din pașii de implementare planificați, conform celei mai recente ediții a studiului Deloitte despre DORA. Intrata în vigoare în 2023, DORA este cea mai importanta inițiativa de reglementare a UE privind reziliența operațională și securitatea cibernetica în sectorul serviciilor financiare și impune organizațiilor sa implementeze modificari specifice în termen de 24 de luni de la adoptarea sa.

Toți cei patru piloni ai DORA – gestionarea riscurilor legate de tehnologia informației și comunicații (TIC), raportarea incidentelor, testarea operațională și de reziliența digitala, precum și managementului riscului generat de furnizorii TIC – genereaza la fel de multe provocari entităților din domeniul financiar, subliniaza studiul, însa o treime dintre respondenți (33%) menționeaza ca al patrulea este cel mai greu de respectat. Raportul evidențiaza faptul ca companiile sunt în urma în ceea ce privește evaluarea riscului generat de terți, în condițiile în care șapte din zece organizații participante la studiu (69%) le efectueaza doar o data pe an, insuficient pentru a respecta cerințele DORA, în timp ce doar 13% le efectueaza în mod continuu, așa cum cere noul regulament. Respectarea acestor cerințe implica, de asemenea, revizuirea periodica a strategiei privind riscul generat de furnizorii de soluții TIC, luând în considerare strategia de a distribui serviciile pe furnizori multipli. O astfel de abordare va fi o provocare pentru jucatorii din industria serviciilor financiare, deoarece 29% dintre respondenți încă își definesc o strategie holistica privind colaborarea cu mai mulți furnizori de soluții de tehnologia informației și comunicații, iar 21% dintre ei vor trebui sa și-o actualizeze până în 2025, pentru ca au definit-o mai devreme de 2022.

Înțelegerea gradului de interconectare dintre furnizorii de soluții TIC și cei de soluții de tehnologie considerate critice este, de asemenea, una dintre provocarile cu care organizațiile se pot confrunta pe parcursul implementarii DORA. Patru din zece instituții financiare participante la studiu (43%) au menționat ca nu au demarat încă acest proces care susține funcțiile critice și importante ale companiei. Studiul evidențiaza faptul ca funcțiile considerate critice și importante sunt autorizarea (14%) și autentificarea tranzacțiilor de plata (12%), urmate de operațiunile IT și tranzacțiile efectuate de clienți prin intermediul canalelor digitale (12% fiecare).

„Pentru a se conforma cerințelor DORA, organizațiile vor fi nevoite sa faca o clasificare a funcțiilor critice sau importante, a caror întrerupere le-ar afecta rezultatele financiare și continuitatea serviciilor, dar și sa-și actualizeze constant lista acestor funcții și sa le identifice de-a lungul întregului lanț al furnizorilor de servicii de tehnologia informației și comunicații, critice sau nu, astfel cum sunt definite în Standardele Tehnice de Reglementare, care vor intra în curând în vigoare. În plus, instituțiile financiare vor trebui sa dezvolte metode de testare a scenariilor de reziliența și strategii multi-furnizor pentru toate sistemele care susțin funcții critice și importante”, a declarat **Sergiu Zaharia, Director Cyber Strategy Advisory, Deloitte România.**

DORA impune, de asemenea, instituțiilor financiare sa efectueze anual teste ale planului de raspuns la incidente. Patru din zece respondenți

(36%) au efectuat astfel de exerciţii în ultimele 12 luni, testând funcţiile critice şi pe cele importante, în timp ce 64% nu au efectuat astfel de teste în ultimele 12 luni.

Având în vedere cerinţele DORA, organizaţiile financiare vor trebui, de asemenea, sa efectueze teste de penetrare bazate pe ameninţari (TLPT) asupra tuturor sistemelor şi aplicaţiilor TIC critice şi asupra funcţiilor importante, în mediul de producţie. Jumatate dintre entitaţile financiare chestionate au efectuat astfel de teste, iar restul au testat doar în mediu non-live. Instituţiile financiare prefera sa efectueze teste de penetrare bazate pe ameninţari utilizând un mix de echipe interne şi de consultanţi, 57% dintre respondenţi având experţi angajaţi de *Blue Team*, responsabili de asigurarea eficienţei masurilor de securitate din cadrul unei organizaţii, în timp ce rolurile de *Red Team*, care vizeaza încercarea de intruziune fizica sau digitala într-o organizaţie, şi cele de *Purple Team*, o combinaţie între echipele *Blue* şi *Red*, sunt acoperite de consultanţi externi.

Ce mai recenta ediţie a studiului Deloitte privind DORA sondeaza opiniile directorilor de securitate a informaţiei (CISO), a directorilor IT (CIO), a managerilor de risc operaţional, de risc IT şi de risc (CRO) din instituţii financiare din 20 de ţari din Europa. Raportul îşi propune sa înţeleaga cât de pregatite sunt instituţiile financiare pentru implementarea modificarilor impuse de DORA, precum şi care sunt provocarile asociate cu care se confrunta aceste instituţii.

Echipa de securitate cibernetica a Deloitte România este specializata în oferirea de **servicii de strategie**, incluzând exerciţii de simulare a crizelor cibernetice şi evaluari holistice ale nivelului de maturitate cibernetica de tip *deep dive*, **servicii de aparare**, inclusiv managementul identitaţii şi accesului, operaţiuni de securitate, procese şi tehnologii de pregatire şi de raspuns la incidente, precum şi **servicii de atac**, vizând în special efectuarea de teste de penetrare, precum exerciţiile de tip *red-teaming* (TIBER-EU).

Echipa locala contribuie activ la cele mai importante exerciţii cibernetice organizate în România. În ultimii ani, Deloitte România a fost una dintre puţinele organizaţii private selectate pentru a participa, alaturi de Ministerul Apararii Naţionale, la exerciţiile anuale organizate de NATO. În 2022, echipa Deloitte a participat la unul dintre cele mai mari exerciţii de securitate cibernetica organizate în România de Centrul Naţional CYBERINT din cadrul Serviciului Român de Informaţii. În plus, experţii locali în securitate cibernetica, care deţin zeci de certificari de specialitate, ofera cursuri şi certificari recunoscute internaţional prin intermediul Deloitte Academy, divizia de formare profesionala a Deloitte România. Deloitte este şi centru oficial autorizat de training în România pentru Consiliul Internaţional de Consultanţi în E-Commerce, cunoscut şi ca EC-Council.

La nivel global, pentru al unsprezecelea an consecutiv, Gartner a clasat Deloitte pe poziţia de lider în servicii de consultanţa în securitate dupa cota de piaţa.