

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

Companiile din Europa Centrala și de Est (ECE), inclusiv din România, prioritizează riscurile “tradiționale”, adică instabilitatea economică, situația geopolitică și volatilitatea macroeconomică, 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 prioritizează riscurile digitale și tehnologice, față de 51% la nivel global, iar 37% acorda o importanță ridicată riscurilor cibernetice, față de 43%. În schimb 47% dintre respondenți considera volatilitatea macroeconomică o prioritate (vs 41% la nivel global).

“Deși le considera îngrijorătoare și cu impact puternic asupra operațiunilor, companiile din regiunea noastră, inclusiv cele românești, încă nu prioritizează riscurile digitale, tehnologice și cibernetice. Totuși, în ultimii ani, au făcut pași importanți în creșterea securității cibernetice și a investițiilor alocate în acest scop. Bugetele însă vor trebui să crească, atât în contextul creșterii numărului și complexității atacurilor cibernetice cât și în contextul normelor Uniunii Europene pentru consolidarea rezilienței infrastructurilor critice la o serie de amenințări, care cresc exigența sistemelor de securitate ale companiilor”, a declarat **Mircea Bozga, Partener de Auditul Riscului, PwC România.**

În evaluarea amenințărilor cibernetice care provoacă îngrijorare în următoarele 12 luni, cele mai multe companii din ECE (44%) menționează operațiunile de hack-and-leak, comparativ cu media globală de 37%, evidențiind accentul regional pe protecția datelor.

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

Creșterea bugetului de investiții, o necesitate

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

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

Interesant este că un număr considerabil mai mare de participanți din ECE au raportat o lipsă de conștientizare cu privire la bugetul cibernetic.

În următoarele 12-18 luni, companiile din regiune vor pune un accent mai mare pe securitatea rețelelor (40%), depășind media globală de 28%, astfel indicând un angajament puternic pentru întărirea infrastructurii de bază. În plus, organizațiile acorda prioritate securității în cloud la 34% și gestionării identității și accesului (30%) într-o măsură puțin mai mare decât omologii la nivel mondial, 33% și, respectiv, 21%.

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

nivel global: 75%). În general, în Uniunea Europeană există un focus destul de mare pe acest aspect, având în vedere cerințele NIS2 / DORA / Cyber Resilience Act, care solicită un nivel ridicat de maturitate și transparență privind practicile cibernetice.

Codași la utilizarea AI în detectarea amenințărilor cibernetice

Inovația se concentrează pe detectarea mai bună a amenințărilor cibernetice existente și îmbunătățirea funcțiilor de securitate pentru a compensa lipsa specialiștilor și a optimiza costurile. Când vorbim despre inovație, inteligența artificială joacă un rol important în lupta contra atacurilor cibernetice. Regiunea ECE rămâne în urma mediei mondiale în ceea ce privește implementarea inițiativelor de securitate cibernetică și realizarea beneficiilor acestora.

Utilizarea Large Language Models (LLM) și a inteligenței artificiale generative în detectarea și reducerea riscurilor se situează 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.