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

Peste 90% dintre companiile din România spun că 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 să prevină exploatarea rețelelor lor în urma unui atac informatic. Aproape jumătate dintre companii (46%) spun însă că 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 locală, care arată direcţia în care marile companii din România au în vedere să se orienteze în perioada următoare în privința măsurilor de securitate cibernetică. Companiile respondente la acest sondaj au peste 100 de angajaţi, 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 producătoare, agricultură, industria petrolieră, construcţii, bunuri de larg consum, transport, servicii financiare etc. Din punct de vedere al organizării funcţiei fiscale, 67% dintre respondenți au menţionat că este organizată intern (ca departament sau echipă specializată). În mod continuu şi chiar mai accentuat în ultima perioadă,

organizaţiile globale redefinesc funcţia fiscală pentru a beneficia de avantajele tehnologiei digitale şi cloud, fiind concentrate pe managementul datelor ca un factor cheie. Desigur, un semn de întrebare rămâne în ce priveşte impactul atacurilor informatice asupra acurateţii datelor fiscale. Este normal să existe această întrebare la nivelul contribuabililor deoarece, odată cu digitalizarea accelerata post-pandemică, a crescut semnificativ şi numărul atacurilor informatice. Aşadar, iată că o concluzie la care contribuabilii au ajuns (nu benevol, din păcate) este că domeniul fiscal poate fi o sursă de date interesante, vulnerabil la atacurile informatice.

Rezultatele sondajului arată de asemenea că, mai ales în această perioadă în care atacurile cibernetice s-au înmulțit semnificativ, firmele trebuie să acorde atenție și acestei zone și să deblocheze resursele financiare necesare realizării investițiilor pentru consolidarea propriei securități cibernetice. 57% dintre respondenţii la sondaj au declarat că urmăresc creşterea investiţiilor pentru îmbunătățirea protecției împotriva atacurilor informatice, iar 28% doresc să îmbunătăţească măsurile existente. Pe de altă parte însă, restul respondenţilor declară fie că nu au resursele financiare necesare, fie consideră că au implementat deja suficiente măsuri sau că le vor avea în vedere în cazul unui atac informatic.

**Clarisa Tesu, Partener, Forensic & Integrity Services, EY România:** *„Odată cu digitalizarea informaţiilor fiscale, vine şi o creştere semnificativă a expunerii acestor informaţii la potenţiale atacuri, care pot atrage sancțiuni de la anumite autorități sau procese lungi şi costisitoare. Implementarea unor soluții de Data Loss Prevention – de prevenire și oprire a exfiltrării de date informatice – şi definirea unui plan de răspuns la incidente informatice sunt esenţiale pentru a identifica, stopa şi răspunde prompt unui astfel de atac, dar şi pentru a proteja datele sensibile şi confidențiale ale*

*companiei*”.

Doar 38% dintre cei care au răspuns sondajului consideră că toate datele sunt vulnerabile în cazul unui atac informatic, restul respondenţilor fiind preocupaţi cel mai mult de datele financiare (inclusiv cele fiscale), urmate de cele comerciale şi, într-o mai mică măsură, de cele care ţin de resurse umane şi de juridic.

„*Atacurile informatice sunt foarte frecvente, puține sunt companiile care să nu se fi confruntat cu vreun incident informatic în ultimele 12 luni. De cele mai multe ori, aşa cum s-a văzut în practică, acestea au și un impact asupra business-ului. Le recomandăm contribuabililor să își protejeze calitatea datelor fiscale, nu doar să se asigure că departamentul specializat sau partenerul extern cu care colaborează efectuează nişte sarcini de rutină*”, declară **Andra Cașu, Partener, Liderul Departamentului de Impozite Directe, EY România**.

Sunt încă multe companii (de dimensiuni mari sau mici) care ignoră riscurile fiscale care pot apărea odată cu modificarea unor date fiscale printr-un atac informatic. Spre exemplu, se pot petrece modificări în contul de profit și pierdere, ceea ce înseamnă un rezultat fiscal denaturat, adică plata unei sume complet diferite. Cu alte cuvinte, orice intervenție asupra datelor poate veni la pachet cu un risc profesional și reputațional deloc de neglijat.

De asemenea, ar trebui acordată o atenție sporită lizibilității datelor, pentru că pot apărea denaturări importante, care pot afecta contribuabilii. Aici marea majoritate a respondenților (80%) la sondajul EY România consideră că deţine toate documentele şi informaţiile într-un format lizibil, ceea ce este un semnal pozitiv în ceea ce priveşte calitatea datelor fiscale.

Nu în ultimul rând, e de avut în vedere faptul că orice

inspecție fiscală presupune examinarea documentelor aflate în dosarul fiscal al contribuabilului. Astfel, în cadrul sondajului, 40% din respondenți au declarat că au fost subiectul unei inspecții fiscale generale, în timp ce 24% au avut o inspecție parțială sau un control inopinat. Cu toate acestea, rămâne un segment de 36% dintre contribuabilii respondenți, care încă nu au făcut obiectul unei inspecții fiscale.

Având în vedere cele de mai sus, este clar că pericolele cibernetice pot avea impact semnificativ din punct de vedere financiar-fiscal. De aceea, companiile trebuie să acorde o atenţie deosebită acestui aspect, pentru a identifica în timp util potenţialele consecinţe negative. Poate fi vorba, pe de o parte, de o revizuire internă a proceselor şi a gradului intern de pregătire a personalului în domeniul riscurilor cibernetice, dar şi de specializarea zonelor de automatizare în domeniul financiar-fiscal, pentru a evita orice expuneri ulterioare generate de afectarea datelor.