OUCH! | Noiembrie 2014

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Ingineria Socială**
- **Detectarea / Stoparea atacurilor de tip inginerie socială**
- **Prevenirea altor atacuri**

Ingineria socială

Generalități

O idee preconcepută pe care mulți o au despre infractorii cibernetici este acea că se folosesc numai de instrumente și tehnologii avansate de hacking pentru a accesa fraudulos calculatoare, conturi sau dispozitive mobile. Acest lucru este pur și simplu fals. Acești răufăcători au învățat că una dintre cele mai simple modalități de a fura informația sau de a vă accesa calculatorul este să vă vorbească și să vă păcălească. În acest buletin informativ vom învăța cum reușesc astfel de atacuri îndreptate asupra oamenilor, denumite atacuri de inginerie socială și ce putem face pentru a ne proteja.

Editor Invitat

Alissa Torres este instructor certificat SANS, specializată în investigații avansate în criminalistica informatică și gestiunea incidentelor. Experiența sa include atât lucrul de teren efectiv cât și ca membru al unei echipe interne de securitate, din postura de anchetator în criminalistică digitală. Alissa poate fi găsită pe Twitter la **@sibertor**.

Ingineria socială

Ingineria socială este un tip de atac psihologic în care atacatorul vă determină să faceți ceva ce el intenționează să faceți. Ingineria socială a existat de mii de ani, ideea de a înșela sau a păcăli pe cineva nu este nouă. Cu toate astea, răufăcătorii au realizat că aplicarea acestei tehnici pe Internet este extrem de eficace și poate fi folosită pentru a ajunge la milioane de oameni. Cel mai ușor mod de a înțelege cum funcționează ingineria socială este să aruncăm o privire la un exemplu banal, din realitatea cotidiană.

Primiți un telefon de la cineva care pretinde că este de la o companie de servicii pentru calculatoare, furnizorul de acces Internet sau poate chiar serviciul tehnic de asistență Microsoft. Apelantul explică apoi că au observat un comportament ciudat în funcționarea calculatorului dumneavoastră, cum ar fi scanarea Internetului sau expedierea de mesaje spam, lucru care-i face să creadă că este infectat. Au fost însărcinați să investigheze problema și să ajute la securizarea calculatorului dumneavoastră. Apoi folosesc o varietate de termeni tehnici și vă ghidează printr-o multitudine de pași complicați pentru a vă convinge că este infectat calculatorul dumneavoastră.

De exemplu, vă pot cere să verificați dacă aveți anumite fișiere pe calculator, ghidându-vă pentru a le localiza. Atunci când le-ați găsit, apelantul vă va asigura că acestea sunt confirmarea infectării calculatorului dumneavoastră, când în realitate acestea sunt de fapt fișierele obișnuite ale sistemului de operare, prezente pe orice alt calculator. Odată ce v-au făcut să credeți că este infectat calculatorul, vă vor determina să mergeți pe un anumit site pentru cumpărarea programului lor de securizare sau vă vor cere să le permiteți accesul la distanță pe calculator pentru remedierea problemei. În realitate programul pe care-l vând este de fapt malware. Dacă-l cumpărați și-l instalați nu numai că v-au tras pe sfoară și v-au infectat calculatorul, dar i-ați și plătit

Ingineria socială

ca să o facă. Dacă le dați accesul la distanță pe calculator pentru a remedia problema le dați, în realitate, accesul ca să-l controleze și să-l infecteze.

Țineți minte, atacurile de inginerie socială precum cel descris mai sus nu se rezumă doar la apeluri telefonice, ele se pot întâmpla prin intermediul oricărei tehnologii, incluzând atacuri de tip phishing prin email, mesaje text, mesaje pe Facebook, Twitter sau conversații online. Esențial este să știți la ce să vă așteptați.

Cel mai sigur și eficace pas făcut către protecția proprie este să învățăm să prevenim, să detectăm și să oprim atacurile de inginerie socială.

Detectarea / Stoparea atacurilor de tip inginerie socială

Cel mai simplu mod de protecție împotriva atacurilor de inginerie socială este să folosim logica elementară. Dacă ceva pare suspect sau nu e tocmai în regulă, ar putea fi un atac. Printre indiciile frecvente care arată un atac de inginerie socială se numără:

- Cineva care creează sentimentul unei mari urgențe. Dacă aveți senzația că sunteți presați să luați o decizie pripită, fiți suspicioși.
- Cineva care cere informații pe care nu ar trebui să le acceseze sau pe care ar trebui să le cunoască deja.
- Ceva ce pare prea bun ca să fie adevărat. Un exemplu banal este să fiți anunțați că ați câștigat la loterie, deși nu ați participat.

Dacă suspectați pe cineva care intenționează să vă facă victima unui atac de inginerie socială, nu mai comunicați cu acea persoană. Dacă e cineva care vă sună la telefon, închideți. Dacă e cineva dintr-o conversație online, închideți-o. Dacă e un mesaj email în care nu aveți încredere, ștergeți-l. Dacă atacul are legătură cu serviciul, asigurați-vă că ați anunțat imediat departamentul Help Desk sau echipa de securitate a informației.

Prevenirea altor atacuri

Din fericire există măsuri de precauție pe care le puteți lua ce ajută în prevenirea expunerii pe viitor la atacuri de inginerie socială.

- **Nu dezvăluiți parolele**. Nicio organizație nu vă va contacta vreodată cerându-vă parolele personale. Dacă cineva vă cere o parolă, este un atac.

- **Nu faceți accesibile prea multe informații**. Cu cât e mai multă informați despre dumneavoastră accesibilă unui atacator, cu atât mai ușor le va fi ca să afle cum vă pot trage pe sfoară determinându-vă să faceți ce vor. Cu

Ingineria socială

cât publicați mai puține informații personale, inclusiv pe site-urile de socializare online, comentariile la produse cumpărate, grupuri sau liste de discuții, cu atât mai puține șansele să fiți atacați.

- **Verificați datele de contact**. Ocazional veți fi contactați din motive întemeiate de către bancă, compania de credit, furnizorul de servicii de telefonie mobile sau alte organizații. Dacă aveți orice fel de îndoială asupra legitimității unui astfel de apel, cereți persoanei care v-a sunat numele și numărul de telefon. Apoi obțineți numărul de telefon al companiei dintr-o sursă de încredere, cum ar fi, spre exemplu, numărul imprimat pe spatele cardului de credit, cel de pe extrasul de cont bancar sau numărul de contact de pe site-ul companiei (scrieți dumneavoastră însivă adresa în programul de navigare Internet). Astfel, atunci când luați legătura cu compania respectivă, sunteți sigur că vorbiți chiar cu ei. Deși poate părea o complicație inutilă, protejarea identității și datelor personale fac să merite efortul suplimentar.

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 http://www.securingthehuman.org

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 suplimentare

Despre atacurile de tip phishing prin email:	http://www.securingthehuman.org/ouch/2013#february2013
Despre siguranța pe platformele de socializare:	http://www.securingthehuman.org/ouch/2013#march2013
Despre evitarea escrocheriilor:	http://www.onguardonline.gov/topics/avoid-scams

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