OUCH! 2021 - 09

Viens vienkāršs solis, lai aizsargātu savus kontus

Vai jums šķiet, ka kibernoziedzniekiem ir burvju nūjiņa, lai iekļūtu jūsu e-pastā vai bankas kontos, un jūs neko nevarat darīt, lai viņus apturētu? Vai nebūtu lieliski, ja jūs varētu spert vienu soli, kas palīdzētu aizsargāt jūs no kibernoziedzniekiem un ļautu jums droši izmantot visas tehnoloģijas? Lai arī ar vienu darbību nevar apturēt visus kibernoziedzniekus, viens no vissvarīgākajiem soļiem, ko varat spert, ir iespējot tā dēvēto divfaktoru autentifikāciju (dažreiz to sauc par 2FA, divpakāpju verifikāciju vai daudzfaktoru autentifikāciju) savos vissvarīgākajos kontos.

Problēma ar parolēm

Runājot par savu kontu aizsardzību, jūs, visticamāk, jau izmantojat kādu paroli. Ir vairāki veidi, kā autentificēties kontā: kaut kas, kas jums ir, kaut kas, ko jūs zināt, kaut kas, kas jūs esat, kaut kur, kur jūs esat. Ja izmantojat vairāk nekā vienu autentifikācijas metodi, jūs pievienojat papildu aizsardzību pret kibernoziedzniekiem – pat ja viņi uzlauž vienu metodi, viņiem joprojām ir jāapiet papildu faktors, lai piekļūtu jūsu kontam. Paroles apstiprina, kas jūs esat, pamatojoties uz kaut ko, ko jūs zināt. Paroļu bīstamība slēpjas tajā, ka visa jūsu konta drošība ir atkarīga tikai no šīs vienas lietas. Ja kibernoziedznieks var uzminēt vai citādi iegūt jūsu paroli, viņš var piekļūt jūsu vissvarīgākajiem kontiem. Turklāt kibernoziedznieki izstrādā aizvien ātrākas un labākas metodes paroļu uzminēšanai, iegūšanai vai apiešanai. Par laimi, jūs varat aizstāvēties, izmantojot divfaktoru autentifikāciju.

Divfaktoru autentifikācija

Divfaktoru autentifikācijas pievienošana ir daudz drošāks risinājums nekā paļaušanās tikai uz parolēm. Tā darbojas, pieprasot nevis vienu, bet divas dažādas metodes, lai autentificētos. Šādā veidā, ja jūsu parole ir apdraudēta, jūsu konts joprojām ir aizsargāts. Viens piemērs ir jūsu bankomāta karte; izņemot naudu no bankomāta, jūs faktiski izmantojat divfaktoru autentifikācijas veidu. Lai piekļūtu savai naudai, jums ir nepieciešamas divas lietas: jūsu bankomāta karte (kaut kas, kas jums ir) un jūsu PIN kods (kaut kas, ko jūs zināt). Ja pazaudējat savu bankomāta karti, neviens, kurš atrod jūsu karti, nevar izņemt jūsu naudu, jo nezina jūsu PIN. Tas pats attiecas uz gadījumiem, ja viņiem ir tikai jūsu PIN, bet nav kartes. Uzbrucējam ir jābūt abiem, lai apdraudētu jūsu bankomāta kontu. Koncepcija ir līdzīga divfaktoru autentifikācijai; jums ir divi drošības līmeņi.

Divfaktoru autentifikācijas izmantošana tiešsaistē

Divfaktoru autentifikācija tiek iestatīta katram kontam atsevišķi.
Patiesībā tas ir pavisam vienkārši: parasti jums nav jādara nekas vairāk par mobilā tālruņa sinhronizāciju ar kontu. Tādā veidā, kad jums jāpieslēdzas savam kontam, jūs ne tikai pieslēdzaties ar sava konta lietotājvārdu un paroli, bet arī izmantojat unikālu vienreizēju kodu, ko saņemat no sava tālruņa. Būtība ir tāda, ka tiek apvienota gan jūsu parole, gan unikālais kods, lai pieslēgtos. Parasti šis unikālais kods tiek nosūtīts uz jūsu mobilo ierīci ar īsziņu vai e-pastu. Jūsu tālrunī var būt arī mobilā lietotne (piemēram, Google vai Microsoft autentifikatora lietotne), kas jums ģenerēs unikālo kodu. Kad vien iespējams, mobilās lietotnes tiek uzskatītas par visdrošāko jūsu unikālā koda iegūšanas iespēju.

Tas ir tik vienkārši tāpēc, ka parasti jums tas ir jādara tikai vienreiz no jebkura datora vai ierīces, kuru izmantojat, lai pieslēgtos. Tiklīdz vietne vai jūsu konts atpazīst jūsu ierīci, turpmāk jums parasti nepieciešama tikai parole, lai pieslēgtos. Ikreiz, kad mēģināt (vai kāds cits mēģina) pieslēgties jūsu kontam no cita datora vai ierīces, viņam atkal būs jāizmanto divfaktoru autentifikācija. Tas nozīmē, ka, ja kibernoziedznieks iegūst jūsu paroli, viņš joprojām nevar piekļūt jūsu kontam, jo nevar piekļūt unikālajam kodam.

Atcerieties, ka divfaktoru autentifikācija parasti nav iespējota pēc noklusējuma, tāpēc jums tā jāiespējo katram svarīgākajam kontam, piemēram, bankas, ieguldījumu, pensijas vai personīgajam e-pastam. Lai gan sākotnēji tas var šķist sarežģīti, tiklīdz tā ir izveidota, to ir ļoti viegli lietot.

Viesredaktors

Lisandrai Kapelai (Lysandra Capella) ir vairāk nekā 15 gadu pieredze informācijas drošības un tehnoloģiju jomā. Viņa ir SANS institūta instruktore apmācībā SANS AUD507, koncentrējoties uz riska novērtēšanu un pārvaldīšanu. Kad Lisandra nemāca, viņa atbalsta vadības komandas, formulējot to stratēģijas, nodrošinot drošību un IT pārvaldību.
https://www.linkedin.com/in/lysandracapella/.

Resursi

Kā padarīt paroles vieglāk iegaumējamas: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/

Tulkojums: CERT.LV