Workforce Security and Risk Training

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Paziņojums par datu noplūdi? Nekrītiet panikā — pārņemiet kontroli

Viens e-pasts mainīja visu

Džastins tikko bija beidzis ēst vakariņas, kad pamanīja e-pastu no autoservisa, kuru nesen bija apmeklējis, lai salabotu sava automobiļa dzinēju. E-pasta temata lauks:

"Svarīgs drošības paziņojums par jūsu kontu"

Sākumā viņš to gandrīz izdzēsa, uzskatot, ka tā ir kārtējā krāpniecība. Tomēr ziņkārība ņēma virsroku. E-pastā tika paskaidrots, ka uzņēmums ir cietis no datu noplūdes, kā rezultātā publiski pieejama kļuvusi klientu informācija, tostarp vārdi, e-pasta adreses, dzīvesvietas adreses un tālruņu numuri. Labā ziņa bija tā, ka bankas karšu dati nebija apdraudēti. Dzīve ritēja saspringtā tempā, un viņš nolēma, ka tas nav nekas īpaši nopietns.

Pagāja dažas dienas. Pēc tam Džastins sāka saņemt dīvainus e-pastus no autoservisa par daudziem kavētiem rēķiniem, kuri nekavējoties jāsamaksā. E-pastos tika draudēts, ka viņš varētu nonākt cietumā, ja viņš nekavējoties nesamaksās. E-pasti izskatījās ticami, jo tajos ne tikai bija uzņēmuma logotips, bet arī bija norādīts viņa vārds, tālruņa numurs un dzīvesvietas adrese. Panikā Džastins noklikšķināja uz saites un samaksāja rēķinu. Tikai vairākas nedēļas vēlāk, sarunājoties ar draugu, viņš saprata, ka e-pasts un rēķins nebija īsti, – tie bija pikšķerēšanas e-pasti, ko bija izveidojuši kibernoziedznieki, izmantojot informāciju, kuru bija nozaguši no uzlauztā autoservisa. Izmantojot nozagto informāciju par Džastinu, kibernoziedznieki spēja izveidot daudz ticamāku uzbrukumu. Diemžēl Džastina stāsts kļūst arvien izplatītāks.

Kas ir datu noplūde?

Datu noplūde specifisks termins, kas apzīmē situāciju, kad organizācijas rīcībā esošie personas dati ir vai nu nozagti kiberuzbrucēju rīcībā, vai nejauši kļuvuši publiski pieejami nepiederošām personām. Dažos gadījumos šīm organizācijām saskaņā ar likumu ir pienākums informēt visus klientus vai partnerus, kuru dati varētu būt pazaudēti vai nozagti saistībā ar šo datu noplūdi. Rodas jautājums, ko darīt, ja saņemat šādu paziņojumu?

Ko vajadzētu darīt pēc datu noplūdes?

Labā ziņa ir tā, ka datu noplūde automātiski nenozīmē, ka jūs kļūsiet par upuri. Svarīgākais ir tas, kā jūs reaģējat.

1. **Nekavējoties nomainiet paroli**. Ja jums ir tiešsaistes konts skartajā organizācijā, nomainiet savu paroli. Vēl svarīgāk – ja šo pašu paroli izmantojāt arī citos kontos, nomainiet paroli arī tajos.

Katram jūsu kontam vajadzētu būt savai unikālai parolei. Gadījumā, ja viens konts tiek apdraudēts, nozagto paroli nevar izmantot, lai piekļūtu citiem jūsu kontiem. Kibernoziedznieki zina, ka cilvēki bieži vien atkārtoti izmanto vienu un to pašu paroli, tāpēc viņi mēģinās izmantot nozagtās paroles, lai piekļūtu jūsu citiem kontiem. Vienkāršākais veids, kā pārvaldīt visas savas unikālās paroles, ir izmantot paroļu pārvaldnieku, kas var izveidot, saglabāt un automātiski ievadīt drošas paroles jūsu vietā.

2. **Ieslēdziet daudzfaktoru autentifikāciju**. Daudzfaktoru autentifikācija, ko bieži dēvē par MFA, papildus parolei pievieno vēl vienu aizsardzības slāni jūsu kontiem. Pat ja kibernoziedznieks nozog jūsu paroli, MFA var liegt tam piekļuvi kontam.
3. **Uzmanieties no turpmākām krāpnieciskām darbībām**. Pēc datu noplūdes noziedznieki var sūtīt viltus e-pastus, īsziņas vai zvanīt, izliekoties par skarto uzņēmumu, jūsu banku vai uzņēmuma atbalsta dienestu. Izmantojot jūsu nozagto informāciju, viņi var izveidot daudz ticamākus e-pastus un īsziņas. Tas, ka kāds zina personīgu informāciju par jums, piemēram, dzīvesvietu, darba vietu vai automobiļa marku, vēl nenozīmē, ka šī persona ir uzticama. Neklikšķiniet uz saitēm un nezvaniet uz tālruņu numuriem, kas ir norādīti šādās ziņās. Tā vietā dodieties tieši uz organizācijas oficiālo tīmekļvietni vai lietotni, lai pārliecinātos, ka šī informācija ir patiesa.
4. **Uzraugiet savus finanšu kontus**. Uzraugiet savas finanses un kontus, lai pamanītu aizdomīgas darbības, piemēram, negaidītus pirkumus, skaidras naudas izņemšanu, paziņojumiem par paroles atiestatīšanu vai izmaiņām profilā. Daudzas bankas un tiešsaistes pakalpojumu sniedzēji ļauj aktivizēt īsziņu vai e-pasta paziņojumus par jebkuru jaunu darījumu vai izmaiņām kontā. Šie brīdinājumi var palīdzēt ātri pamanīt problēmas.

Dažos gadījumos organizācijas, kas ir piedzīvojušas datu noplūdi, saviem klientiem piedāvā trešo pušu nodrošinātus identitātes zādzības aizsardzības pakalpojumus. Lai gan šie pakalpojumi nepalīdz aizsargāt jūsu datus, tie var palīdzēt uzraudzīt bankas kontus, aizsardzību pret bankas karšu ļaunprātīgu izmantošanu un bieži vien nodrošina apdrošināšanu vai citus aizsardzības pasākumus, ja datu noplūdes rezultātā kļūstat par identitātes zādzības upuri. Pārbaudiet identitātes uzraudzības pakalpojuma sniedzēja autentiskumu, jo, izveidojot kontu, jūs tam sniegsiet savu personisko informāciju.

Diemžēl jūs maz ko varat darīt, lai aizsargātu savus datus, kurus uzkrāj citas organizācijas, jo lielākoties jums nav kontroles pār tiem. Taču, veicot šīs vienkāršās darbības, varat būtiski uzlabot savu drošību, ja tomēr notiktu datu noplūde.

Viesredaktore

Brandi Narvaesa (Brandi Narvaez) ir vecākā kiberdrošības konsultante ar vairāk nekā 25 gadu pieredzi informācijas drošības un infrastruktūras projektu īstenošanā. Viņa specializējas organizāciju lietotāju un resursu aizsardzībā, sensitīvu datu drošībā un kiberdrošības stratēģiju saskaņošanā ar biznesa mērķiem, lai uzlabotu kibernoturību un darbības efektivitāti.

Resursi

Kā kibernoziedznieki izmanto jūsu emocijas: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions
Frāžveida paroļu spēks: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
Nepieļaujiet paroļu radītas galvassāpes: izmantojiet paroļu pārvaldnieku: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
Sevis pasargāšana, ja īsta privātuma sasniegšana nav iespējama: https://www.sans.org/newsletters/ouch/protecting-yourself-when-true-privacy-is-impossible

Tulkoja: CERT.LV
 Redkolēģija: Fils Hofmans (Phil Hoffman), Leslija Ridauta (Leslie Ridout), Prinsesa Janga (Princess Young).
Vairāk informācijas par Ouch! Varat atrast šajā saitē: https://www.sans.org/newsletters/ouch