OUCH! | Iulie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Ce este escrocheria CEO?**
- **Cum să vă protejați**

Escrocheria CEO

Ce este escrocheria CEO?

Infractorii cibernetici sunt vicleni, ei găsesc mereu mijloace noi prin care să obțină ceea ce vor. Una dintre metodele lor cele mai eficiente este să aibă în vizor oameni ca dumneavoastră. Răufăcătorii și-au dat seama că oamenii neștiutori sunt veriga slabă într-o organizație, uitând că cei informați, cum sunt cititorii buletinului informativ OUCH!, pot fi cea mai bună defensivă a unei companii.

Editor Invitat

Angela Pappas este directorul programului de instruire în securitatea informației la Thomson Reuters. În această postură, Angela este responsabilă de coordonarea ambasadorilor programului, a programului de eLearning, cât şi de educarea angajaților cu privire la atacurile de phishing.

Infractorii cibernetici au creat un nou tip de atac, denumit escrocherie CEO, cunoscut și drept Compromiterea Email-ului de Business. În acest gen de atac, răufăcătorul pretinde că este șeful executiv — CEO — sau alt director din compania dumneavoastră. Infractorii trimit un email către angajați ca dumneavoastră încercând să vă păcălească să faceți ceva ce nu ar trebui să faceți. Aceste tipuri de atacuri sunt extrem de eficiente pentru că, de obicei, răufăcătorii își fac temele. Ei studiază site-ul companiei dumneavoastră pentru a afla informații despre localizarea acesteia, cine sunt conducătorii ei și numele altor companii cu care colaborează. Apoi, infractorii adună cât mai multe informații despre angajații companiei de pe site-uri ca LinkedIn, Facebook sau Twitter. Odată ce cunosc structura organizațională, încep să se informeze asupra anumitor angajați. Ei își aleg victimele potrivit scopurilor pe care le urmăresc. Dacă răufăcătorii vor bani, își vor concentra atenția asupra angajaților din departamentul plăți. Dacă urmăresc informații fiscale, vor viza angajații departamentului de resurse umane. Dacă au în vedere accesul la bazele de date, ei pot lua în colimator pe cineva din departamentul IT.

Odată ce-au stabilit ce urmăresc și cine le e victima, încep să-și pregătească atacul. Deseori folosesc atacurile de phishing țintite (Spear phishing). Phishing este atunci când atacatorul trimite un email la milioane de oameni cu scopul de a-i determina să facă ceva anume, bunăoară deschizând un fișier infectat sau vizitând un site compromis. Atacurile de phishing țintite sunt similare, dar în loc să trimită un email generic la milioane de oameni, vor trimite un mesaj personalizat, ce se adresează unui număr restrâns de oameni aleși cu grijă. Aceste mesaje de phishing țintit sunt foarte realiste ca aspect și greu de identificat. Deseori ele par să fie trimise de cineva cunoscut sau cu care colaborați, cum ar fi un coleg de serviciu sau superiorul ierarhic. Mesajele sunt realiste pentru că reproduc limbajul folosit de colegi; ele pot conține logo-ul organizației

Escrocheria CEO

sau chiar semnătura oficială a unuia dintre directori. Aceste mesaje creează adesea un sentiment deosebit de urgență, cerându-vă să acționați imediat, fără a informa pe altcineva. Scopul răufăcătorilor este să vă grăbească să faceți o greșeală. Iată trei dintre cele mai frecvente scenarii:

Escrocheria CEO este un atac puternic ce poate depăși majoritatea elementelor de securitate. În ultimă instanță, tu însuți ești cea mai bună defensivă.

- **Transferul bancar**: Un răufăcător este în căutare de bani. Asta înseamnă că vor căuta și vor afla cine lucrează în departamentul de plăți sau echipa care gestionează finanțele organizației. Infractorii vor crea și trimite apoi un mesaj pretinzând că sunt superiorul acestora; mesajul le spune că a intervenit o urgență și trebuie transferați bani neîntârziat către un anumit cont.

- **Frauda fiscală**: Infractorii cibernetici vor să obțină informații despre colegii dumneavoastră de serviciu, așa că vor pretinde că sunt angajați, pentru a fura date fiscale. Ei studiază compania și află cine gestionează datele personalului, spre exemplu cineva din departamentul de resurse umane. Plecând de la asta, răufăcătorii trimit mesaje email falsificate pretinzând că sunt unul dintre directorii executivi sau poate cineva din departamentul juridic, cerând apoi ca anumite documente să le fie trimise imediat.

- **Uzurparea identității avocatului**: Nu toate escrocheriile de acest gen implică doar folosirea email-ului, sunt întâlnite și alte variante cum ar fi folosirea telefonului. În acest scenariu, infractorii încep prin a vă trimite un email, pretinzând că sunt unul dintre conducătorii organizației, aducându-vă la cunoștință că vă va suna un avocat în legătură cu o chestiune urgentă. Infractorul vă sună din nou, pretinzând că este avocatul. Acesta vă induce astfel un sentiment deosebit de urgență, în timp ce vorbește de chestiuni confidențiale ce nu suportă niciun fel de amânare. Acest sentiment de urgență vă înșală, făcându-vă să acționați imediat.

Cum să vă protejați

Așadar, ce puteți face pentru a vă proteja organizația și pe dumneavoastră înșivă? Simțul realității este cea mai bună defensivă. Dacă primiți de la șef sau de la un coleg un mesaj care nu sună tocmai în regulă, ar putea fi un atac. Indiciile ar putea fi caracterul extrem de urgent al mesajului, o semnătură care nu pare corectă, un anumit ton pe care nu l-ați fi așteptat niciodată sau numele folosit în mesaj nu corespunde modului în care sunteți apelat de obicei. Un alt indiciu

Escrocheria CEO

ar fi acela că răufăcătorul folosește o adresă de email sau un număr de telefon pe care nu le-ați mai văzut niciodată, sau poate folosește o adresă de email foarte asemănătoare dar nu tocmai aceea pe care o are colegul sau superiorul dumneavoastră. Atunci când aveți suspiciuni sunați persoana respectivă pe un număr de telefon de încredere sau întâlniți-vă personal (nu răspundeți la email) și confirmați dacă v-a trimis acel mesaj. Nu ocoliți niciodată politicile și procedurile de securitate. Compania s-ar putea să aibă politici ce definesc procedurile corecte pentru autorizarea transferurilor de fonduri sau dezvăluirea de informații confidențiale. Cererile care încearcă să ocolească aceste politici, indiferent de originea lor aparentă, trebuie să fie considerate suspecte și verificate înaintea oricărei alte acțiuni. Dacă primiți o atare solicitare și nu știți ce-i de făcut, contactați-vă imediat superiorul ierarhic, biroul helpdesk sau echipa de securitate a informației.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS securingthehuman.sans.org/ouch/archives

Versiunea în limba română

Grupul Cegeka este un furnizor privat de servicii IT&C fondat în 1992. Având sediul central în Belgia, Cegeka este prezentă în Austria, Republica Cehă, Franța, Germania, Italia, Luxemburg, Olanda, România și Republica Slovacă. Compania furnizează servicii clienților din întreaga Europă: soluții Cloud pentru companii, servicii de securitate, dezvoltare de aplicații folosind tehnicile Agile, mentorat în metodologii Agile și externalizarea infrastructurii IT&C. Cegeka are 3200 de angajați și a realizat o cifră de afaceri combinată de 330 milioane euro în 2013. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Ingineria socială:	https://securingthehuman.sans.org/ouch/2014#november2014
Despre Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
Ce sunt programele malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Verificarea în doi paşi:	https://securingthehuman.sans.org/ouch/2015#september2015
Recomandarea zilei:	https://www.sans.org/tip-of-the-day

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducere: Cosmin Hănulescu