Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

“CEO Fraud”

Kas ir “CEO Fraud”?

Kibernoziedznieki ir viltīgi - tie pastāvīgi nāk klajā ar jauniem veidiem, kā iegūt to, ko vēlas. Viena no visefektīvākajām metodēm ir izmantot tādus cilvēkus kā Jūs. Kiberuzbrucēji labi apzinās, ka nezinoši cilvēki ir vājākais posms jebkurā organizācijā, taču viņi ir aizmirsuši, ka zinoši cilvēki, piemēram, OUCH! lasītāji, var būt organizācijas labākā aizsardzība.

Viesredaktors

Angela Pappas ir Thomson Reuters informācijas drošības apmācības un informēšanas direktore. Angela ir atbildīga par e-mācībām un darbinieku apmācībām par pikšķerēšanu.

Kibernoziedznieki ir izstrādājuši jaunu uzbrukumu “CEO Fraud”, kas ir krāpšanas veids, kas pazīstams arī kā biznesa e-pasta kompromitēšana (BEC). Šādā uzbrukumā kibernoziedznieks izliekas par kādu no Jūsu organizācijas vadības. Noziedznieki sūta e-pastu darbiniekiem, lai mēģinātu Jūs piespiest darīt kaut ko, ko Jums nevajadzētu darīt. Šāda tipa uzbrukumi ir ļoti efektīvi, jo kibernoziedznieki parasti ir ”izpildījuši mājasdarbu”. Viņi izpēta Jūsu organizācijas mājas lapu, lai iegūtu informāciju par tās atrašanās vietu, tās vadītājiem un citām organizācijām, ar ko Jūs sadarbojaties. Nākamajā solī kibernoziedznieki izpēta visu iespējamo par jūsu kolēģiem sociālajos tīklos, piemēram, LinkedIn, Facebook vai Twitter. Saprotot organizācijas struktūru, viņi sāk pētīt un pievērsties konkrētiem darbiniekiem. Viņi izvēlas savus mērķus, pamatojoties uz savām vajadzībām. Ja kibernoziedznieki meklē naudu, viņi var vērsties pie darbiniekiem grāmatvedības departamentā. Ja viņi meklē nodokļu informāciju - pie personāla departamenta. Ja viņi vēlas piekļūt datu bāzes serveriem, viņi var mērķēt uz kādu no IT.

Sapratuši, ko viņi vēlas un kurš būs mērķis, viņi sāk veidot savu uzbrukumu. Visbiežāk viņi izmanto personalizētu pikšķerēšanu. Pikšķerēšana ir, kad uzbrucējs sūta e-pastu miljoniem cilvēku ar mērķi tos apmānīt, lai viņi kaut ko izdarītu, piemēram, atvērtu inficētu pielikumu vai apmeklētu ļaundabīgu mājas lapu. Personalizēta pikšķerēšana (Spear phishing) ir līdzīga, taču tā vietā, lai nosūtītu vispārēju e-pastu miljoniem cilvēku, viņi nosūta īpaši izveidotu e-pastu ļoti mazam speciāli

"CEO Fraud"

izvēlētu cilvēku skaitam. Šādas e-pasta vēstules izskatās ļoti patiesas un tās ir grūti atklāt. Bieži vien tās šķietami nāk no paziņas vai kolēģa, vai pat Jūsu vadītāja. E-pasti šķiet ticami, jo tie var izmantot profesionālo žargonu; viņi var izmantot organizācijas logo vai pat oficiālo parakstu. Vēstules bieži rada steidzamības iespaidu, pieprasot, lai jūs nekavējoties rīkotos un nevienam neko neteiktu. Kibernoziedznieku mērķis ir piespiest Jūs steigā kļūdīties. Populāri ir trīs scenāriji:

"CEO Fraud" ir spēcīgs uzbrukums, kas var apiet vairumu no mūsu drošības pasākumiem. Galu galā Jūs esat mūsu labākā aizsardzība.

- **Pārskaitījums**: Noziedznieki vēlas izkrāpt naudu. Tas nozīmē, tie izpēta, kas strādā grāmatvedības departamentā un pārvalda organizācijas finanses. Tad tiek izveidots un nosūtīts e-pasts it kā no vadītāja. Tas dod rīkojumu steidzami pārskaitīt naudu uz noteiktu kontu.

- **Nodokļu krāpniecība/Personas datu izkrāpšana**: Noziedznieki vēlas personas datus par Jūsu kolēģiem, lai veiktu, piemēram, krāpšanos ar nodokļiem. Tie izpēta organizāciju, saprot, kur glabājas personas dati, piemēram, personāla nodaļā. Tad tiek sagatavots viltus e-pasts it kā no vadītāja vai Juridiskā departamenta, prasot nekavējoties sniegt noteiktu informāciju vai dokumentus.

- **Izlikšanās par juristu/advokātu**: Ne visi krāpniecības mēģinājumi notiek, izmantojot e-pastu. Var tikt izmantotas citas metodes, piemēram, telefona zvans. Šādā gadījumā noziedznieki sāk ar e-pastu, izliekoties par vadības pārstāvi, informējot, ka Jums zvanīs advokāts steidzamā jautājumā. Tad Jums piezvana noziedznieks, kas izliekas par advokātu. Tiek radīta steidzamības sajūta, runājot par konfidenciāliem steidzamiem jautājumiem. Tādā veidā Jūs tiekat apmānīts un piespiests rīkoties nekavējoties un nedomājot.

Kā sevi pasargāt

Ko Jūs varat darīt sevis un savas organizācijas pasargāšanai? Labākā aizsardzība ir veselais saprāts. Ja Jūs saņemat ziņu no Jūsu priekšnieka vai kolēģa un tajā ir kaut kas aizdomīgs, tas varētu būt uzbrukuma mēģinājums. Uz to varētu norādīt,

“CEO Fraud”

piemēram, steidzamības sajūta, aizdomīgs paraksts, neatbilstošs vēstules tonis, neparasta uzruna. Vēl par uzbrukumu var liecināt tas, ka tiek izmantota e-pasta adrese vai telefons, ko Jūs iepriekš neesat redzējis, vai adrese ir ļoti līdzīga, bet ne gluži tāda, kā parasti. Šaubu gadījumā piezvaniet attiecīgajai persona pa uzticamu tālruni vai pajautājiet klātienē par to, vai šāds e-pasts ir tiešām nosūtīts (atbildei neizmantojat e-pastu). Nekad neapejiet drošības politiku vai procedūras. Jūsu organizācijai var būt īpaši dokumenti, kas nosaka procedūras maksājumu veikšanai vai konfidenciālas informācijas sniegšanai. Pieprasījums apiet šo dokumentu prasības neatkarīgi no to šķietamā avota jāuzskata par aizdomīgu un jāpārbauda pirms darbību veikšanas. Ja Jūs saņemat šādu pieprasījumu un neesat pārliecināti, ko darīt, nekavējoties sazinieties ar Jūsu vadītāju, palīdzības dienestu vai informācijas drošības komandu.

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

Sociālā inženierija:	https://securingthehuman.sans.org/ouch/2014#november2014
Pikšķerēšana:	https://securingthehuman.sans.org//ouch/2015#december2015
Kas ir ļaunatūra:	https://securingthehuman.sans.org/ouch/2016#march2016
Divpakāpju verifikācija:	https://securingthehuman.sans.org/ouch/2015#september2015
Dienas padoms:	https://www.sans.org/tip-of-the-day

License

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