OUCH! 2020. gada

SANS SECURITY AWARENESS

Sociālās inženierijas uzbrukumi

Pārskats

Plaši izplatīts kļūdains priekšstats par kiberuzbrukumiem, ka tajos tiek izmantoti tikai sarežģīti rīki un metodes, lai piekļūtu svešiem datoriem un kontiem. Taču kiberuzbrucēji ir atklājuši, ka vienkāršākais veids, kā nozagt informāciju, piekļūt kontam, vai inficēt sistēmu, ir panākt, ka jūs to izdarāt viņu vietā. Šim nolūkam tiek izmantots paņēmiens, ko sauc par sociālo inženieriju. Palūkosimies, kā šie uzbrukumi strādā un kā jūs varat sevi pasargāt.

Kas ir sociālā inženierija?

Sociālā inženierija ir psiholoģisks uzbrukums, kurā uzbrucējs ar viltu un manipulāciju panāk, ka izdarāt kaut ko, ko jums nevajadzētu darīt. Iedomājieties krāpniekus vai viltvāržus; tas ir tieši tāpat. Taču mūsdienu tehnoloģijas jebkuram uzbrucējam no jebkuras pasaules vietas sniedz iespēju izlikties, par ko vien viņš vēlas, un uzbrukt jebkuram brīvi izvēlētam upurim, ieskaitot jūs. Aplūkosim divus reālus piemērus:

Jūs saņemat telefona zvanu no kāda, kas apgalvo, ka pārstāv ieņēmumu dienestu un ka jums ir izveidojies nodokļu parāds, kura nomaksa ir jāveic nekavējoties, citādi jums draud sods vai pat arests. Tad zvanītājs cenšās jūs pierunāt veikt maksājumu telefoniski, izmantojot jūsu maksājumu karti vai pārskaitījumu, draudot ar apcietinājumu, ja maksājums netiks veikts. Zvanītājs patiesībā nemaz nav no ieņēmumu dienesta, bet gan ir uzbrucējs, kurš cenšās jūs piemānīt, lai izkrāptu no jums maksājumu.

Otrs piemērs ir e-pasta uzbrukums jeb pikšķerēšana. Šajā gadījumā uzbrucējs izmanto e-pasta vēstuli, ar kuras palīdzību cenšās panākt jūsu darbību, piemēram, lai jūs atvērtu inficētu e-pasta pielikumu, uzklikšķinātu uz kaitīgas saites vai atklātu sensitīvu informāciju. Dažreiz pikšķerēšanas e-pasti ir ļoti vispārīgi un viegli atpazīstami, piemēram, e-pasts, kuru saņemat it kā no bankas. Bet ir reizes, kad pikšķerēšanas e-pasti tiek īpaši pielāgoti, un uzbrucējs pirms tam savu upuri rūpīgi izpēta, piemēram, tas var būt e-pasts, kuru saņemat it kā no sava vadītāja.

Atcerieties, ka sociālās inženierijas uzbrukumi neaprobežojas tikai ar telefona zvaniem vai e-pastiem; tie var tikt veikti jebkādā formā, ieskaitot SMS, sociālos tīklus, vai pat uzrunājot jūs klātienē. Galvenais ir zināt, kam jāpievērš uzmanība.

Izplatītākās sociālās inženierijas pazīmes

Par laimi veselais saprāts ir jūsu labākā aizsardzība. Ja kaut kas liekas aizdomīgs vai nešķiet līdz galam pareizi, tas var būt uzbrukums. Izplatītākās pazīmes:

- Izteikta steidzamības vai krīzes sajūta. Uzbrucēji cenšas panākt, ka steigā pieļausiet kļūdu. Jo lielāka steidzamības sajūta, jo lielāka iespēja, ka tas ir uzbrukums.
- Spiediens apiet vai neievērot drošības noteikumus vai procedūras, kuras jums būtu jāievēro jūsu darbā.
- Pieprasījums atklāt sensitīvu informāciju, kuru viņiem nebūtu jāzina, vai kuru viņiem jau vajadzētu zināt, kā piemēram, jūsu konta numuru.
- E-pasts vai ziņojums no drauga vai kolēģa, kuru jūs pazīstat, bet ziņojums nemaz nelīdzinās tiem, ko šis cilvēks parasti sūta, iespējams izmantotie vārdi vai teikumu salikums ir dīvains, vai paraksts ir netipisks.
- E-pasts, kuru saņemat it kā no kolēģa vai kāda reāla uzņēmuma, taču tas tiek sūtīts no personīgās e-pasta adreses, piemēram, @gmail.com.
- Centieni izmantot jūsu ziņkāri, vai arī kaut kas pārāk labs, lai būtu patiess. Piemēram, jūs saņemat paziņojumu, ka jūsu sūtījums ir aizkavējies, pat ja neko neesat pasūtījuši, vai ka jūs esat vinnējuši loterijā, kurā neesat piedalījušies.

Ja jums rodas aizdoma, ka kāds cenšas jūs piemānīt, nekomunicējiet ar viņu. Atcerieties, veselais saprāts ir jūsu labākā aizsardzība.

Viesredaktors

Christian Nicholson (@GuardianCosmos) ir SANS kursu SANS SEC560 un SANS SEC504 instruktors, kā arī ir "Indelible" partneris/vadošais kiberdrošības eksperts (https://indelible.global). Christian specializējas lietotņu drošībā, drošības pārbaudēs un pilnveidošanā (Purple Teamig), kā arī drošas integrācijas, programmēšanas un inženierijas automatizācijā.

Resursi

Krāpnieciski telefona zvani: https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams
Kā atpazīt pikšķerēšanu: https://www.sans.org/security-awareness-training/resources/stop-phish
Iejaukšanās biznesa sarakstē: https://www.sans.org/security-awareness-training/resources/ceo-fraudbec
Personalizēta krāpšana: https://www.sans.org/security-awareness-training/resources/personalized-scams

Tulkojums: CERT.LV