Frauda „Mesaj de la șef” în perioada pandemiei

Anual, sute de mii de companii devin victime ale unei fraude cu un mod de operare îndrazneț, frauda pentru care specialiștii au oferit nume diferite, precum Mesaj de la șef, CEO Fraud, Business Email Compromise, Email Account Compromise sau Invoice Fraud. Indiferent de denumire, potrivit statisticii, se estimeaza ca în fiecare luna pierderile sunt de peste 300 milioane de USD.

Apariția pandemiei COVID-19 și limitarile aduse au generat un context favorabil pentru autorii unor astfel de fraude, motiv pentru care, în aceasta perioada, numarul acestora a cunoscut o explozie fara precedent. Astfel, cu titlu de exemplu:

- prin *spoofing*, atacatorul pretinde ca e CEO-ul companiei, impersonând adresa de e-mail folosita de acesta, și anunța ca tocmai a fost infectat cu COVID-19. Drept urmare, susține ca are nevoie de ajutorul angajatului „victima” pentru finalizarea unei tranzacții sensibile, urgente și confidențiale;
- atacatorul, care pretinde ca este liderul companiei, solicita departamentului financiar efectuarea unei plați urgențe pentru achiziționarea de medicamente, teste sau echipament de protecție, cu „*maxima urgența*”;
- atacatorul, folosind o adresa de email care pare sa aparțina unui CEO sau altei persoane cu autoritate din cadrul companiei, transmite un mesaj „*Stay safe!*” (specific acestei perioade), urmat de solicitarea disponibilității angajatului “victima” de a-i oferi sprijin pentru finalizarea unor tranzacții;
- atacatorul, care pretinde ca e angajat al companiei, anunța departamentul HR sau financiar despre schimbarea contului pentru plata drepturilor sale, având în vedere limitarile de deplasare impuse de pandemie;
- atacatorul, care pretinde ca e CEO sau alta persoana cu autoritate în companie, solicita finalizarea urgenta și confidențiala a unei tranzacții (investiție, depozit, achiziție, fuziune, etc) care a fost întârziata de pandemie.

Pe scurt, faptuitorul pretinde, în mod credibil și prin diverse metode, a fi CEO sau o alta persoana cu autoritate din cadrul companiei, pentru a determina efectuarea unei plați autorizate catre un cont aflat sub controlul sau.

În România, în fiecare saptamâna, departamentele antifrauda și de conformitate din cadrul bancilor sunt confruntate cu solicitari ale autorităților de aplicare a legii sau ale clienților legate de tranzacții efectuate ca urmare a acestui tip de frauda, în condițiile în care nu este neobișnuit ca o singura asemenea tranzacție sa aiba o valoare de mai multe sute de mii de euro. De exemplu, în 2013 reprezentanța din România a unei companii multinaționale din domeniul telecomunicațiilor a fost prejudiciata cu 1,8 milioane EUR. În 2016, o alta companie care activeaza și în România a efectuat plați în valoare de 40 milioane EUR prin una dintre modalitațile de comitere a acestei fraude.

Acest tip de frauda speculeaza cea mai vulnerabila veriga din lanțul de aparare împotriva fraudei: omul. Prin

verificari şi testari specializate şi preferabil independente ale cadrului intern de prevenire şi identificare a fraudei, prin pregatire periodica şi de substanţa a personalului companiei, se poate preveni cu succes apariţia unui astfel de caz care ar putea sa ameninţe însaşi sustenabilitatea afacerii.

Ce trebuie facut daca tocmai am aflat ca am fost victima unei astfel de fraude?

În primul rând, se va încerca cât mai repede **oprirea plații** respective. Se va contacta urgent banca prin care s-a ordonat transferul şi i se va solicita sprijin pentru oprirea plații în banca corespondenta. Este de avut în vedere faptul ca o întârziere de câteva ore poate face acest demers inutil. Atacatorii vor redirecționa sumele încasate catre o alta jurisdicție, de îndata ce banii au intrat în contul aflat în controlul lor.

În al doilea rând, se va urmari **limitarea pagubei**. Mai precis, se va stabili daca sunt programate alte plați catre contul indicat de atacator şi daca au fost schimbate recent şi alte conturi ale furnizorilor sau angajaților, catre care ar urma sa se efectueze plata.

În continuare, se impune o **investigare exhaustiva** a condițiilor care au determinat efectuarea plații. Investigația trebuie facuta în cea mai profesionista maniera pentru a culege toate datele şi a stabili cu precizie situația de fapt şi persoanele implicate, dar şi pentru a nu contamina probele pentru acțiunile legale ulterioare (fie penale, civile sau administrative). O atenție marita trebuie acordata mediului electronic care trebuie conservat fara a fi alterat (forensic data acquisition), dar şi modului de susținere a interviurilor cu personalul implicat (se va avea în vedere şi scenariul în care, la comiterea fraudei, s-a oferit sprijin din interior).

Investigația va urmari stabilirea gravitații atacului şi identificarea tuturor datelor sensibile care au fost puse la dispoziția atacatorilor.

Dupa ce au fost colectate toate probele din mediul digital, se va proceda la **restaurarea şi remedierea sistemelor afectate**, schimbarea parolelor, îmbunatațirea politicii de acces, adaugarea de noi controale, etc.

Angajații companiei şi, îndeosebi, cei din poziții cheie, (contabilitate, financiar, resurse umane, etc) vor fi instruiți cu privire la modul în care s-a savârşit frauda pentru a se preveni apariția unui atac similar (care va fi mai facil pentru atacator, având în vedere ca deja a avut acces la multe date confidențiale).

Împreuna cu specialiştii, se va analiza existența unei eventuale raportari a incidentului: în cazul în care au fost expuse date personale, obligația de raportare catre Autoritatea Națională de Supraveghere a Prelucrarii Datelor cu Caracter Personal sau, în cazul unui atac informatic la un operator de servicii esențiale conform Directivei NIS, transpusa prin legea 362/2018, obligația de raportare catre CERT-RO.

Totodata, se va analiza şi gestiona relația cu partenerii de afaceri afectați de incident (de exemplu furnizori ale caror date au fost transmise atacatorilor), pentru ca, la rândul lor, aceştia pot deveni victime pe baza informațiilor sensibile transmise.

Nu în ultimul rând, deşi de cele mai multe ori exista o reținere în acest sens, se recomanda **formularea unei plângeri penale**. Chiar daca probabilitatea de recuperare a sumelor transferate nu este foarte mare, un astfel de demers legal va avea un efect de descurajare pe termen lung a autorilor unei astfel de fraude.

Principalele modalitați prin care un infractor poate determina o companie sa efectueze o plata neautorizata catre un cont pe care îl controleaza

Cea mai ingenioasa şi aparent cea mai simpla metoda este social engineering – ingineria sociala: atacatorul culege date despre companie şi despre reprezentanții sai, dupa care interacționeaza telefonic sau prin email cu angajați din

poziții cheie (contabilitate, financiar, HR) pentru a obține date sensibile (de exemplu, lista furnizorilor cu facturi de valoare mare ce urmeaza a fi scadente în perioada urmatoare) sau pentru a determina efectuarea unei plaţi pentru o achiziție urgenta.

O alta metoda, mai tehnica, presupune trimiterea unor email-uri care urmaresc obținerea accesului la sistemul informatic al companiei (phishing, spear phishing, executive whaling) în vederea schimbarii coordonatelor de plata ale principalilor furnizori sau pentru executarea unor noi plați.

Aceste modalitați de comitere au trei elemente comune:
- atacatorul **pretinde a fi altcineva**, în cadrul companiei (CEO, CFO) sau din afara acesteia (avocat, auditor, furnizor);
- se invoca **urgența** și **confidențialitate**, respectiv plata trebuie efectuata în cel mai scurt timp în contul indicat, fara a fi informate alte persoane din companie;
- se solicita **o plata catre un cont anume** sau **schimbarea contului** pentru o plata ce urmeaza sa fie facuta catre un furnizor existent.