Cybertax: Cum să îți crești protecția datelor și a informațiilor fiscale în șapte pași

Autori:

Andra Caşu, Partener Asociat, Liderul Departamentului de Consultanță Fiscală în Impozite Directe, EY România

Răzvan Tufiș, Manager, Servicii de Investigație și Analiză Criminalistică Cibernetică, EY România

La fiecare 39 de secunde, undeva, pe net, se petrece un atac informatic. În fiecare zi, mai bine de 30.000 de site-uri sunt sparte, în condițiile în care lockdown-ul a crescut cu peste 600% rata de *cybercrime*. Iar atacul poate veni de acolo de unde te aștepți mai puțin, de exemplu: cinci din cele șapte milioane de bulgari aflați în baza de date a Fiscului din țara vecină s-au trezit în 2019 cu datele furate după un atac al hackerilor; Serviciul de Taxe și Impozite Tulcea a fost blocat vreme de două zile din cauza unui atac informatic; în timpul perioadei de declarare a impozitelor din 2018, IRS (fiscul american) a primit 234 de rapoarte despre posibile furturi de date, în creștere cu 29% față de numărul celor primite în același interval cu un an înainte. Deși considerat poate de mulți ca anost, domeniul fiscal este o sursă de date interesante, vulnerabil la atacurile informatice.

Există diverse tipuri de companii care produc sau gestionează informații legate de impozite, care sunt expuse riscului: bănci, companii ipotecare, firmele de investiții și valori mobiliare, cu alte cuvinte, orice companie plătitoare de salarii și beneficii către angajați. Cum statisticile globale din IT arată că doar 5% din totalul fișierelor utilizate în cadrul unei companii sunt complet securizate, nu putem ignora că tocmai unul dintre cele mai importante departamente, care deține unele dintre cele mai sensibile și vitale informații, ar putea fi vizat de hackeri.

Când se poate petrece un atac informatic în zona taxelor și impozitelor? Practic, cam tot timpul: și când îți îndeplinești obligațiile de raportare, și când îți evaluezi situația fiscală în timpul unei tranzacții, și când îți analizezi

documentele fiscale, pentru a depista potențialele riscuri, ba chiar și atunci când completezi declarațiile cerute de organismele internaționale, în număr din ce în ce mai mare. Mai mult, poate ar trebui să ne dea de gândit faptul că transparența va fi noua normă în fiscalitate, cu un volum în creștere de date de comunicat instituțiilor internaționale sau locale, ceea ce pentru hackeri ar putea însemna un număr sporit de ocazii.

O cifră schimbată, și balanța arată diferit. Eventuale modificări în contul de profit și pierdere, și ai un rezultat fiscal denaturat, pentru care poți să ajungi să plătești un impozit mai mic sau, dimpotrivă, mai mare. Dar un impozit micșorat, cu suma diminuată printr-un atac informatic te poate duce departe, chiar și până în zona evaziunii fiscale. La fel și o tranzacție nedeclarată, „omisă" din vina denaturării unui fișier. Cu alte cuvinte, o modificare banală a unor date și informații fiscale te poate plasa într-o zonă de risc fiscal și reputațional.

Cum 2021 a venit cu versiuni mai evoluate de atacuri cibernetice, cu scopul principal de a „infecta" nișe specifice ale industriei, recomandăm companiilor șapte pași prin care și-ar putea crește nivelul de protecție:

1. Implementarea de controale tehnice sporite de securitate: ex., Firewall, IPS (*Intrusion Prevention System*), MFA (*Multi Factor Authentication*), AV (*Antivirus*);
2. Traininguri de *Cyber Security Awareness* pentru a crește vigilența angajaților în fața diverselor tipuri de atac utilizate și de a nu cădea ușor pradă celei mai comune metode – Phishing-ul;
3. Crearea unor praguri minime de complexitate a parolelor pentru angajați (folosirea de caractere speciale, atât litere, cât și numere, o anumită lungime a parolei), dar și implementarea unei politici de schimbare a parolelor cât mai frecventă care să nu permită totodată

refolosirea aceleiași parole pentru o perioadă mai îndelungată de timp;
4. Upgradare și patching al tuturor dispozitivelor și sistemelor (patching de vulnerabilități);
5. Folosirea unei soluții centralizate de stocare a datelor, de exemplu, *Cloud storage*, și menținerea unui backup al datelor;
6. Creșterea securității în ceea ce privește utilizarea unei conexiuni de tip VPN (*Virtual Private Network*) prin adăugarea unor straturi suplimentare în metoda de autentificare a angajatului la rețeaua interna (ex.: MFA – *Multi Factor Authentication*);
7. Folosirea unor software-uri de criptare pentru a proteja datele companiei și a restricționa accesul utilizatorilor neautorizați.

Poate părea complicat, dar este un demers necesar având în vedere impactul negativ pe care l-ar putea avea, din punct de vedere fiscal, pentru contribuabili. Iar statisticile globale arată că, dacă până acum nu ai fost victima unui atac informatic, înseamnă că nu ai aflat încă de el.

În concluzie, cum pericolele pot proveni atât din intern, cât și din extern, ele trebuie combătute printr-o strategie bine pusă la punct, care să implice oameni, procese și tehnologie. În plus, experiența ne-a arătat că, dacă rolurile sunt segregate, iar angajații sunt ținuți la curent cu noutățile din zona pericolelor cibernetice, conform unor politici clare de securitate ale companiei, atât dispozitivele, cât și sistemele de perimetru sau rețeaua sunt protejate corespunzător. În acest fel, activitățile din rețea sunt înregistrate și monitorizate, deci probabilitatea de a deveni o victimă a acestor atacuri cibernetice va fi redusă semnificativ și potențialul impact fiscal negativ va fi evitat.