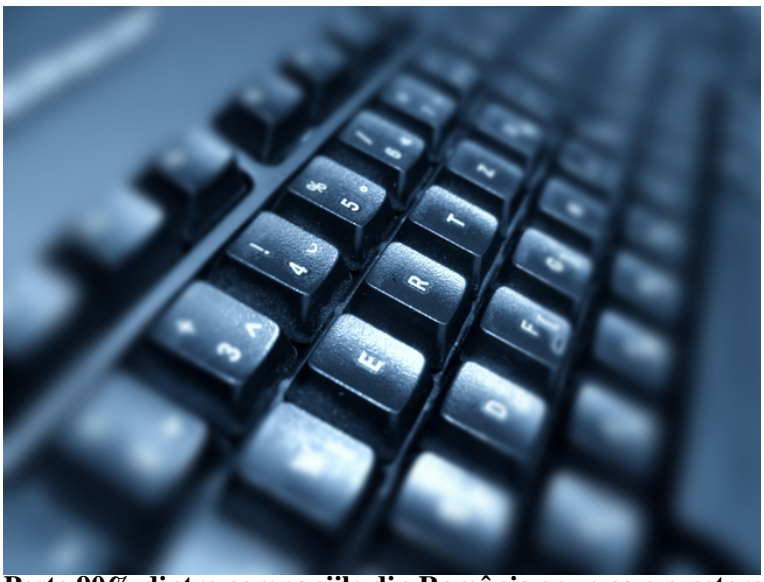
Sondaj EY România: Marile companii locale vor face investitii pentru a se proteja de atacuri cibernetice si impactul lor asupra datelor financiar-fiscale



Peste 90% dintre companiile din România spun ca o creștere a incidenței atacurilor informatice le poate perturba serios activitatea. Un procent de 72% dintre acestea au un departament intern specializat sau un partener extern care sa previna exploatarea rețelelor lor în urma unui atac informatic. Aproape jumatate dintre companii (46%) spun, însa, ca au arii care nu sunt acoperite sau nu sunt suficient protejate de atacurile hackerilor.

Acestea sunt principalele concluzii rezultate în urma unui sondaj *Tax & Cyber*, derulat recent de EY pe piața locala, care arata directia în care marile companii din România au în vedere sa se orienteze în perioada urmatoare în privința masurilor de securitate cibernetica. Companiile respondente la acest sondaj au peste 100 de angajati, iar 77% dintre ele au cifra de afaceri de peste 10 milioane de euro, domeniile de activitate din care provin incluzând 16 zone, între care industria producatoare, agricultura, industria petroliera, constructii, bunuri de larg consum, transport, servicii financiare etc.

Din punct de vedere al organizarii functiei fiscale, 67% dintre respondenți au mentionat ca este organizata intern (ca departament sau echipa specializata).În mod continuu si chiar mai accentuat în ultima perioada, organizatiile globale redefinesc functia fiscala pentru a beneficia de avantajele tehnologiei digitale si cloud, fiind concentrate pe managementul datelor ca un factor cheie. Desigur, un semn de întrebare ramâne în ce priveste impactul atacurilor informatice asupra acuratetii datelor fiscale. Este normal sa existe aceasta întrebare la nivelul contribuabililor deoarece, odata cu digitalizarea accelerata post-pandemica, a crescut semnificativ si numarul atacurilor informatice. Asadar, iata ca o concluzie la care contribuabilii au ajuns (nu benevol, din pacate) este ca domeniul fiscal poate fi o sursa de date interesante, vulnerabil la atacurile informatice.

Rezultatele sondajului arata de asemenea ca, mai ales în aceasta perioada în care atacurile cibernetice s-au înmulțit semnificativ, firmele trebuie sa acorde atenție și acestei zone și sa deblocheze resursele financiare necesare realizarii investițiilor pentru consolidarea propriei securitați cibernetice. 57% dintre respondentii la sondaj au declarat ca urmaresc cresterea investitiilor pentru îmbunatațirea protecției împotriva atacurilor informatice, iar 28% doresc sa îmbunatateasca masurile existente. Pe de alta parte, însa, restul respondentilor declara fie ca nu au resursele financiare necesare, fie considera ca au implementat deja suficiente masuri sau ca le vor avea în vedere în cazul unui atac informatic.

Clarisa Tesu, *Partener, Forensic & Integrity Services, EY România*: „Odata cu digitalizarea informatiilor fiscale, vine si o crestere semnificativa a expunerii acestor informatii la potentiale atacuri, care pot atrage sancţiuni de la anumite autoritaţi sau procese lungi si costisitoare. Implementarea unor soluţii de Data Loss Prevention - de prevenire şi oprire a exfiltrarii de date informatice - si definirea unui plan de raspuns la incidente informatice sunt esentiale pentru a identifica, stopa si raspunde prompt unui astfel de atac, dar si pentru a proteja datele sensibile si confidenţiale ale companiei."

Doar 38% dintre cei care au raspuns sondajului considera ca toate datele sunt vulnerabile în cazul unui atac informatic, restul respondentilor fiind preocupati cel mai mult de datele financiare (inclusiv cele fiscale), urmate de cele comerciale si, într-o mai mica masura, de cele care tin de resurse umane si de juridic.

„Atacurile informatice sunt foarte frecvente, puţine sunt companiile care sa nu se fi confruntat cu vreun incident informatic în ultimele 12 luni. De cele mai multe ori, asa cum s-a vazut în practica, acestea au şi un impact asupra business-ului. Le recomandam contribuabililor sa îşi protejeze calitatea datelor fiscale, nu doar sa se asigure ca departamentul specializat sau partenerul extern cu care colaboreaza efectueaza niste sarcini de rutina", declara **Andra Caşu**, *Partener, Liderul Departamentului de Impozite Directe, EY România.*

Sunt înca multe companii (de dimensiuni mari sau mici) care ignora riscurile fiscale care pot aparea odata cu modificarea unor date fiscale printr-un atac informatic. Spre exemplu, se pot petrece modificari în contul de profit şi pierdere, ceea ce înseamna un rezultat fiscal denaturat, adica plata unei sume complet diferite. Cu alte cuvinte, orice intervenţie asupra datelor poate veni la pachet cu un risc profesional şi reputaţional deloc de neglijat.

De asemenea, ar trebui acordata o atenţie sporita lizibilitaţii datelor, pentru ca pot aparea denaturari importante, care pot afecta contribuabilii. Aici marea majoritate a respondenţilor (80%) la sondajul EY România considera ca detine toate documentele si informatiile într-un format lizibil, ceea ce este un semnal pozitiv în ceea ce priveste calitatea datelor fiscale.

Nu în ultimul rând, e de avut în vedere faptul ca orice inspecţie fiscala presupune examinarea documentelor aflate în dosarul fiscal al contribuabilului. Astfel, în cadrul sondajului, 40% din respondenti au declarat ca au fost subiectul unei inspectii fiscale generale, în timp ce 24% au avut o inspectie partiala sau un control inopinat. Cu toate acestea, ramâne un segment de 36% dintre contribuabilii respondenti, care înca nu au facut obiectul unei inspectii fiscale.

Având în vedere cele de mai sus, este clar ca pericolele cibernetice pot avea impact semnificativ din punct de vedere financiar-fiscal. De aceea, companiile trebuie sa acorde o atentie deosebita acestui aspect, pentru a identifica în timp util potentialele consecinte negative. Poate fi vorba, pe de o parte, de o revizuire interna a proceselor si a gradului intern de pregatire a personalului în domeniul riscurilor cibernetice, dar si de specializarea zonelor de automatizare în domeniul financiar-fiscal, pentru a evita orice expuneri ulterioare generate de afectarea datelor.