|  |  |
| --- | --- |
| Punct de vedere  13 septembrie 2021 | |
| Contact: | Anda Huțanu |
| Companie: | EY România |
| Tel: | +40 21 402 4000 |
| E-mail: | [anda.hutanu@ro.ey.com](mailto:anda.hutanu@ro.ey.com) |

**Pericolul din spatele zidurilor de apărare, când amenințarea vine din interior**

*Autor: Cristian Zaharia, Manager, Forensic Technnologies and Discovery Services, EY România*

Amenințarea cu un atac informatic nu îi mai surprinde demult pe cei care au în mână destinele unei companii, motiv pentru care, încurajați și de legislația în vigoare referitoare la GDPR, încep să ia cât mai multe măsuri pentru a stopa o eventuală exfiltrare[[1]](#footnote-1) de date sau alterare a acestora. Toate acestea sunt însă în van dacă 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](https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf), lider în domeniul protecției 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 creștere față de valoarea din 2018, de 8.76 milioane dolari/companie. De asemenea, în același interval de timp și numărul de atacuri informatice generate de persoane din interiorul companiei a crescut cu 47%.

Dacă în majoritatea cazurilor vorbim de actuali angajați care se pretează la un moment dat la astfel de acțiuni, nu trebuie neglijați nici partenerii sau colaboratorii care sunt în strânsă legătură cu o companie ori foști angajați care cunosc arhitectura interioară 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 să 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 mână în luptă?”**

Cauzele care duc la aceste incidente pot fi diverse și majoritatea au o strânsă legătură 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 activități:

- **Angajatul neglijent**: în majoritatea companiilor, angajații parcurg cursuri despre modalitatea în care trebuie prelucrate și transmise datele, amenințările la care să fie atenți și procedurile de urmat atunci când constată o activitate suspectă în mediul online. Nu de puține ori se întâmplă să existe persoane care, fie din neștiință, superficialitate ori din dorința de a trece peste anumite reguli pentru a rezolva mai repede o sarcină de serviciu, expun datele informatice ale angajatorului la un risc sporit de a fi transferate neautorizat în mediul extern ori să le afecteze iremediabil (vezi situația unui atac de tip ransomware, când date ale companiei sunt criptate și chiar o eventuală restaurare poate să nu ducă la o recuperare completă a acestora).

- **Angajatul rău-intenționat**: o mărire de salariu care nu a fost pe măsura așteptărilor, o avansare care nu a venit la timpul dorit ori încetarea unilaterală din partea angajatorului a contractului de muncă sunt situații în care anumite persoane își pierd simțul rațiunii și recurg la acte de răzbunare. 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 gravă formă 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 să le vândă pe Darkweb și să obțină astfel avantaje materiale. De asemenea, au mai fost întâlnite deseori situații în care persoane care supravegheau active financiare ale companiei, beneficiind de încrederea care li se acordă combinată cu anumite lipsuri în supravegherea activității acestora, au extras, prin diferite artificii în sistemul informatic al companiei, sume de bani pe care le-au folosit ulterior în interes personal.

**Cum protejăm datele companiei respectând dreptul angajatului la viața privată?**

Din ce în ce mai multe companii au adoptat o cultură organizațională sănătoasă care pune în centrul ei angajatul și fidelizarea acestuia. Din acest motiv, implementarea unor măsuri care să prevină situațiile în care unul dintre aceștia s-ar putea întoarce împotriva angajatorului trebuie luate cu mare atenție pentru a nu afecta libertatea și drepturile majorității. Această abordare face însă ca un astfel de atac să fie și mai greu de identificat.

Practica a arătat că mecanismele care trebuie adoptate trebuie să aibă în vedere atât nevoia de a proteja datele companiei, cât și dreptul angajatului la viața privată. Este prevăzut fără echivoc atât de către legislația muncii, cât și de cea privind protecția datelor cu caracter personal faptul că angajatul beneficiază de dreptul la viață privată chiar și atunci când operează de pe dispozitive aflate în administrarea companiei la care lucrează. Astfel, răspunsul la această problemă nu este unul singur, ci mai degrabă reprezintă un mixt între diferitele controale care pot fi puse la un loc pentru a preveni sau identifica la timp acest tip de activități.

1) Controale tehnice: implementarea de soluții de prevenire și stopare a exfiltrării de date informatice, așa numitele *Data Loss Prevention,* care pot fi configurate pe nevoia fiecărei companii în parte, astfel încât să alerteze și/sau stopeze în momentul când anumite date sunt scoase în afara companiei. De asemenea, această măsură este bine să fie completată și prin configurarea unor mecanisme prin care datele stocate sau în tranzit sunt criptate, astfel orice interceptare a acestora, fie ea și accidentală, să nu supună compania la un risc.

2) Măsuri 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 normală să poată fi semnalate. În plus, principiul separației sarcinilor trebuie să fie o regulă astfel încât o acțiune să nu poată fi dusă la bun sfârșit decât prin colaborarea a două sau mai multe persoane, fiecare cu diferite atribuții. Un exemplu clasic ar fi situația în care cineva identifică acțiunea care trebuie întreprinsă și demarează procedurile, o altă persoană aprobă și o a treia execută plata.

În completarea acestor măsuri ar trebui să 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 căror activitate zilnică implică schimbul de date constant cu entități din afara companiei, cu siguranță există numeroase alte compartimente care lucrează cu date sensibile și care nu ar implica transferul de date spre exterior.

Nu în ultimul rând, nu trebuie uitată existența unei proceduri de lucru de răspuns la acest tip de evenimente constând într-un plan de răspuns la incidente informatice și diferite fluxuri de activități în funcție de specificul fiecărui atac suferit.

3) Coordonare între departamentul de HR și IT: Poate cea mai delicată componentă din lista recomandărilor întrucât nevoia unei astfel de colaborări are loc în momentul în care sunt suspiciuni clare cu privire la existența unui atacator din interior. Astfel, departamentele de HR pot să anunțe echipa de monitorizare a incidentelor în momentul în care sunt indicii că o persoană a manifestat intenții vădite cu privire la o astfel de activitate. Această măsură trebuie cuprinsă expres în cadrul unei proceduri, cu indicarea clară a situației în care activitatea profesională este monitorizată, pentru a nu lăsa loc abuzurilor din partea angajatorilor, care în ideea protejării rețelei exercită un control ce poate fi intimidant și chiar ilegal pentru persoanele de bună credință, care, din fericire, reprezintă majoritatea covârșitoare.

**Echilibru în adoptarea măsurilor**

Realitatea a dovedit că astfel de activități de rea-credință îndreptate împotriva datelor informatice ale companiei (în unele cazuri chiar împotriva propriilor colegi) sunt o realitate de care fiecare decident trebuie să țină cont. Însă, cel mai important este găsirea unui echilibru între crearea unei culturi organizaționale axate pe încredere și profesionalism și dezvoltarea unor mecanisme obiective de monitorizare, identificare și răspuns eficient în cazul în care sunt indicii ale unui atac informatic din interior. Oricare mișcare spre una dintre cele două extreme poate cauza fie un mediu impropriu de lucru pentru cea mai importantă resursă, oamenii, fie un risc iminent de compromitere a datelor informatice, această situație din urmă venind la pachet și cu alte inconveniente atât de natură contravențională, cât și penală în anumite cazuri.

\*\*\*

**Despre EY România**

EY este una dintre cele mai mari firme de servicii profesionale la nivel global, cu 312.250 de angajați în peste 700 de birouri în 150 de țări și venituri de aproximativ 40 miliarde de USD în anul fiscal încheiat la 30 iunie 2021. Rețeaua noastră este cea mai integrată la nivel global, iar resursele din cadrul acesteia ne ajută să le oferim clienților servicii prin care să beneficieze de oportunitățile din întreaga lume.  
Prezentă în România din anul 1992, EY este liderul de pe piața serviciilor profesionale. Cei peste 800 de angajați din România și Republica Moldova furnizează servicii integrate de audit, asistență fiscală, juridică, strategie și tranzacții, consultanță către companii multinaționale și locale. Avem birouri în București, Cluj-Napoca, Timișoara, Iași și Chișinău. EY România s-a afiliat în 2014 singurei competiții de nivel mondial dedicată antreprenorialului, EY Entrepreneur Of The Year. Câștigătorul ediției locale reprezintă România în finala mondială ce are loc în fiecare an, în luna iunie, la Monte Carlo. În finala mondială se acordă titlul World Entrepreneur Of The Year. Pentru mai multe informații, vizitați pagina noastră de internet: [www.ey.com](http://www.ey.com)

1. exfiltrarea datelor reprezintă furtul sau eliminarea sau mișcarea neautorizată a oricăror date de pe un dispozitiv [↑](#footnote-ref-1)