Kit juridic pentru companii în caz de atacuri cibernetice

A devenit o realitate cvasi-cotidiana faptul ca tot mai multe companii sunt ținte ale atacurilor cibernetice. Autorii acestor infracțiuni informatice ramân 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 pregatirii de specialitate în domeniul investigarii 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 aflarii adevarului (reminiscența a principiului oficialității), organelor judiciare penale le revine obligația de a asigura, pe baza de probe, aflarea adevarului cu privire la împrejurarile cauzei, precum și cu privire la persoana suspectului sau inculpatului. Însa, pentru reconstituirea adevarului judiciar este necesara administrarea probelor furnizate în primul rând de parți, 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 pregatirea și nivelul companiei a unui ghid de reacție în caz de atac cibernetic. Acesta ar trebui sa conțina – pe lânga 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 sesizarii organelor de urmarire penala.

Pregatirea 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 particularitațile fiecarui dosar penal. Ca regula generala, urmatoarele elemente pot ajuta o companie victima a unui atac cibernetic sa își susțina ferm poziția în dosarul penal:

1. Raportul de audit informatic, întocmit de catre specialişti în securitate informatica, angajaţi de companie. Acest raport conţine, ideal, o radiografie cât mai fidela a incidentului informatic şi, deşi echivaleaza cu un raport de expertiza extra-judiciara, le furnizeaza organelor de ancheta un diagnostic rapid asupra stadiului curent al sistemului informatic atacat, din perspectiva recuperarii şi conservarii datelor informatice.

2. Declaraţiile de martor, printre care apreciem utila depoziţia experţilor în domeniul IT din interiorul sau din afara organizaţiei. În acest sens, compania ar trebui sa ia masuri pentru a documenta prompt aceste declaraţii, imediat dupa producerea incidentului sau în proximitatea atacului cibernetic, pentru a pastra acurateţea detaliilor tehnice asupra incidentului.

3. Alte înscrisuri relevante, utile cauzei, de exemplu, corespondenţa electronica dintre companie şi faptuitori (daca exista) şi/sau informaţii despre datele de acces (utilizator/parola), istoricul conectarilor la sistem, caracteristicile sistemelor informatice de pe care s-a realizat accesul neautorizat, etc.

4. Orice informaţie pe care compania prejudiciata o are cu privire la potenţialii infractori este de asemenea deosebit de valoroasa în cadrul anchetei. Este important de avut în vedere ca, pentru a le fi utile investigatorilor, astfel de informaţii trebuie sa fie trasabile şi/sau disponibile, adica ideal recuperabile chiar din sistemul informatic supus atacului.

5. Soluţiile în cazuri similare de criminalitate informatica pot avea rol orientativ pentru organele judiciare. Jurisprudenţa din cauze conexe (naţionale şi/sau internaţionale) poate fi valorificata în kitul judiciar; deşi nu reprezinta un mijloc de proba, în definiţia sa clasica, aceasta poate consolida probele particulare ale cauzei.

Este important ca, pe lânga programe de training organizate periodic la nivelul companiilor în scopul prevenirii incidentelor de securitate informatica şi al asigurarii reacţiei prompte în cazul producerii unui atac cibernetic, angajaţii relevanţi sa fie instruiţi şi cu privire la momentul optim şi modul efectiv în care aceştia pot contribui la conservarea probelor ce ar putea fi folosite de catre companie într-un dosar penal.

Pregatind din timp aceste probe, companiile prejudiciate vor creşte şansele de reuşita în urmarirea şi condamnarea infractorilor cibernetici, cu consecinţa posibilitaţii reale de recuperare de catre companii a prejudiciului produs de catre aceştia.