Raport PwC: Riscurile cibernetice sunt prioritizate de numai un sfert dintre companiile din ECE față de jumatate la nivel global

Companiile din Europa Centrala și de Est (ECE), inclusiv din România, prioritizeaza riscurile "tradiționale", adica instabilitatea economica, situația geopolitica și volatilitatea macroeconomica, în detrimentul celor digitale, tehnologice sau cibernetice (cum ar fi ransomware, piraterie și urmarire), conform studiului PwC 2024 Digital Trust Insights Survey. Doar 27% dintre companiile din ECE prioritizeaza riscurile digitale și tehnologice, fața de 51% la nivel global, iar 37% acorda o importanța ridicata riscurilor cibernetice, fața de 43%. În schimb 47% dintre respondenți considera volatilitatea macroeconomica o prioritate (vs 41% la nivel global).

"Deși le considera îngrijoratoare și cu impact puternic asupra operațiunilor, companiile din regiunea noastra, inclusiv cele românești, înca nu prioritizeaza riscurile digitale, tehnologice și cibernetice. Totuși, în ultimii ani, au facut pași importanți în creșterea securității cibernetice și a investițiilor alocate în acest scop. Bugetele însa vor trebui sa creasca, atat în contextul creșterii numarului și complexității atacurilor cibernetice cat și în contextul normelor Uniunii Europene pentru consolidarea rezilienței infrastructurilor critice la o serie de amenințari, care cresc exigența sistemelor de securitate ale companiilor", a declarat **Mircea Bozga**, *Partener de Auditul Riscului, PwC România.*

În evaluarea amenințarilor cibernetice care provoaca îngrijorare în urmatoarele 12 luni, cele mai multe companii din ECE (44%) menționeaza operațiunile de hack-and-leak, comparativ cu media globala de 37%, evidențiind accentul regional pe protecția datelor.

Consecințele unui atac cibernetic care îi îngrijoreaza pe cei mai mulți respondenți din ECE (54%) se refera la pierderea datelor despre clienți, angajați sau tranzacții, aproape de media globala de 52%. Preocuparile legate de daunele aduse brandului companiei, inclusiv pierderea încrederii clienților, sunt aproape identice, cu 49% în ECE și 50% în media globala.

Creșterea bugetului de investiții, o necesitate

La nivel de buget, companiile din Europa Centrala și de Est par sa caute modalități de creștere a investițiilor în securitate cibernetica. În acest moment, exista discrepanțe și investiții inegale în soluții, instrumente și formare de securitate cibernetica.

Doar 7% dintre respondenți (vs 10% la nivel global) se așteapta la o creștere substanțiala a bugetului de investiții, de peste 15%, iar 21% dintre organizații estimeaza o majorare de 6-10% a bugetului (vs 31% global). În același timp, 23% dintre respondenții din regiune intenționeaza sa își mențina bugetele cibernetice neschimbate, spre deosebire de 9% la nivel global și în Europa de Vest.

Interesant este ca un numar considerabil mai mare de participanți din ECE au raportat o lipsa de conștientizare cu privire la bugetul cibernetic.

În urmatoarele 12-18 luni, companiile din regiune vor pune un accent mai mare pe securitatea rețelelor (40%), depașind media globala de 28%, astfel indicând un angajament puternic pentru întarirea infrastructurii de baza. În plus, organizațiile acorda prioritate securității în cloud la 34% și gestionarii identității și accesului (30%) într-o masura puțin mai mare decât omologii la nivel mondial, 33% și, respectiv, 21%.

Tot la categoria bugete, majoritatea companiilor din ECE se așteapta la creșterea costurilor de conformitate (la

nivel global: 75%). În general, în Uniunea Europeana exista un focus destul de mare pe acest aspect, având în vedere cerințele NIS2 / DORA / Cyber Resilience Act, care solicita un nivel ridicat de maturitate si transparența privind practicile cibernetice.

Codași la utilizarea AI în detectarea amenințarilor cibernetice

Inovația se concentreaza pe detectarea mai buna a amenințarilor cibernetice existente și îmbunatațirea funcțiilor de securitate pentru a compensa lipsa specialiștilor și a optimiza costurile. Când vorbim despre inovație, inteligența artificiala joaca un rol important în lupta contra atacurilor cibernetice. Regiunea ECE ramâne în urma mediei mondiale în ceea ce privește implementarea inițiativelor de securitate cibernetica și realizarea beneficiilor acestora.

Utilizarea Large Language Models (LLM) și a inteligenței artificiale generative în detectarea și reducerea riscurilor se situeaza la doar 9%, spre deosebire de 21% la nivel global. În plus, 20% dintre respondenții din ECE nu au planuri de implementare a acestor inițiative, spre deosebire de 7% dintre respondenții la nivel mondial.