

Raport PwC: 72% dintre directorii generali din ECE anticipeaza cresterea criminalitatii cibernetice în 2022

Aproape trei sferturi (72%) dintre directorii generali din Europa Centrala si de Est (ECE), inclusiv din România, anticipeaza cresterea criminalitatii cibernetice în 2022, în conditiile în care anul trecut a fost unul dintre cei mai dificili din istorie în materie de securitate cibernetica, reiese din editia pentru Europa Centrala si de Est (ECE) a studiului "PwC 2022 Digital Trust Insights".

Comparativ, în EMEA (Europa, Orientul Mijlociu si Africa) sau la nivel global, doar 60% dintre directorii executivi se asteapta la o majorare a criminalitatii cibernetice, diferenta explicându-se prin maturitatea ecosistemelor de securitate cibernetica.

În ECE, desi majoritatea companiilor au crescut investitiile în securitatea cibernetica si în protectia datelor, doar 20% spun ca au vazut beneficii pâna în prezent, ceea ce ridica întrebarea cum ar trebui alocate investitiile viitoare pentru a fi eficiente.

"Datele raportului arata ca exista un grad înalt de constientizare a faptului ca riscurile de securitate cibernetica se afla în crestere. Totodata, organizatiile înțeleg ca exista provocari tot mai mari atunci când vor sa câștige încrederea clientilor si a altor parteneri de afaceri ca datele lor vor fi protejate. În aceste conditii investitiile în securitate cibernetica au crescut, dar în lipsa unei strategii coerente de adoptare si implementare a tehnologiilor, rezultatul a fost, de multe ori, doar o mai mare complexitate în cadrul organizatiilor, fara beneficii vizibile ale alocarii acestor fonduri. Din pacate, complexitatea ridicata amplifica riscurile cibernetice", a declarat Mircea Bozga, Partener Risk Assurance PwC România.

Astfel, aproximativ jumătate dintre respondentii din ECE confirma ca o complexitate organizationala mare genereaza riscuri cibernetice si de confidentialitate, iar guvernanta datelor (64%) si cloud-ul (63%) ocupa primele locuri în acest sens. Procentul este mai ridicat la nivel global, aproape trei sferturi dintre respondenti aratând ca o complexitate organizationala mare genereaza riscuri de securitate si de confidentialitate.

Obiceiurile organizationale riscante includ: folosirea mai multor solutii tehnologice care nu functioneaza împreuna si nerespectarea proceselor de gestionare a datelor sau a riscurilor cu terte parti.

Potrivit sursei citate, fara o atentie concentrata asupra simplificarii ecosistemelor cibernetice, organizatiile pot deveni vulnerabile, iar consecintele se vor propaga la nivelul tuturor operatiunilor unei organizatii.

"Atunci când vorbim despre securitate cibernetica simplificata, adoptarea mai multor solutii tehnologice reprezinta doar o parte din solutie. Este însa necesara o strategie unitara, care sa implice toata organizatia - tehnologia, procesele, echipele si managementul, aliniata la obiectivele de business si care va consolida rezilienta la orice tip de perturbari", a aratat Robert Girdoc, Senior Manager Risk Assurance PwC România.

În comunicatul companiei se mentioneaza ca principala consecinta a complexitatii cibernetice în ECE este "lipsa rezilientei operationale sau incapacitatea de recuperare dupa un atac cibernetic sau un esec tehnologic". Aceasta este urmat de incapacitatea de a retine talentele si pierderile financiare generate de bresele de securitate sau de atacuri cibernetice.

Întrebat unde își vor orienta cheltuielile pentru a simplifica securitatea cibernetica, respondentii din ECE au declarat ca se vor concentra mai mult pe rationalizarea tehnologiei si restructurarea echipelor de securitate, urmate de introducerea controalelor la nivelul proceselor si reducerea folosirii tehnologiilor învechite.

Digital Trust Insights Survey 2022 ECE face parte Global Digital Trust Insights 2022 si a fost efectuat în rândul companiilor din Polonia, Cehia, Ungaria, România, Kazahstan, Ucraina, Croatia, Bulgaria si Letonia.