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

Dinamica societații și tehnologizarea tot mai evidenta a tuturor ramurilor de care omul modern se lovește zi de zi a creat cadrul favorabil apariției și dezvoltarii unui fenomen care nu mai este deloc nou în România: criminalitatea informatica. Fie ca își are originea în țara noastra, fie ca o "importam", din ce în ce mai multe persoane fizice sau juridice cad victima 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 societaţi comerciale o pot face. Plecând de la premisa enunțata, acțiunile lor sunt în aceasta direcție. Astfel, lipsa alocarii unui buget în vederea protejarii împotriva atacurilor informatice sau o instruire deficitara a personalului în acest sens sunt doar câteva dintre „strategiile" care transforma companiile într-o victima sigura.

Concepția des întâlnita precum ca, atâta timp cât nu ai nimic de ascuns și de interes pentru atacatori, ești în siguranța, este greșita. Cele mai multe dintre atacurile informatice au drept scop obținerea unor foloase materiale și, în egala masura, a unor resurse informatice care sa fie folosite ulterior în generarea altor atacuri. Practica judiciara în domeniu este bogata în cazuri în care infrastructura unor terțe societați comerciale a fost folosita în savârșirea unor infracțiuni informatice.

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

Achiziția şi configurarea inițiala a unor soluții hardware şi/sau software care sa ajute la stoparea sau reducerea unor astfel de atacuri este o prima acțiune pe calea protejarii datelor şi activelor companiei. Nu este însa suficienta.

Nu de puține ori s-au întâlnit situaţii când licențele de antivirus erau expirate şi semnaturile nu erau la zi sau regulile din firewall nu mai erau de actualitate. O practica trecuta des cu vederea este acumularea de privilegii în rândul angajaților care sunt de o perioada mai mare de timp în companie. Pe masura ce ocupa mai multe roluri cu sarcini diferite, ei ajung într-un final sa aiba mult mai multe drepturi de acces în sistemele informatice decât au nevoie. Astfel, managementul „user-ilor" este deficitar, putând facilita fie o eventuala frauda din partea acelui angajat, fie marirea suprafeței de atac împotriva companiei, în cazul în care contul este compromis de terțe persoane.

Poate cel mai rasunator caz generat de aceasta greșeala este „Wannacry", iar principala cauza care a generat acest atac a fost tocmai lipsa instalarii unor update-uri de securitate menite sa remedieze anumite vulnerabilitați cunoscute deja de catre 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 sa 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 responsabila cu gestionarea echipamentelor de IT, care, pe parcurs, instaleaza și configureaza 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 catre o persoana care nu are pregatirea necesara reprezinta înca un risc pentru compania respectiva. De foarte multe ori, percepția ca ești protejat, când în realitate ai o mare vulnerabilitate, este mai periculoasa, întrucât compania va desfașura activitați și va expune în mediul online date informatice care, în alte condiții, ar fi mult mai bine protejate.

4. Folosirea inadecvata 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 pregatire minima în legatura cu modul de pastrare al acestora.

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

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

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 toata lumea joaca dupa aceleași reguli. Un atac informatic se va întâmpla oricând, e doar o chestiune de timp.

Mai mult, prin Legea 362/2018 care transpune directiva europeana 1148/2016 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, toate companiile care furnizeaza servicii esențiale catre populație trebuie sa minimizeze riscurile și sa ia masuri interne manageriale și de natura tehnica, astfel încât sa diminueze riscul cibernetic. Ceea ce înseamna ca vor fi obligate sa bugeteze și sa realizeze investiții în aceasta direcție, având în vedere ca, de multe ori, acest aspect nu a fost unul de o importanța majora pentru managementul unui operator de servicii esențiale.

Art. 42 al acestei legi intrata în vigoare în ianuarie 2019 indica faptul ca entitațile care acționeaza în sectoarele vizate au un termen de 2 ani în care sa depuna documentația de autoevaluare a îndeplinirii cerințelor minime de securitate și notificare. Sunt prevazute și o serie de contravenții substanțiale în cazul în care, dupa producerea unui incident informatic grav, se constata ca acea companie nu a întreprins masurile necesare pentru a-l împiedica sau pentru a-i diminua efectele.

Producerea unui incident informatic, de orice natura ar fi el (phishing, malware infection, DDOS attack, website defacement etc.), obliga la acționarea imediata a unui plan de raspuns care sa duca la înlaturarea efectelor negative sau macar la diminuarea lor pe cât posibil. Nu întâmplator, la nivel internațional, au fost create mai multe cadre de reglementare a acestor situații în care sunt descrise activitațile care trebuie întreprinse.

Cele mai populare doua 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 doua metodologii ajuta la formularea unui raspuns mai bun în cazul unui atac informatic, bazat pe un

set de paşi pe care oricine din organizaţie ar trebui sa îi aplice, atunci când îşi propune sa investeasca în aceasta zona. Sigur ca aceştia trebuie adaptaţi specificului organizaţiei şi implementaţi, de preferat, înaintea producerii unui atac informatic.

Conştientizam greşelile: care este urmatorul pas?

Unele dintre aspectele menţionate mai sus sunt uşor de remediat, necesitând doar o conştientizare mai mare din partea factorilor de decizie dintr-o companie a pericolelor la care o expun atunci când aplica ceea ce mulţi specialişti considera a fi o strategie cunoscuta drept „security through obscurity”.

În baza acesteia, mecanismele de securitate sunt cunoscute doar de catre membrii care o aplica şi o folosesc, iar un eventual atac informatic ar putea reuşi doar daca acestea sunt cunoscute, lucru considerat puţin probabil. Practica a dovedit ca aceasta strategie este drumul sigur catre o ţinta uşoara a hackerilor.

Dinamica atacurilor informatice şi versatilitatea lor fac imposibila aplicarea unei reţete universale care sa funcţioneze ca un „panaceu”. Factorii de decizie care îşi desfaşoara chiar şi o mica parte din activitatea lor prin utilizarea unor servicii şi tehnologii informatice trebuie sa-şi adapteze strategia de securitate în funcţie de specificul şi natura activitaţii întreprinse, iar apelarea la servicii profesioniste în domeniu ar putea ca pe termen lung sa faca diferenţa între existenţa şi prosperitatea pe piaţa sau disoluţie.