http://www.luju.ro/atentie-la-frauda-bec-zeci-de-mii-de-societati-comerciale-romane-si-straine-au-ajuns-victimele-schemei-informatice-supranumite-business-e-mail-compromise-fraud-in-doar-trei-ani-frauda-de-tip-bec-a-provocat-daune-de-peste-6-miliarde-dolari-in-romania-igpr

LUMEA JUSTITIEI

ATENTIE LA FRAUDA BEC – Zeci de mii de societati comerciale romane si straine au ajuns victimele schemei informatice supranumite Business E-mail Compromise Fraud. In doar trei ani, frauda de tip BEC a provocat daune de peste 6 miliarde dolari. In Romania, IGPR a inregistrat sute de sesizari pe frauda BEC, fiind reclamate prejudicii si de 40 milioane euro. Tansferurile online pentru efectuare platilor usureaza munca hackerilor. Datele din e-mail vulnerabilizeaza firmele

Scris de E.D. | Data: 26.09.2019 17:29

Lumea Justitiei aduce in atentia publica un fenomen care ia amploare in Romania si care are consecinte dintre cele mai negative pentru societatiile comerciale din tara, pradate deja de milioane de euro, anual, de hackeri care au implementat un sistem ce capata dimensiuni inimaginabile. Este vorba despre un mod de operare numit **Business E-mail Compromise Fraud – cunoscut si ca frauda de tip BEC** – care **vizeaza transferurile bancare efectuate intre societati comerciale**. Conform descrierii expertilor care au analizat fenomenul, **frauda de tip BEC este definita ca fiind unul dintre cele mai complexe moduri de operare ale hackerilor care si-au stabilit ca tinte societatile comerciale care lucreaza cu furnizori sau clienti straini** (activitati de comert exterior) **si care efectueaza cu regularitate plati prin transfer bancar.** Mai grav este ca frauda de tip BEC implica scheme complexe de anonimizare din partea hackerilor si sunt dificil sau aproape imposibil de identificat, avand in vedere sistemele informatice de anonimizare a traficului, utilizarea de documente falsificate si caracterul transfrontalier al activitatilor.

Atentie la BEC

Astfel cum precizam mai sus, Business Email Compromise (BEC) este o schema informatica care vizeaza atat intreprinderile mari cat si pe cele mici, de pe urma carora sa poata fi realizate importante castiguri financiare. Astfel cum este descrisa, BEC poate lua multe forme. Cea mai frecventa dintre acestea presupune fie ca un **fals angajat** sa modifice datele de facturare ale unei societati cu datele de cont ale acestuia, fie sa solicite **transferuri de fonduri intr-un timp foarte scurt**. Multe cazuri de BEC se bazeaza exclusiv pe **tehnici de inginerie sociala si adrese pe e-mailuri clonate**, ori soft-uri de tip malware, care pot distruge calculatoarele, astfel incat sa faca posibila accesarea sistemelor informatice si a informatiilor despre companie de catre hackeri.

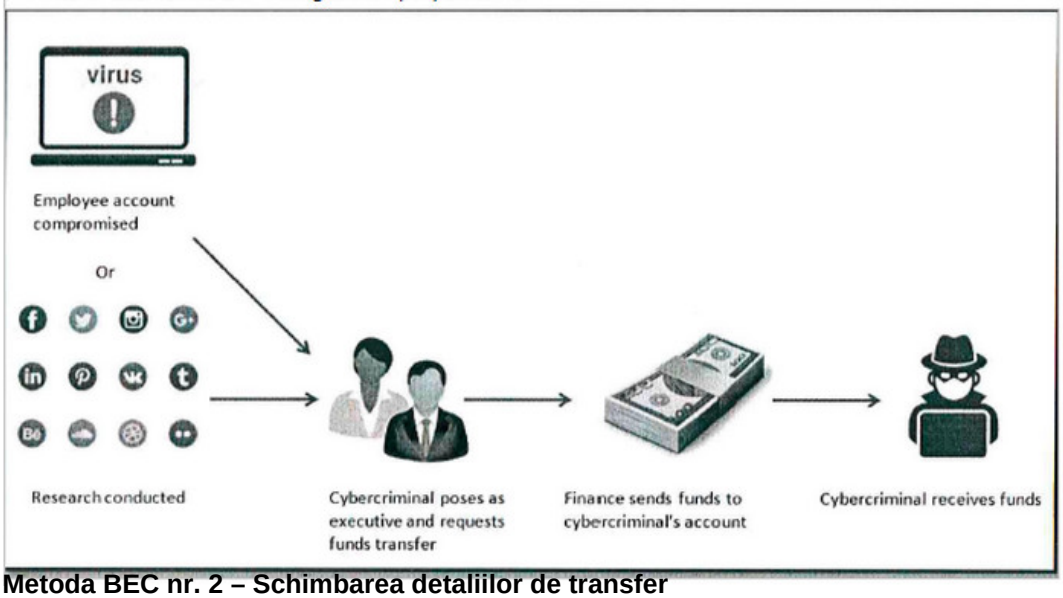
Prezentam mai jos cele mai utilizate metode de BEC:

Metoda BEC nr. 1 – Seful companiei

Cea mai comuna metoda BEC este cea in care **un "actor informatic" se prezinta ca fiind directorul executiv al unei companii, clonand adresa de e-mail a directorului executiv real, calitate din care solicita transferuri urgente de fonduri**. Acest "actor informatic", inainte de a actiona, efectueaza o documentare a societatii comerciale pornind de la bazele de date publice. In continuare, "actorul informatic" poate compromite conturile de e-mail ale angajatilor, in vederea obtinerii de informatii despre angajati, structura afacerii, stilurile de scriere ale directorilor si angajatilor, pentru a le imita intocmai.

Figura 1:

FIGURE 1: BEC method one - Posing as a company executive.

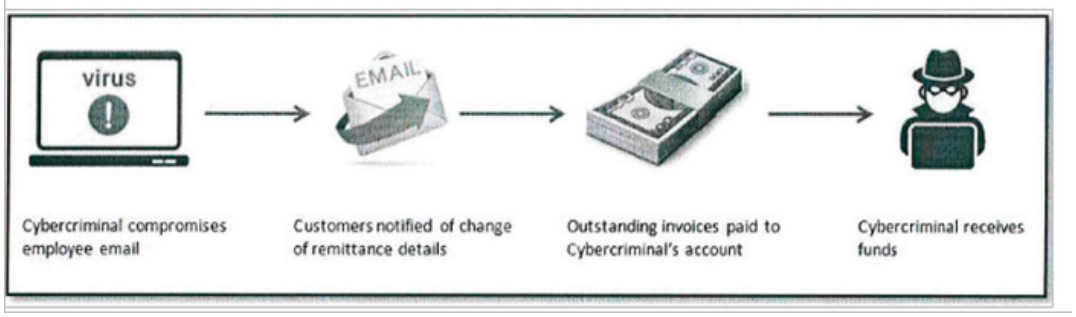


Metoda BEC nr. 2 – Schimbarea detaliilor de transfer

De aceasta metoda sunt vizate, in principal, **societatile comerciale care au stabilit relatii financiare cu furnizorii.** In aceste cazuri, "actorul informatic" urmareste compromiterea computerului unui angajat al societatii in vederea obtinerii datelor legate de furnizori si plati/facturi. Odata virusat computerul angajatului, **"actorul informatic" cloneaza adresa acestuia de e-mail de unde mai apoi inlocuieste datele de facturare si detaliile bancare, astfel incat sumele sa fie transferate in conturile hackerilor.** Se ajunge in situatia ca, in timp, toate facturile sa fie platite in conturile hackerilor, in loc sa fie platite in conturile societatii comerciale.

Figura 2:

FIGURE 2: BEC Method Two - Change of Remittance Details.

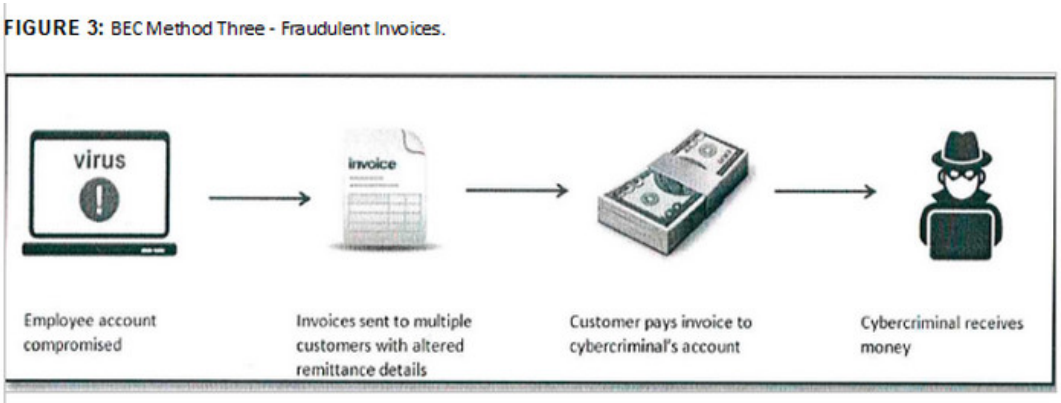


Metoda BEC nr. 3 – Facturi frauduloase

Cea de-a treia metoda BEC este similara cu cea de-a doua, dar mai "proactiva" in sensul ca, dupa compromiterea computerului unui angajat al unei societati comerciale in vederea obtinerii datelor companiei, "actorul informatic" nu se va limita la a inlocui datele de facturare astfel incat platile sa se efectueze in conturile sale. **Folosindu-se de adrese de e-mail clonate, "actorul informatic" va transmite clientilor societatii comerciale mai multe facturi pentru diverse servicii in vederea achitarii acestora.**

Figura 3:

FIGURE 3: BEC Method Three - Fraudulent Invoices.



Politia Romana alertata de fenomenul BEC

La nivelul institutiilor de aplicare a legii din Romania, incepand cu luna decembrie a anului 2015, au fost primite din ce in ce mai multe **sesizari referitoare la modul de operare Business E-mail Compromise Fraud „BEC Fraud”.** Conform datelor statistice, **la nivelul Politiei Romane s-a constatat ca firmele din Romania care desfasoara activitati comerciale (cu personalitate juridica romana) cu societatile comerciale straine au dobandit calitatea de victima a hackerilor.** De altfel, aceeasi analiza a relevat ca in aproape toate cazurile in care a fost semnalata compromiterea sistemelor informatice ale unor societatilor comerciale straine, acestea se aflau in relatii comerciale cu cele romanesti, fiecare dintre agentii comerciali precizand ca **utilizeaza transferuri online ca metoda curenta de efectuare a platilor catre furnizori sau parteneri externi de afaceri, in baza unei relatii comerciale anterioare si a bunei credinte in practica comerciala.**

De retinut este insa ca societatile comerciale romanesti fraudate nu au un tipic anume de activitate, **singurul element comun fiind reprezentat de faptul ca toate desfasoara activitati de comert exterior si efectueaza plati curente in strainatate.**

Astfel, incepand cu anul 2016, la nivelul Inspectoratului General al Politiei Romane – Directia de Combatere a Criminalitatii Organizate (DCCO) au fost inregistrate peste 200 de sesizari oficiale referitoare la frauda BEC, prejudiciile cauzate societatilor comerciale din Romania fiind variate, in sensul ca cel mai mare a fost de 40 milioane de euro, in timp ce valoarea medie se situeaza la 100.000 de euro.

Alarmant este ca la nivel global emergenta acestui tip de frauda a generat pierderi documentate de peste 6 miliarde de dolari, in perioada 2016-2017, fiind inregistrate peste 40.000 de incidente de acest tip.

Frauda de tip BEC are urmatoarele componente principale:

1.**Componenta de Social Engineering** – prin care se strang date istorice online referitoare la societatile tintite (sediu social, persoane din management, CUI, cont bancar, adrese de posta electronica, portofoliu de clienti, eventuale documente accesibile online ce prezinta elemente de identificare ale societatii comerciale) ce pot fi utilizate pentru a crea aparenta de legitimitate;

2.**Componenta de intruziune/compromitere a adresei de posta electronica.** (EAC – Email Account Compromise.)

3**.Deschiderea unei societati comerciale in afara tarii** unde isi desfasoara activitatea compania tinta;

4.**Deschiderea unui cont bancar sau conturi bancare cu acte reale sau false** in strainatate pe numele furnizorului sau clientului strain al companiei tinta;

5**.Generarea unor transferuri bancare** prin manipularea segmentului financiar contabil a companiei tinta.

Schema infractionala presupune accesarea in mod neautorizat a conturilor de e-mail ale unor societati comerciale din strainatate, monitorizarea corespondentei purtate de catre angajatii respectivei societati si simularea corespondentei reale cu societatea partenera din Romania, prin intermediul unei adrese de e-mail asemanatoare sau identice.

Aceasta activitate are de regula ca finalitate, deturnarea transferului de bani catre un cont bancar diferit fata de cel al beneficiarului legitim, acest cont bancar fiind controlat de catre alti membri ai gruparii infractionale.

Elemente generale de protectie si preventie din zona guvernantei corportive :

Societatile comerciale care constientizeaza si inteleg existenta acestui tip de frauda prezinta un risc mult mai scazut de a cadea victima acestui tip de activitate si pot recunoaste mai usor tentativele de acest gen, astfel probabilitatea efectuarii unor transferuri eronate scazand substantial.

Instruirea personalului referitor la tipologia de frauda

Societatile comerciale care beneficiaza de un sistem de securitate online solid (mai ales pentru sistemele informatice utilizate de personalul „front line”) prezinta un risc mult mai scazut de a cadea victima incidentelor de tip EAC.

Implementarea de masuri IT si politici de securitate

Se recomanda o atentie sporita la publicarea in mediul online, in special in zona social media si pe site-ul companiei, a informatiilor detaliate privind ierarhia persoanelor ce activeaza in cadrul companiei, a indatoririlor acestora sau a detaliilor de tip out of office precum si a conturilor bancare si a detaliilor complete si mijloacelor de comunicatie utilizate.

Strategii de protectie si preventie impotriva EAC/BEC:

-**A se evita utilizarea conturilor de email web-based (yahoo, hotmail, gmail etc)** pentru activitatea societatii comerciale. Recomandabila este utilizarea unor conturi de email dintr-un domeniu propriu.

-Atentie la mesajele in care se solicita efectuarea unor operatiuni in secret sau a unor operatiuni rapide catre destinatari incerti sau neverificati.

-**Luarea in considerare a posibilitatii crearii unor proceduri minimale de audit IT** si de securitate referitoare la plati, in sensul implementarii unei verificari in minim doi pasi.

-Stabilirea unei comunicari alternative, cum ar fi cea telefonica cu furnizorul sau clientul strain pentru a valida orice schimbare a practicii comerciale statuate, pentru a elimina posibilitatea hackerului de a intercepta o eventuala comunicatie.

-Utilizarea de semnaturi digitale sau a criptarii mesajelor intre partile implicate in activitatea comerciala.

-Raportarea si nedeschiderea mesajelor nesolicitate sau de tip SPAM acestea putand contine malware.

-Nu se recomanda utilizare functiei „Reply” pentru a raspunde in corespondenta de serviciu. In schimb se recomanda functia „Forward” si scrierea manuala a adresei de email unde se doreste transmiterea mesajului.

Recomandare generala pentru preventia unor astfel de atacuri de tip BEC vizeaza precautia in ce priveste schimbarea subita a unor practici comerciale stabilite anterior, in special a conturilor de e-mail sau conturilor bancare si a valutelor in care se fac platile, precum si tarii in care sunt deschise conturile. Pentru aceasta este recomandabila verificarea telefonic, si nu prin e-mail, direct la furnizor/client a oricarei schimbari de practica, intotdeauna pe un numar de telefon detinut anterior si verificat.

***Cititi aici mai multe detalii despre Frauda de tip BEC**