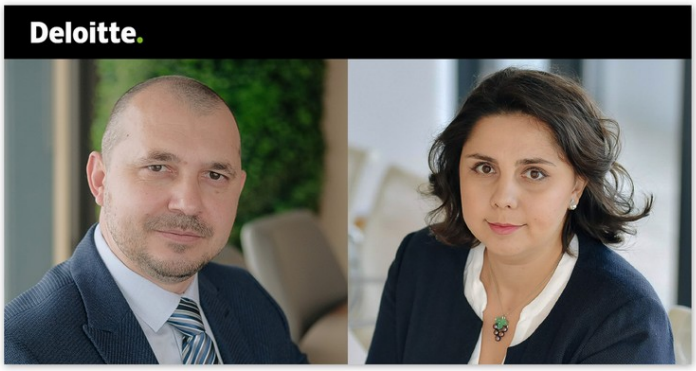
Cum îți pregatești organizația sa raspunda unei potențiale crize cibernetice?



*Organizațiile, din sectorul public sau privat, trebuie sa aiba în vedere implementarea unei **strategii de securitate**, menita sa asigure pe termen lung rezistența proceselor esențiale ale acestora la atacuri cibernetice țintite sau oportuniste. Pe de alta parte, asigurarea unei aparari perfecte este un obiectiv dificil de atins, având în vedere ca aceasta necesita mobilizarea de resurse financiare considerabile, dar și umane, aspect care a devenit o provocare pentru organizații din cauza lipsei deja cronice de experți în domeniul securității cibernetice.*

În acest sens, **exercițiile de simulare a crizelor cibernetice** ar trebui sa se regaseasca periodic ca o prioritate pe agenda tuturor companiilor, în special ca o masura de limitare a impactului asupra reputației și a aspectelor de natura legala și operațională, dar nu în ultimul rând financiara, în cazul nefericit al unui atac major reușit asupra unor procese critice sau al scurgerilor neautorizate de date (*data exfiltration)* strict reglementate.

Deși crizele cibernetice se înscriu în categoria evenimentelor rare care pot aparea în cadrul unei organizații, acestea au de cele mai multe ori un impact major. Studiile Deloitte arata ca, în cele mai multe cazuri, acest impact produce efecte care nu sunt exclusiv de natura cibernetica, ci se pot extinde în arii care nu sunt legate în mod tradițional de domeniul securității cibernetice. De exemplu, efectele unui incident cu valențe de criza pot avea un impact negativ și asupra retenției angajaților, pot cauza pierderea încrederii clienților, dar și prejudicii asupra reputației companiei, cu potențial de transformare într-o criza mediatica.

Care sunt aspectele pe care companiile le pot exersa într-o simulare a unei crize cibernetice?

În timpul exersarii unui incident de natura cibernetica, este aproape imposibil sa simulezi și adrenalina specifica unei situații reale. În plus, anumite decizii cheie, luate în situații de criza cu totul unice, pot fi cu greu replicate prin simulari.

Pe de alta parte, sunt aspecte care pot fi instruite, iar unul dintre cele mai importante paliere este cel care privește **luarea deciziilor cheie cu privire la criza** respectiva. Este esențial de stabilit persoana sau grupul de persoane care pot lua aceste hotarâri în situații de criza și criteriile în funcție de care acestea sunt desemnate. În mare parte, acest rol decizional revine membrilor din top managementul unei companii și este atribuit în funcție de natura impactului pe care o decizie o poate avea asupra organizației. Spre exemplu, oprirea temporara a producției unei companii ar trebui sa fie o decizie luata de directorul general.

Zona de comunicare poate, de asemenea, fi exersata într-un scenariu de criza cibernetica. Modalitatea și momentul în care se comunica cu autoritățile, angajații, presa sau pe rețelele sociale, platforme care au o capacitate

uriașa de a amplifica mesajele catre clienți care ar putea fi afectați de criza cibernetica, sunt aspecte care pot fi exersate în cadrul simularii și perfecționate ulterior daca este necesar. Acțiunile celulei de comunicare necesita coordonarea cu cele desfașurate de alte echipe, parte din echipa multidisciplinara responsabila de raspunsul la criza, deoarece o desincronizare ar putea avea un puternic impact asupra reputației companiei.

În momentul simularii unui incident cibernetic major, pot fi exersate și aspectele care țin de partea de **raspuns la incidente din punct de vedere juridic**. Organizațiile trebuie sa știe în ce moment raporteaza incidentul catre autoritați, care sunt pașii de urmat în cazul în care criza respectiva are efecte asupra unor date cu caracter personal, daca trebuie facuta o plângere penala și cum anume trebuie aceasta redactata, daca implica sau nu și experții în *forensics,* interni*,* daca exista, sau externi.

Nu în ultimul rând, în funcție de natura crizei cibernetice, **planul de continuitate a afacerii** poate sa constituie un punct important din cadrul exercițiului. Spre exemplu, simularea unui incident cu puternic impact asupra sistemelor critice poate reprezenta un moment bun pentru a cunoaște și observa capacitatea de reacție a unor departamente, precum cel de IT, și pentru a evalua daca are sens activarea planului de continuitate sau al planului de recuperare în caz de dezastru.

De ce este importanta organizarea unui exercițiu de simularea a unei crize cibernetice?

Având în vedere nivelul de complexitate la care au ajuns atacurile cibernetice în ultimii ani, organizațiile trebuie sa ia în considerare includerea unor exerciții de simulare a crizelor în strategiile de securitate.

Cu ajutorul unui exercițiu de simulare concertat și **care reda fidel scenariul unui atac cibernetic transformat în criza**, o companie poate înțelege ce **capacitate are de a raspunde amenințarilor** din ce în ce mai diverse și complexe, într-o era a progresului transformarii digitale.

Nu în ultimul rând, un exercițiu de simulare este o **oportunitate de a îmbunatați**, daca este necesar, unele aspecte care țin de procesele de management al crizelor pentru a preveni nu numai compromiterea activelor companiei, ci și a angajaților acesteia, clienților și partenerilor sai de business.