OUCH! | Ianuarie 2017

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Ce este ingineria socială**
- **Detectarea și stoparea atacurilor de inginerie socială**

Ingineria socială

Generalități

O convingere greșită pe care mulți oameni o au despre infractorii cibernetici este că aceștia folosesc instrumente și tehnici foarte avansate pentru a accesa fraudulos conturile și calculatoarele altora. Acest lucru este pur și simplu fals. Acești răufăcători au învățat că, deseori, cel mai ușor mod în care vă pot fura informațiile personale, accesa conturile sau infecta sistemele este să vă determine să faceți o greșeală. În acest buletin informativ veți învăța cum reușesc aceste atacuri numite inginerie socială și cum să vă protejați de ele.

Editor Invitat

James Lyne (**@jameslyne**) este instructor certificat SANS și coordonatorul programului de cercetare la nivel global al companiei Sophos. Analizează disecând prin inginerie inversă cele mai recente și proeminente realizări ale infractorilor cibernetici. Este de asemenea autor al cursurilor Metasploit (SEC580) și Ingineria Socială (SEC567) la institutul SANS.

Ce este ingineria socială

Ingineria socială este un tip de atac psihologic în care atacatorul vă determină să faceți ceva ce nu ar trebui să faceți. Conceptul de inginerie socială nu este nou, a existat de mii de ani. Gândiți-vă la șarlatani și farsori, este aceeași idee. Ce face ca tehnologia actuală să fie atât de eficace pentru răufăcători este că nu-i puteți vedea fizic, ei pot pretinde cu ușurință că sunt orice sau oricine vor, și pot viza milioane de oameni de oriunde în lume, inclusiv pe dumneavoastră. În plus, atacurile de inginerie socială pot ocoli multe tehnologii de protecție. Cel mai ușor mod de a înțelege cum funcționează acest tip de atacuri și a vă proteja este să aruncăm o privire la două exemple 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 de la compania Microsoft. Apelantul vă explică apoi că sistemul dumneavoastră scanează activ rețeaua Internet, lucru care-i face să creadă că este infectat și că au fost însărcinați să vă ajute să vă securizați calculatorul. 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 din lume. Odată ce v-au făcut să credeți că este infectat calculatorul, vor face presiuni 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

Ingineria socială

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 ca să o facă. Dacă le dați accesul la distanță pe calculator, vor prelua controlul asupra acestuia, vă vor fura datele personale sau îl vor folosi pentru ofertele lor.

Simțul realității este cea mai puternică defensivă în identificarea și stoparea majorității atacurilor de inginerie socială.

Un alt exemplu este atacul prin intermediul mesajelor email, cunoscut ca Escrocheria CEO, deseori întâlnit la serviciu. Acesta se întâmplă atunci când un răufăcător studiază online compania la care lucrați și identifică numele superiorului ierarhic sau al directorului executiv. Escrocul construiește apoi un mesaj email ce pretinde că vine de la acea persoană și vă trimite email. Mesajul vă cere imperativ să faceți anumite lucruri, cum ar fi să efectuați un transfer de bani sau să trimiteți date confidențiale despre angajați. Deseori aceste mesaje susțin că este o urgență ce impune să ignorați procedurile standard de securitate, spre exemplu vă pot cere să trimiteți date confidențiale către un cont personal la gmail.com. Ce face acest tip de atacuri țintite să fie periculoase este că infractorii studiază temeinic victimele înainte de a le lansa. În plus, tehnologiile de securitate, cum ar fi programele antivirus sau cele de protecție de tip firewall, nu pot detecta sau bloca acesta atacuri pentru că nu conțin malware sau adrese web susceptibile.

Țineți minte că atacurile de inginerie socială ca acestea nu sunt limitate la apeluri telefonice sau mesaje email, ele pot surveni sub orice formă, inclusiv mesajele text pe telefon (SMS), pe platformele de socializare online sau chiar în persoană. Cheia stă în a ști la ce să vă așteptați, deoarece voi înșivă sunteți cea mai bună defensivă.

Detectarea și stoparea atacurilor de inginerie socială

Din fericire stoparea unor astfel de atacuri este mai simplă decât v-ați aștepta, simțul realității este cea mai bună defensivă. Dacă ceva arată suspect sau nu pare a fi tocmai în regulă, ar putea fi un atac. Cele mai frecvente indicii care arată un atac de inginerie socială includ:

- Cineva care creează sentimentul unei mari urgențe, acesta încearcă să vă determine să faceți o greșeală.
- Cineva cere informații pe care nu ar trebui să le acceseze sau pe care ar trebui să le cunoască deja, cum ar fi numerele dumneavoastră de cont.
- Cineva care vă solicită dezvăluirea unei parole personale; nicio organizație legitimă nu va face așa ceva.
- Cineva care vă presează să evitați sau să ignorați procesele și procedurile de securitate pe care sunteți obligat să le urmați la serviciu.

Ingineria socială

- Ceva ce pare prea bun ca să fie adevărat. De exemplu, sunteți anunțați că ați câștigat la jocurile de noroc, sau un iPad, deși nu ați participat niciodată la loterie.
- Primiți un mesaj bizar de la un coleg de muncă ce conține expresii ce nu sunt caracteristice acelei persoane. Un răufăcător e posibil să fi accesat fraudulos contul acestuia și încearcă să vă păcălească. Pentru a vă proteja verificați astfel de solicitări luând legătura cu colegul de serviciu prin intermediul altui mijloc de comunicare, cum ar fi direct, personal, sau telefonic.

Dacă suspectați că cineva intenționează să vă păcălească, nu mai comunicați cu acea persoană. Dacă atacul are legătură cu serviciul, asigurați-vă că ați anunțat imediat departamentul Help Desk sau echipa de securitate a informației. Rețineți, simțul realității este deseori cea mai bună defensivă.

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

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Despre Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Escrocheria CEO:	https://securingthehuman.sans.org/ouch/2016#july2016
Despre ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Arhiva buletinelor OUCH:	https://securingthehuman.sans.org/ouch/archives

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