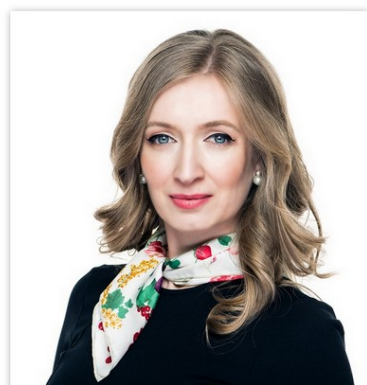


Kit juridic pentru companii în caz de atacuri cibernetice



schönherr

A devenit o realitate cvasi-cotidiana faptul ca tot mai multe companii sunt ținte ale atacurilor cibernetice. Autorii acestor infracțiuni informatice rămân însa, de cele mai multe ori, nepedepsiți, ceea ce nu face decât sa încurajeze acest fenomen infracțional.

Practica în domeniul penal a demonstrat ca, în România, multe cauze de criminalitate informatica sunt clasate. Pe de o parte, aceasta situație are legatura cu lipsa pregătirii de specialitate în domeniul investigării infracțiunilor informatice. Dar, și mai acut, soluțiile de clasare au legatura directa cu faptul ca persoanele vatamate se afla în imposibilitatea de a-și susține sesizarile printr-un probatoriu adecvat.

În baza principiului aflării adevărului (reminiscenta a principiului oficialității), organelor judiciare penale le revine obligația de a asigura, pe baza de probe, aflarea adevărului cu privire la împrejurările cauzei, precum și cu privire la persoana suspectului sau inculpatului. Însa, pentru reconstituirea adevărului judiciar este necesara administrarea probelor furnizate în primul rând de părți, acestea având principalul interes în a-și dovedi cauza. Iar, de cele mai multe ori, companiile prejudiciate nu reușesc sa genereze probe suficiente, care sa le permita organelor de cercetare penala sa construiasca un caz solid împotriva celui care a comis atacul cibernetic.

Top 5 mijloace de proba care pot crește șansele companiilor într-un dosar penal împotriva infractorilor cibernetici

Pentru a contribui la schimbarea acestei situații, companiile se pot pregati astfel încât sa poata reacționa rapid și eficient în cazul în care se confrunta cu un incident de securitate informatica. În acest sens, este recomandabila popularizarea și pregătirea și nivelul companiei a unui ghid de reacție în caz de atac cibernetic. Acesta ar trebui sa conțină – pe lângă regulamente interne și/sau protocoale de conformitate bine stabilite – și (cel puțin) cinci mijloace de proba pe care compania sa le aiba pregatite în momentul sesizării organelor de urmarire penala.

Pregătirea unui astfel de ghid privind mijloacele de proba este esențiala, în special având în vedere volatilitatea și fragilitatea datelor și informațiilor stocate în sistemele informatice, care face ca orice manipulare necorespunzatoare a probelor digitale sa le poata altera iremediabil.

În cele ce urmeaza, prezentam un top 5 orientativ al elementelor care ar putea fi incluse în lista de mijloace de proba esențiale din ghidul unei companii. Acest kit juridic de lupta împotriva infractorilor informatici va putea fi adaptat în funcție de particularitățile fiecarui dosar penal. Ca regula generala, urmatoarele elemente pot ajuta o companie victima a unui atac cibernetic sa își susțină ferm poziția în dosarul penal:

1. Raportul de audit informatic, întocmit de către specialiști în securitate informatică, angajați de companie. Acest raport conține, ideal, o radiografie cât mai fidelă a incidentului informatic și, deși echivalează cu un raport de expertiză extra-judiciară, le furnizează organelor de anchetă un diagnostic rapid asupra stadiului curent al sistemului informatic atacat, din perspectiva recuperării și conservării datelor informatice.
2. Declarațiile de martor, printre care apreciem utilă depozitia experților în domeniul IT din interiorul sau din afara organizației. În acest sens, compania ar trebui să ia măsuri pentru a documenta prompt aceste declarații, imediat după producerea incidentului sau în proximitatea atacului cibernetic, pentru a păstra acuratețea detaliilor tehnice asupra incidentului.
3. Alte înscrisuri relevante, utile cauzei, de exemplu, corespondența electronică dintre companie și faptuitori (dacă există) și/sau informații despre datele de acces (utilizator/parola), istoricul conexiunilor la sistem, caracteristicile sistemelor informatice de pe care s-a realizat accesul neautorizat, etc.
4. Orice informație pe care compania prejudiciată o are cu privire la potențialii infractori este de asemenea deosebit de valoroasă în cadrul anchetei. Este important de avut în vedere că, pentru a le fi utile investigatorilor, astfel de informații trebuie să fie trasabile și/sau disponibile, adică ideal recuperabile chiar din sistemul informatic supus atacului.
5. Soluțiile în cazuri similare de criminalitate informatică pot avea rol orientativ pentru organele judiciare. Jurisprudența din cauze conexe (naționale și/sau internaționale) poate fi valorificată în kitul judiciar; deși nu reprezintă un mijloc de probă, în definiția sa clasică, aceasta poate consolida probele particulare ale cauzei.

Este important ca, pe lângă programe de training organizate periodic la nivelul companiilor în scopul prevenirii incidentelor de securitate informatică și al asigurării reacției prompte în cazul producerii unui atac cibernetic, angajații relevanți să fie instruiți și cu privire la momentul optim și modul efectiv în care aceștia pot contribui la conservarea probelor ce ar putea fi folosite de către companie într-un dosar penal.

Pregătind din timp aceste probe, companiile prejudiciate vor crește șansele de reușită în urmărirea și condamnarea infractorilor cibernetic, cu consecința posibilității reale de recuperare de către companii a prejudiciului produs de către aceștia.