OUCH! | 2017.gada janvāris

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

- **Ko nozīmē sociālā inženierija**
- **Sociālās inženierijas uzbrukumu pamanīšana/apturēšana**

Sociālā inženierija

Pārskats

Bieži cilvēki maldīgi domā, ka kibernoziedznieki izmanto tikai izsmalcinātas metodes un rīkus, lai uzlauztu cilvēku datorus vai kontus. Taču tā tas nav. Kibernoziedznieki ir sapratuši, ka bieži visvienkāršākais veids, kā nozagt informāciju, uzlauzt kontus vai inficēt sistēmas, ir Jūs apmānīt un piespiest kļūdīties. Šajā izdevumā pastāstīsim, kā šādi uzbrukumi, ko sauc par sociālo inženieriju, strādā un ko jūs varat darīt, lai aizsargātos.

Viesredaktors

James Lyne (**@jameslyne**) ir sertificēts pasniedzējs SANS institūtā un globālās drošības izpētes vadītājs drošības uzņēmumā Sophos. Viņš analizē un reversē kibernoziedznieku jaunākos darinājumus. Viņš ir arī autors Metasploit (SEC580) un Sociālās inženierijas (SEC567) kursiem SANS.

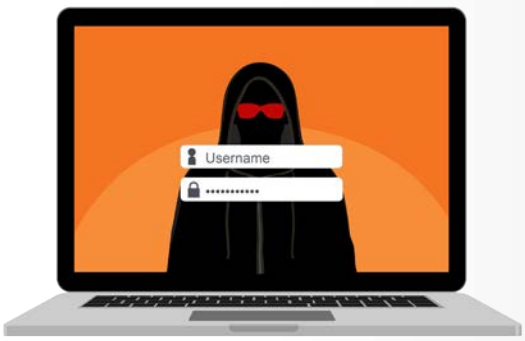
Kas ir sociālā inženierija

Sociālā inženierija ir psiholoģisks uzbrukums, kura laikā uzbrucējs mēģina jūs piemānīt, lai jūs izdarītu kaut ko, ko jums nevajadzētu darīt. Ideja nav jauna, tā ir eksistējusi jau tūkstošiem gadu. Krāpniecība, mānīšanās - tas ir tas pats. Mūsdienu tehnoloģijas kibernoziedzniekiem dod iespēju paslēpties - jūs viņus nevarat redzēt, tādēļ tie var izlikties par ko vien vēlas un mēģināt apmānīt miljoniem cilvēku visā pasaulē, ieskaitot jūs. Sociālās inženierijas uzbrukumi var apiet arī daudzas drošības tehnoloģijas. Vienkāršākais veids, kā saprast šādus uzbrukumus, ir apskatīt divus reālus piemērus.

Jūs saņemat telefona zvanu no kāda, kas uzdodas par datoru atbalsta kompāniju, jūsu Interneta pakalpojumu sniedzēju vai, iespējams, Microsoft tehniskā atbalsta darbinieku. Zvanītājs izstāsta, ka jūsu dators aktīvi skenē Internetu un viņi uzskata, ka tas ir inficēts, un viņam ir uzdots jums palīdzēt “izārstēt” jūsu datoru. Tad viņš izmanto dažādus tehniskus terminus un apraksta virkni darbību, lai pārliecinātu jūs, ka dators tiešām ir inficēts. Piemēram, viņš var prasīt jums pārbaudīt, vai jūsu datorā ir attiecīgi faili, un palīdzēt jums tos atrast. Kad jūs atrodat šos failus, zvanītājs jūs pārliecina, ka šie faili nozīmē, ka jūsu dators ir inficēts, kaut gan patiesībā tie ir parasti sistēmas faili, ko var atrast gandrīz katrā datorā. Tiklīdz viņi ir pārliecinājuši jūs par infekciju, jums tiek uzspiests vai nu nopirkt drošības risinājumu vai atļaut viņiem attālinātu piekļuvi jūsu datoram problēmas novēršanai. Taču programmatūra, kuru viņi jums pārdod, patiesībā ir ļaunatūra. Ja jūs to nopērkat un instalējat, krāpnieki ne tikai ir jūs pierunājuši inficēt datoru, bet jūs par to esat arī

Sociālā inženierija

samaksājis. Ja jūs piešķirat attālinātu piekļuvi, viņi pārņem datoru savā kontrolē un nozog datus vai izmanto jūsu datoru citiem saviem mērķiem.



Veselais saprāts ir labākā aizsardzība pret sociālās inženierijas uzbrukumiem.

Otrs piemērs ir e-pasta uzbrukums, kas tiek saukts par "CEO krāpšanu" (CEO Fraud), šāda veida uzbrukums visbiežāk notiek darba vietā. Kibernoziedznieks izpēta par jūsu organizāciju pieejamo informāciju tiešsaistē un identificē jūsu priekšnieka vai kolēģa vārdu. Tad uzbrucējs izveido e-pastu, izliekoties, ka tas ir no kolēģa vai priekšnieka, un nosūta to jums. E-pastā parasti tiek prasīta steidzīga rīcība, piemēram, pārskaitīt līdzekļus vai nosūtīt konfidenciālu vai sensitīvu informāciju. Pietiekami bieži šie e-pasti izveidoti tā, lai mudinātu jūs apiet ikdienas drošības procedūras, piemēram, tie var prasīt nosūtīt sensitīvu informāciju uz personīgo (piemēram, @gmail.com) kontu. Tas, kas padara šādus mērķētus uzbrukumus īpaši bīstamus, ir tas, ka kibernoziedznieki veic iepriekšēju izpētī. Papildu drošības tehnoloģijas, piemēram, antivīruss vai uguns siena, nespēj šādus uzbrukumus atpazīt, jo tur nav ļaunatūra vai ļaundabīgas saites.

Atcerieties, ka sociālās inženierijas uzbrukumi nav tikai e-pasti vai telefona zvani. Tie var notikt jebkādā veidā, ieskaitot īsziņas, sociālos tīklus vai pat personīgi. Galvenais ir zināt, kā atpazīt šādus uzbrukumus, tad jūs varēsiet sekmīgi aizsargāties.

Sociālās inženierijas uzbrukumu pamanīšana/apturēšana

Par laimi šādu uzbrukumu apturēšana ir vienkāršāka nekā varētu likties - labākā aizsardzība ir veselais saprāts. Ja kaut kas liekas aizdomīgs vai nepareizs, tas var būt uzbrukums. Parasti uz sociālās inženierijas uzbrukumu norāda šādas pazīmes:

- Kāds rada steidzamības sajūtu un mēģina jūs pierunāt veikt kļūdainu darbību;
- Kāds prasa informāciju, kuru tas nedrīkst zināt, vai kuru tam jau vajadzētu zināt tāpat;
- Kāds prasa jūsu paroles, neviena saprātīga organizācija nekad tā nedarītu;

Sociālā inženierija

- Kāds jūs mēģina piespiest ignorēt drošības procedūras vai procesus, ko jums ikdienā jāievēro;
- Kaut kas izklausās pārāk labi, lai būtu taisnība. Piemēram, jums paziņo par loterijas laimestu vai iPad laimēšanu, lai gan jūs neesat piedalījies loterijā vai konkursā;
- Jūs saņemat dīvainu e-pastu no kolēģa vai drauga, kas neizskatās pēc viņu rakstīta. Kibernoziedznieks, iespējams, ir uzlauzis attiecīgās personas kontu un mēģina jūs apmānīt. Lai aizsargātu sevi, pārbaudiet šī e-pasta patiesumu, sazinoties ar attiecīgo personu izmantojot citu sakaru kanālu, piemēram, piezvanot.

Ja Jums ir aizdomas, ka kāds mēģina jūs apmānīt, neturpiniet komunikāciju ar šo personu. Ja uzbrukums ir saistīts ar darbu, nekavējoties ziņojiet palīdzības dienestam vai drošības komandai. Atcerieties - veselais saprāts ir jūsu labākā aizsardzība.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni securingthehuman.sans.org/ouch/archives.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Pikšķerēšana:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO krāpšana:	https://securingthehuman.sans.org/ouch/2016#july2016
Izspiedējvīrusi:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH arhīvs:	https://securingthehuman.sans.org/ouch/archives

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Tulkojums: Edgars Tauriņš