Pericolul din spatele zidurilor de aparare, când amenințarea vine din interior

Amenințarea cu un atac informatic nu îi mai surprinde demult pe cei care au în mâna destinele unei companii, motiv pentru care, încurajați și de legislația în vigoare referitoare la GDPR, încep sa ia cât mai multe masuri pentru a stopa o eventuala exfiltrare de date sau alterare a acestora. Toate acestea sunt însa în van daca sursa atacului vine din interior, iar consecințele pot fi infinit mai mari decât în cazul unui atac informatic efectuat de un hacker.

Conform unui raport furnizat de Proofpoint, lider în domeniul protecţiei împotriva atacurilor de tip phishing, în 2020, 60% dintre companiile analizate au avut cel puțin 30 de incidente legate de o amenințare din interior și, în cele mai multe cazuri, timpul de identificare a acestora a fost mai mare de 30 de zile, cauzând în final pierderi în medie de 11 milioane dolari/companie, în creştere faţa de valoarea din 2018, de 8.76 milioane dolari/companie. De asemenea, în același interval de timp și numarul de atacuri informatice generate de persoane din interiorul companiei a crescut cu 47%.

Daca în majoritatea cazurilor vorbim de actuali angajați care se preteaza la un moment dat la astfel de acțiuni, nu trebuie neglijați nici partenerii sau colaboratorii care sunt în strânsa legatura cu o companie ori foşti angajaţi care cunosc arhitectura interioara și automat și punctele slabe. Atacurile din interior sunt printre cele mai greu de depistat întrucât persoanele enumerate mai sus au de cele mai multe ori acces extins în cadrul sistemelor de lucru, cunosc în multe cazuri și metodele de depistare și cum sa le evite. Mai grav este atunci când, prin natura rolului îndeplinit, persoana are acces la informații sensibile, cum ar fi date financiare sau clienți și informații confidențiale legate de aceștia.

„Ce-i mâna în lupta?”

Cauzele care duc la aceste incidente pot fi diverse și majoritatea au o strânsa legatura cu motivația pe care fiecare atacator o are pentru a-și duce la bun sfârșit planul. Pentru a înțelege factorii declanșatori ai unui astfel de incident trebuie înțelese diferențele între tipurile de persoane care recurg la acest tip de activitați:

- Angajatul neglijent: în majoritatea companiilor, angajaţii parcurg cursuri despre modalitatea în care trebuie prelucrate și transmise datele, amenințarile la care sa fie atenți și procedurile de urmat atunci când constata o activitate suspecta în mediul online. Nu de puține ori se întâmpla sa existe persoane care, fie din neștiința, superficialitate ori din dorința de a trece peste anumite reguli pentru a rezolva mai repede o sarcina de serviciu, expun datele informatice ale angajatorului la un risc sporit de a fi transferate neautorizat în mediul extern ori sa le afecteze iremediabil (vezi situația unui atac de tip ransomware, când date ale companiei sunt criptate și chiar o

eventuala restaurare poate sa nu duca la o recuperare completa a acestora).

- Angajatul rau-intenționat: o marire de salariu care nu a fost pe masura așteptarilor, o avansare care nu a venit la timpul dorit ori încetarea unilaterala din partea angajatorului a contractului de munca sunt situaţii în care anumite persoane își pierd simțul rațiunii și recurg la acte de razbunare. Nu puține au fost cazurile când astfel de atacatori au șters bazele de date ale companiei sau le-au transferat pe un mediu de stocare personal, șantajând ulterior compania cu publicarea acestora în mediul public.

- Angajatul „infractor în timpul liber": aici se are în vedere cea mai grava forma a acestui tip de atac, în care persoane care au primit acces în mediul informatic al unei companii se folosesc de drepturile pe care le au pentru a copia sistematic informații confidențiale pe care ulterior sa le vânda pe Darkweb și sa obțina astfel avantaje materiale. De asemenea, au mai fost întâlnite deseori situaţii în care persoane care supravegheau active financiare ale companiei, beneficiind de încrederea care li se acorda combinata cu anumite lipsuri în supravegherea activitaţii acestora, au extras, prin diferite artificii în sistemul informatic al companiei, sume de bani pe care le-au folosit ulterior în interes personal.

Cum protejam datele companiei respectând dreptul angajatului la viaţa privata?

Din ce în ce mai multe companii au adoptat o cultura organizaţionala sanatoasa care pune în centrul ei angajatul și fidelizarea acestuia. Din acest motiv, implementarea unor masuri care sa previna situaţiile în care unul dintre aceștia s-ar putea întoarce împotriva angajatorului trebuie luate cu mare atenție pentru a nu afecta libertatea și drepturile majorității. Aceasta abordare face însa ca un astfel de atac sa fie și mai greu de identificat.

Practica a aratat ca mecanismele care trebuie adoptate trebuie sa aiba în vedere atât nevoia de a proteja datele companiei, cât și dreptul angajatului la viaţa privata. Este prevazut fara echivoc atât de catre legislaţia muncii, cât și de cea privind protecția datelor cu caracter personal faptul ca angajatul beneficiaza de dreptul la viaţa privata chiar și atunci când opereaza de pe dispozitive aflate în administrarea companiei la care lucreaza. Astfel, raspunsul la aceasta problema nu este unul singur, ci mai degraba reprezinta un mixt între diferitele controale care pot fi puse la un loc pentru a preveni sau identifica la timp acest tip de activitați.

1) Controale tehnice: implementarea de soluții de prevenire și stopare a exfiltrarii de date informatice, așa numitele Data Loss Prevention, care pot fi configurate pe nevoia fiecarei companii în parte, astfel încât sa alerteze și/sau stopeze în momentul când anumite date sunt scoase în afara companiei. De asemenea, aceasta masura este bine sa fie completata și prin configurarea unor mecanisme prin care datele stocate sau în tranzit sunt criptate, astfel orice interceptare a acestora, fie ea și accidentala, sa nu supuna compania la un risc.

2) Masuri administrative – Deși nu întotdeauna posibil, în funcție de natura rolului, sarcinile de serviciu pot fi îndeplinite prin rotație de mai multe persoane, astfel încât eventuale abateri de la procedura normala sa poata fi semnalate. În plus, principiul separației sarcinilor trebuie sa fie o regula astfel încât o acțiune sa nu poata fi dusa la bun sfârșit decât prin colaborarea a doua sau mai multe persoane, fiecare cu diferite atribuții. Un exemplu clasic ar fi situația în care cineva identifica acțiunea care trebuie întreprinsa și demareaza procedurile, o alta persoana aproba și o a treia executa plata.

În completarea acestor masuri ar trebui sa fie menționate și anumite proceduri clare prin care datele companiei pot fi totuși scoase din companie. Deși acest lucru nu este posibil pentru departamentele a caror activitate zilnica implica schimbul de date constant cu entitați din afara companiei, cu siguranţa exista numeroase alte compartimente care lucreaza cu date sensibile și care nu ar implica transferul de date spre exterior.

Nu în ultimul rând, nu trebuie uitata existența unei proceduri de lucru de raspuns la acest tip de evenimente constând într-un plan de raspuns la incidente informatice și diferite fluxuri de activitați în funcție de specificul

fiecarui atac suferit.

3) Coordonare între departamentul de HR şi IT: Poate cea mai delicata componenta din lista recomandarilor întrucât nevoia unei astfel de colaborari are loc în momentul în care sunt suspiciuni clare cu privire la existenţa unui atacator din interior. Astfel, departamentele de HR pot sa anunţe echipa de monitorizare a incidentelor în momentul în care sunt indicii ca o persoana a manifestat intenţii vadite cu privire la o astfel de activitate. Aceasta masura trebuie cuprinsa expres în cadrul unei proceduri, cu indicarea clara a situaţiei în care activitatea profesionala este monitorizata, pentru a nu lasa loc abuzurilor din partea angajatorilor, care în ideea protejarii reţelei exercita un control ce poate fi intimidant şi chiar ilegal pentru persoanele de buna credinţa, care, din fericire, reprezinta majoritatea covârşitoare.

Echilibru în adoptarea masurilor

Realitatea a dovedit ca astfel de activitaţi de rea-credinţa îndreptate împotriva datelor informatice ale companiei (în unele cazuri chiar împotriva propriilor colegi) sunt o realitate de care fiecare decident trebuie sa ţina cont. Însa, cel mai important este gasirea unui echilibru între crearea unei culturi organizaţionale axate pe încredere şi profesionalism şi dezvoltarea unor mecanisme obiective de monitorizare, identificare şi raspuns eficient în cazul în care sunt indicii ale unui atac informatic din interior. Oricare mişcare spre una dintre cele doua extreme poate cauza fie un mediu impropriu de lucru pentru cea mai importanta resursa, oamenii, fie un risc iminent de compromitere a datelor informatice, aceasta situaţie din urma venind la pachet şi cu alte inconveniente atât de natura contravenţionala, cât şi penala în anumite cazuri.