ITIESĪBAS

Foto: dreamstime.com

http://itiesibas.lv/raksti/komercdarbiba/datu-aizsardziba/izplatitakie-kibernoziegumi-latvija/12470

Izplatītākie kibernoziegumi Latvijā

AUTORS
Viktorija Jarkina
ZAB "Sorainen"
zvērināta advokāte, Dr.iur.

Katru gadu Latvijā reģistrē vairākus kibernoziegumus - internetā tiek izplatīta aizliegta rakstura informācija, konstatējami uzbrukumi datu bāzēm, nesankcionēti pieslēgumi datorsistēmām utt. Praksē tiek uzskatīts, ka viens no izplatītākajiem kibernoziegumiem jeb datorkrāpšanas formām ir pikšķerēšana, no kuras cieš visvairāk cilvēku.

Kibernoziegumu statistikas dati pieejami Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV mājas lapā.

Pikšķerēšana

Latvijas tiesību aktos pikšķerēšana nav definēta. Akadēmisko terminu datubāzē pikšķerēšana (*phishing*) skaidrota kā neapdomīgu lietotāju aizvilināšana uz tīmekļa vietnēm, kas atdarina reālu organizāciju vietnes. Aizvilināšanas nolūks ir iegūt klientu paroles, kredītkaršu informāciju, ziņas par sociālo apdrošināšanu vai citus personas datus, kurus zaglis pēc tam varētu ļaunprātīgi izmantot.

Praksē pikšķerēšana ir krāpnieciska darbība tiešsaistē, kas ar e-pasta vai mobilā telefona starpniecību, uzdodoties par "leģitīmu" datu apstrādes institūciju (banku, apdrošināšanas kompāniju, sadarbības partneri u.c.), tiek vērsta pret konkrētu personu, lai tiktu atklāta personiskā informācija, ar kuras palīdzību krāpnieks varētu, piemēram:

- citas personas vārdā pieteikties un saņemt kredītu;
- izlietot svešā bankas kontā esošos līdzkļus un iztērēt kredītkaršu limitus;
- izņemt naudu no svešiem kontiem;
- izmantot debetkartes kopiju, lai izņemtu svešu naudu jebkurā pasaules valstī.

Pikšķerēšanas piemēru ir ļoti daudz. Kibernoziedznieki var izveidot viltus vietni, kas identiska bankas vai kādas interneta maksājumu sistēmas vietnei, aicinot lietotājus apmeklēt šo vietni un ievadīt savus konfidenciālos datus, piemēram, lietotājvārdu, paroli vai PIN kodu.

Parasti lietotājus viltotajā vietnē ievilina ar masveidā sūtītām e-pasta vēstulēm it kā no bankas vai citas reālas finanšu iestādes, šajās vēstulēs ievietojot viltotās vietnes hipersaiti. Ja lietotājs izmanto hipersaiti, viņš nonāk krāpnieku izveidotajā interneta lapā, kur tiek pieprasīts ievadīt viņa konta rekvizītus. Nereti pikšķerēšanas vēstulēm ir tādi paši logotipi un noformējums kā īstās bankas sūtījumiem, un arī adrese hipersaitē ir līdzīga īstās bankas interneta adresei. Turklāt bieži paziņojumā lietotāju uzrunā vārdā – kā to varētu sagaidīt īstā vēstulē no bankas. Vēstulē parasti ir minēts ticams iemesls, kādēļ lietotājam jāievada savi dati "bankas vietnē".

Pikšķerēšanas uzbrukumiem kļūstot aizvien sarežģītākiem, lietotājam ir grūtāk noteikt, vai e-pasta ziņojums vai tīmekļa vietne nav ļaunprātīga. Turklāt katru gadu parādās jaunas shēmas. Mūsdienās viltotie e-pasta ziņojumi un tīmekļa vietnes ir saistītas ar īstu uzņēmumu labi zināmu zīmolu logotipiem, nereti tajās var būt pat norādīti partneru vārdi, e-pasta ziņojumi var būt sūtīti no partnera e-pasta utt. Tādējādi viss var izskatīties pat ļoti ticami un likumīgi. Tādēļ pikšķerēšanas shēmas kibernoziedznieku vidū ir tik izplatītas un sekmīgas.

Daudzas pikšķerēšanas shēmas lūdz atvērt pielikumus, kas var inficēt datoru ar vīrusu vai spiegprogrammatūru. Ja datorā ir lejupielādēta spiegprogrammatūra, tā var reģistrēt taustiņsitienus, ko izmantojat, lai pieteiktos savos tiešsaistes kontos. Protams, labāk nekad neatvērt aizdomīgus

pielikumus. Tomēr, ja vēlaties šos pielikumus aplūkot, pirms atvēršanas saglabājiet pielikumu datorā un skenējiet to ar atjauninātu pretvīrusu programmu. Lai palīdzētu aizsargāt datoru, programma "Outlook" automātiski bloķē noteiktu veidu pielikumu failus, kas var izplatīt vīrusus. Ja programma "Outlook" atrod aizdomīgu ziņojumu, tajā tiek bloķēti visi pielikumi neatkarīgi no failu tipa.

Neviens nevar droši pateikt, ka nekad nekļūs par pikšķerēšanas upuri. Vienlaikus internetā pieejami vairāki piesardzības noteikumi un ieteikumi, kā mazināt riskus. Šāda informācija ir pieejama banku mājas lapās, Valsts policijas mājas lapā, datoru antivīrusu izstrādātāju mājas lapās, Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas mājas lapā un citos avotos.

Viltotās vēstules

Viens no "sāpīgākajiem" kibernoziedzieku uzbrukuma veidiem ir viltotu vēstuļu nosūtīšana klientiem to biznesa partneru vārdā. Nereti, lai būtu lielāka ticamība, noziedznieki var nosūtīt elektronisko vēstuli it kā sadarbības partnera vārdā ar viņa adresi. Pirmajā mirklī aplūkojot, šāda vēstule neatšķirsies no oriģināla. Šādās vēstulēs tiek nosūtīts pieprasījums par naudas summu pārskaitīšanu uz jauniem rekvizītiem, turklāt, ja noziedzniekiem ir pieejama klienta (uzņēmuma) informācija par darījumiem, viņi var sagatavot pārliecinošu, aizdomas neizraisošu maksājuma dokumentu.

Krāpnieki bieži ir informēti un var sekot klienta un partnera biznesa būtībai un attīstībai, jo viņi nereti kontrolē arī abu pušu saraksti. Mūsdienās krāpnieki rūpīgi sagatavojas un iesaistās sarakstē ar abām pusēm, pat operējot ar gaidāmā darījuma detaļām. Jāņem vērā, ka krāpnieki var nosūtīt viltotu vēstuli ar zīmogiem un parakstu no partnera uzņēmuma par rekvizītu maiņu. Atsūtītās veidlapas augšpusē, visticamāk, būs norādīts partnera nosaukums, bet saņēmēja bankas rekvizīti būs mainīti.

Datorvīrusi

Datorvīrusi ir kibernoziedzieku "labākie draugi". Praksē vairāki kibernoziegumi tiek īstenoti, cilvēkiem pašiem aktivizējot inficētus failus, kas saņemti e-pastā. Ar kaitnieciskās programmas palīdzību var pārķert tekstu, kas ievadīts ar datora klaviatūru (piemēram, lietotāja kodu, paroli un autorizācijas kodu) un, lietotājam nemanot, nodot to noziedzniekam. Dažas kaitnieciskās programmas pat spēj piekļūt klienta datora interneta pārlūkprogrammai un, kad klients sāk darbu i nternetbankā, tiek parādīta viltota forma, kurā piedāvāts ievadīt autorizācijas kodus, lai it kā apstiprinātu drošības sertifikātu.

Kibernoziedznieki kļūst gudrāki, maldināšanas veidi un datorkrāpnieciskās shēmas smalkākas, datorvīrusi modificējas un parādās jauni. Tādēļ arī interneta lietotājiem ir jābūt piesardzīgākiem.

Ieteicams nesniegt personas un bankas datus, atbildot uz e-pastiem, neapmeklēt aizdomīgas interneta vietnes, neatbildēt uz aizdomīgiem e-pastiem, neatvērt šādu e-pasta pielikumus, kā arī vienmēr sazināties ar saviem biznesa partneriem, ja pēkšņi saņemti paziņojumi par bankas rekvizītu maiņu un lūgumiem veikt maksājumus uz citiem rekvizītiem.

Viedtālruņi un planšetdatori

Interneta lietošana mūsdienās neaprobežojas ar datoriem. Ņemot vērā cilvēku "apsēstību" ar viedtālruņiem un planšetdatoriem, pēdējo gadu laikā ļoti strauji palielinās mobilo ierīču lietotāju skaits. Tā rezultātā ir pieauguši arī draudi mobilo ierīču lietotājiem. Noziedznieki pastiprināti mēģina "uzlauzt" mobilās ierīces un piekļūt tajās esošajai konfidenciālajai informācijai, tostarp arī personas autentifikācijas līdzekļiem internetbankas sistēmā. Tāpat kā datorus, arī viedtālruņus un planšetdatorus vai inficēt ar vīrusiem, apmeklējot aizdomīgas interneta vietnes, vai arī atverot e-pasta vai kādas mobilās lietotnes, piemēram, "WhatsApp", pielikumu.

Lai aizsargātu mobilās ierīces, ieteicams:

- bloķēt ierīci, kad to nelieto;
- noteikt ierīcei pietiekami drošu paroli;
- lai dati nenokļūtu noziedznieku rokās, var aktivizēt datu iznīcināšanas funkciju pēc vairākiem neveiksmīgiem paroles ievades mēģinājumiem;
- laikā, kad netiek izmantots internets, atslēgt ierīci no tīkla;
- neizmantot aizdomīgas programmas. Vairums kaitīgo programmu, kas inficē mobilos tālruņus, ir trojāņi, kurus ir grūti atšķirt no legālām un derīgām programmām, tādējādi ieteicams lejupielādēt programmas tikai no uzticamiem avotiem, piemēram, "Apple App Store" vai "Google Play";
- uzstādīt ražotāja piedāvātos atjauninājumus, kas ļauj novērst atklātās ievainojamības, rezultātā samazinot iespēju, ka noziedznieki varētu pārņemt kontroli pār mobilo ierīci un piekļūt informācijai tajā.