SANS SECURITY AWARENESS
CERT.LV Information Technologies Security Incident Response Institution

OUCH! | 2017.gada decembris

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Sargājiet savus lietotāja datus

Pārskats

Viesredaktors
Tiffany Schoenike ir kampaņu un iniciatīvu direktore Nacionālajā Kiberdrošības Aliansē (**@staysafeonline**). 2016.gadā viņa strādāja kopā ar Balto namu, valdību un industriju, lai izstrādātu un palaistu STOP. THINK. CONNECT.™ iniciatīvas kampaņu par lietotāja datu drošību "Lock Down Your Login" par divu faktoru autentifikāciju.

Autentifikācijas process, t.i. pierādīšana, ka esi tas, par ko uzdodies, ir jūsu informācijas aizsardzības pamatā gan e-pastā, gan sociālajos tīklos, gan tiešsaistes banku kontos. Jūs varbūt nezināt, bet ir trīs veidi, kā pierādīt, kas jūs esat: kaut kas, ko zināt – piemēram, parole; kaut kas, kas jums ir – piemēram, vadītāja apliecība; un kāda daļa no jums – piemēram, pirkstu nospiedumi. Katrai metodei ir savas priekšrocības un trūkumi. Visizplatītākā metode ir paroles – kaut kas, ko jūs zināt. Diemžēl izmantot tikai paroles kļūst arvien nedrošāk. Šajā izdevumā mēs parādīsim, kā aizsargāt sevi un savus lietotāja datus daudz labāk, kā tikai ar paroli, un šāda metode tiek saukta par divu faktoru autentifikāciju.

Ar parolēm vairs nepietiek

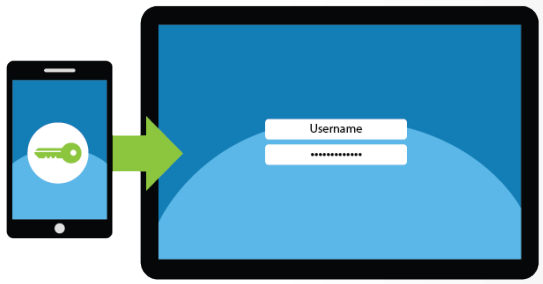
Parole pierāda jūsu identitāti, balstoties uz kaut ko, ko jūs zināt. Taču, ja kāds var uzminēt vai kā citādi iegūt jūsu paroli, tas var izlikties par jums un piekļūt visai jūsu informācijai. Kompromitētas paroles ir viens no galvenajiem uzlauztu kontu iemesliem. Tādēļ jums māca izmantot paroļu frāzes, kuras citiem ir grūti uzminēt, lietot atšķirīgu paroli katram kontam un nekad neizpaust paroles citiem. Lai arī šie ieteikumi paliek spēkā, paroles vairs nav tik efektīvas. Par laimi ir vienkāršs un ātrs veids, kā jūs varat kontrolēt savu personīgo informāciju - tas tiek saukts par divu faktoru autentifikāciju.

Kas ir divu faktoru autentifikācija?

Divu faktoru autentifikācija (tiek saukta arī par divu soļu verifikāciju, vairākfaktoru autentifikāciju, 2FA) ir daudz drošāka par

Sargājiet savus lietotāja datus

tikai paroles lietošanu. Tā prasa identitātes pierādīšanai izmantot nevis vienu, bet divas dažādas metodes. Labs piemērs ir kredītkarte. Izņemot naudu, jūs faktiski lietojat divu faktoru autentifikāciju. Lai piekļūtu naudai, jums vajag divas lietas – jūsu karti (kaut kas, kas jums ir) un jūsu PIN (kaut kas, ko jūs zināt). Ja jūs karti pazaudējat vai jums to nozog, citi nevar piekļūt naudai bez PIN. Citam būtu vajadzīga gan karte, gan PIN, lai noņemtu naudu. Divu faktoru autentifikācija izmanto tieši šādu principu.



Aizsargājiet savus datus, izmantojot divu faktoru autentifikāciju, kad vien iespējams. Tas ir viens no labākajiem aizsardzības pasākumiem tiešsaistē.

Kā tas darbojas

Divu faktoru autentifikācija ir pieejama vairumā banku, e-pastu, sociālo tīklu un citās tīmekļa vietnēs. Papildus vairums pakalpojumu sniedzēju piedāvā vienkāršu instrukciju, kā aktivizēt divu faktoru autentifikāciju (sīkāk resursu sadaļā zemāk). Ieslēgta, tā darbojas sekojoši. Vispirms jūs pierakstāties savā kontā kā ierasts - ar lietotājvārdu un paroli. Tas ir pirmais faktors – kaut kas, ko zināt. Tad jums, piemēram, īsziņā tiek atsūtīts unikāls kods. Šo kodu ierakstāt attiecīgajā logā. Tas ir otrais faktors – jums ir telefons, uz kuru atnāca īsziņa ar kodu. Tagad jūsu konts ir labāk aizsargāts. Pat ja kāds nozog paroli, bez telefona jūsu kontam piekļūt nav iespējams.

Viedtālrunī jūs varat arī uzstādīt speciālu autentifikācijas aplikāciju. Šī mobilā aplikācija ģenerē kodu katru reizi, kad vēlaties pieslēgties. Šādas metodes priekšrocība ir papildu drošība, jo kods netiek sūtīts īsziņā. Papildus tas ir arī ērtāk, jo nav nepieciešams tīkla pārklājums unikālā koda saņemšanai. Aplikācija nepārtraukti ģenerē jaunus kodus, ko varat izmantot, lai pieslēgtos jūsu kontam.

Sargājiet savus lietotāja datus

Sākotnēji divu faktoru autentifikācija var likties sarežģīta un vairāk darbu prasoša, taču jūsu konti, to izmantojot, būs lielākā drošībā. Negaidiet, kamēr kāds uzlauž jūsu kontu, aizsargājiet savus lietotāja datus pieslēdzot divu faktoru autentifikāciju svarīgākajiem kontiem – e-pastam, bankai, sociālajiem tīkliem. Tādejādi jūs varat izbaududīt lielāku drošību par saviem datiem.

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

Paroļu frāzes:	https://securingthehuman.sans.org/ouch/2017#april2017
Pakalpojumi, kas atbalsta divu faktoru autentifikāciju:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Google divu faktoru verifikācija:	http://www.google.com/landing/2step/

License

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

Tulkojums: Edgars Tauriņš