

Top 5 greșeli comune facute înainte sau în timpul unui incident informatic



Dinamica societății și tehnologizarea tot mai evidentă a tuturor ramurilor de care omul modern se lovește zi de zi a creat cadrul favorabil apariției și dezvoltării unui fenomen care nu mai este deloc nou în România: criminalitatea informatică. Fie că își are originea în țara noastră, fie că o “importăm”, din ce în ce mai multe persoane fizice sau juridice cad victimă și, nu de puține ori, pierderile sunt greu de recuperat.

1. „Mie nu mi se poate întâmpla”

Este poate cea mai mare eroare pe care atât persoanele fizice, dar mai ales factorii de decizie ai unor societăți comerciale o pot face. Plecând de la premisa enunțată, acțiunile lor sunt în această direcție. Astfel, lipsa alocării unui buget în vederea protejării împotriva atacurilor informatice sau o instruire deficitară a personalului în acest sens sunt doar câteva dintre „strategiile” care transformă companiile într-o victimă sigură.

Concepția des întâlnită precum că, atâta timp cât nu ai nimic de ascuns și de interes pentru atacatori, ești în siguranță, este greșită. Cele mai multe dintre atacurile informatice au drept scop obținerea unor foloase materiale și, în egală măsură, a unor resurse informatice care să fie folosite ulterior în generarea altor atacuri. Practica judiciară în domeniu este bogată în cazuri în care infrastructura unor terțe societăți comerciale a fost folosită în savârșirea unor infracțiuni informatice.

2. Protejarea împotriva atacurilor informatice nu este o activitate care se face o dată și bine

Achiziția și configurarea inițială a unor soluții hardware și/sau software care să ajute la stoparea sau reducerea unor astfel de atacuri este o primă acțiune pe calea protejării datelor și activelor companiei. Nu este însă suficientă.

Nu de puține ori s-au întâlnit situații când licențele de antivirus erau expirate și semnăturile nu erau la zi sau regulile din firewall nu mai erau de actualitate. O practică trecută des cu vederea este acumularea de privilegii în rândul angajaților care sunt de o perioadă mai mare de timp în companie. Pe măsură ce ocupă mai multe roluri cu sarcini diferite, ei ajung într-un final să aibă mult mai multe drepturi de acces în sistemele informatice decât au nevoie. Astfel, managementul „user-ilor” este deficitar, putând facilita fie o eventuală fraudă din partea aceluiași angajat, fie mărirea suprafeței de atac împotriva companiei, în cazul în care contul este compromis de terțe persoane.

Poate cel mai rasunător caz generat de această greșeală este „Wannacry”, iar principala cauză care a generat acest atac a fost tocmai lipsa instalării unor update-uri de securitate menite să remedieze anumite vulnerabilități cunoscute deja de către profesioniștii în domeniu ca fiind ușor exploatabile. Rezultatul a fost un atac informatic de tip ransomware de proporții, fiind criptate peste 230.000 de calculatoare de pe întreg mapamondul, cu pierderi totale de peste 1 miliard de dolari.

3. „Încerc sa fac totul de unul singur”

Nevoia de a ține costurile sub control împinge multe companii să încredințeze management-ul soluțiilor de securitate unei persoane interne al carei rol de zi cu zi este cu totul altul. Cel mai des întâlnit caz este acela de a apela la persoana responsabilă cu gestionarea echipamentelor de IT, care, pe parcurs, instalează și configurează și echipamentele de rețea (router/switch), firewall, soluțiile software de pe stații, cloud, etc.

Fiecare dintre tehnologiile anterior enumerate are caracteristici diferite, iar gestionarea acestora și configurarea de către o persoană care nu are pregătirea necesară reprezintă încă un risc pentru compania respectivă. De foarte multe ori, percepția că ești protejat, când în realitate ai o mare vulnerabilitate, este mai periculoasă, întrucât compania va desfășura activități și va expune în mediul online date informatice care, în alte condiții, ar fi mult mai bine protejate.

4. Folosirea inadecvată a parolelor de acces și a altor metode de autentificare

Managementul parolelor de acces nu este un lucru ușor, mai ales când sistemele în care user-ul se va autentifica sunt multiple, politicile de complexitate și de expirare a acestora sunt diferite de la un serviciu la altul, iar persoana care le folosește nu are o pregătire minimă în legătură cu modul de păstrare al acestora.

Un exemplu des întâlnit este cel al sticky-note-urilor lipite de monitor sau agende uitate printr-o sală de conferință, conținând parolele de acces într-un anumit sistem informatic. Aceste incidente au generat adoptarea clară a unei politici de „clean desk”, care ar putea crea cadrul favorabil prin care angajații să fie instruiți pentru a nu expune parolele de acces.

5. Lipsa unor procese clare în cazul unui incident informatic sau aplicarea lor haotică

Companiile care sunt conștiente de aceste riscuri au investit, în mod constant, în remedierea problemelor mai sus amintite. Cu toate acestea, oricât de puțin s-ar reduce suprafața de atac, oricâte tehnologii de prevenție, detecție și stopare s-ar implementa, nu toată lumea joacă după aceleași reguli. Un atac informatic se va întâmpla oricând, e doar o chestiune de timp.

Mai mult, prin Legea 362/2018 care transpune directiva europeană 1148/2016 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, toate companiile care furnizează servicii esențiale către populație trebuie să minimizeze riscurile și să ia măsuri interne manageriale și de natură tehnică, astfel încât să diminueze riscul cibernetic. Ceea ce înseamnă că vor fi obligate să bugeteze și să realizeze investiții în această direcție, având în vedere că, de multe ori, acest aspect nu a fost unul de o importanță majoră pentru managementul unui operator de servicii esențiale.

Art. 42 al acestei legi intrată în vigoare în ianuarie 2019 indică faptul că entitățile care acționează în sectoarele vizate au un termen de 2 ani în care să depună documentația de autoevaluare a îndeplinirii cerințelor minime de securitate și notificare. Sunt prevăzute și o serie de contravenții substanțiale în cazul în care, după producerea unui incident informatic grav, se constată că acea companie nu a întreprins măsurile necesare pentru a-l împiedica sau pentru a-i diminua efectele.

Producerea unui incident informatic, de orice natură ar fi el (phishing, malware infection, DDOS attack, website defacement etc.), obligă la acționarea imediată a unui plan de răspuns care să ducă la înlăturarea efectelor negative sau macar la diminuarea lor pe cât posibil. Nu întâmplător, la nivel internațional, au fost create mai multe cadre de reglementare a acestor situații în care sunt descrise activitățile care trebuie întreprinse.

Cele mai populare două astfel de cadre de lucru sunt cele elaborate de către NIST (National Institute of Standards and Technology) și SANS (SysAdmin, Audit, Network, and Security). Acestea nu sunt substanțial diferite, oricare dintre cele două metodologii ajută la formularea unui răspuns mai bun în cazul unui atac informatic, bazat pe un

set de pași pe care oricine din organizație ar trebui să îi aplice, atunci când își propune să investească în această zonă. Sigur că aceștia trebuie adaptați specificului organizației și implementați, de preferat, înaintea producerii unui atac informatic.

Conștientizăm greșelile: care este următorul pas?

Unele dintre aspectele menționate mai sus sunt ușor de remediat, necesitând doar o conștientizare mai mare din partea factorilor de decizie dintr-o companie a pericolelor la care o expun atunci când aplică ceea ce mulți specialiști consideră a fi o strategie cunoscută drept „security through obscurity”.

În baza acesteia, mecanismele de securitate sunt cunoscute doar de către membrii care o aplică și o folosesc, iar un eventual atac informatic ar putea reuși doar dacă acestea sunt cunoscute, lucru considerat puțin probabil. Practica a dovedit că această strategie este drumul sigur către o țintă ușoară a hackerilor.

Dinamica atacurilor informatice și versatilitatea lor fac imposibilă aplicarea unei rețete universale care să funcționeze ca un „panaceu”. Factorii de decizie care își desfașoară chiar și o mică parte din activitatea lor prin utilizarea unor servicii și tehnologii informatice trebuie să-și adapteze strategia de securitate în funcție de specificul și natura activității întreprinse, iar apelarea la servicii profesionale în domeniu ar putea să pe termen lung să facă diferența între existența și prosperitatea pe piața sau disoluție.