OUCH! Septembar 2021

Zaštitite vaše naloge primenom jednog jednostavnog koraka

Pomislite li ponekad da sajber kriminalci imaju čaroban štapić za pristup vašoj elektronskoj pošti ili bankovnim računima i da nema načina da ih u tome zaustavite? Zar ne bi bilo sjajno kada bi postojao jedan korak koji bi mogao da vas zaštiti od sajber kriminalaca i koji bi vam omogućio da na bezbedan način koristite savremene tehnologije? Korak koji bi mogao da zaustavi sve sajber kriminalce ne postoji, ali postoji jedan koji je najvažniji, a podrazumeva da na vašim najvažnijim nalozima omogućite nešto što se zove dvofaktorska autentifikacija (ponekad se naziva 2FA, verifikacija u dva koraka ili multifaktorska autentifikacija).

U čemu je problem sa lozinkama?

Za zaštitu vaših naloga najverovatnije već koristite neku vrstu lozinke. Postoji nekoliko načina da se autentifikujete na nalog: nešto što imate, nešto što znate, nešto što jeste, negde gde ste. Kada koristite više načina autentifikacije, primenjujete dodatni sloj zaštite od sajber kriminalaca - čak i ako razotkriju jedan način, oni će morati da nađu način da zaobiđu i dodatni faktor ili faktore kako bi pristupili vašem nalogu. Korišćenjem lozinki dokazujete ko ste na osnovu nečega što znate. Opasnost kada koristite samo lozinke leži u tome što one predstavljaju slabu tačku. Ako sajber kriminalci mogu da pogode ili kompromituju vašu lozinku, oni lako mogu pristupiti vašim najvažnijim nalozima. Osim toga, sajber kriminalci neprestano razvijaju brže i bolje tehnike pogađanja, kompromitovanja ili zaobilaženja lozinki. Srećom, može vas zaštititi dvofaktorska autentifikacija..

Dvofaktorska autentifikacija

Omogućavanje dvofaktorske autentifikacije je daleko sigurnije rešenje od oslanjanja samo na lozinke. Ona funkcioniše tako što zahteva ne jedan već dva različita načina za autentifikaciju. Tako će, čak i ako je vaša lozinka kompromitovana, vaš nalog i dalje ostati zaštićen. Jedan primer je upotreba platne kartice; kada podižete novac sa bankomata vi zapravo koristite jedan oblik dvofaktorske autentifikacije. Da biste pristupili svom novcu, potrebne su vam dve stvari: vaša platna kartica (nešto što imate) i PIN broj (nešto što znate). Ako izgubite platnu karticu, niko ko je pronađe neće moći da podigne novac jer ne zna vaš PIN. Isto važi i ako neko ima vaš PIN, ali ne i karticu. Kako bi ugrozio vaš račun u banci napadač mora imati i platnu karticu i PIN. Sličan koncept se primenjuje i kod dvofaktorske autentifikacije za vaše naloge - ona vam pruža dva sloja bezbednosti.

Korišćenje dvofaktorske autentifikacije na internetu

Dvostruka autentifikacija omogućava se posebno za svaki od vaših naloga na internetu.
Postupak je veoma jednostavan: obično nije potrebno da uradite ništa više od sinhronizacije vašeg mobilnog telefona sa nalogom. Nakon što je omogućite, kada sledeći put budete želeli da se prijavite na svoj nalog, ne samo da će biti potrebno vaše korisničko ime i lozinka, nego će vam biti potreban i jedinstveni jednokratni kod sa vašeg telefona. Suština je da je za uspešnu autentifikaciju potrebna kombinacija vaše lozinke i jedinstvenog koda. Jedinstveni kod se uobičajeno dostavlja u vidu tekstualne poruke na vaš mobilni uređaj ili adresu elektronske pošte. Takođe, na vašem telefonu možete imati i mobilnu aplikaciju (poput Google ili Microsoft Authenticator aplikacije) koja će generisati jedinstveni kod za vas. Mobilne aplikacije se smatraju najbezbednijim načinom za dobavljanje jedinstvenog koda.

Dvostruku autentifikaciju jednostavnom čini to što je obično dovoljno da se sa svakog računara ili uređaja koji koristite za pristup nalogu samo jednom autentifikujete na ovaj način. Kada veb lokacija ili vaš nalog prepoznaju vaš uređaj, za dalji pristup će vam najčešće biti potrebno da samo unesete lozinku. Svaki put kada pokušate (vi ili neko drugi) da se prijavite na vaš nalog sa nekog drugog računara ili uređaja, biće potrebno da ponovo upotrebite dvofaktorsku autentifikaciju. To znači da, čak i ako saznaju vašu lozinku, sajber kriminalci neće moći da pristupe vašem nalogu jer ne mogu da pristupe jedinstvenom kodu.

Ne zaboravite da dvofaktorska autentifikacija obično nije podrazumevano omogućena (*by default*), već je potrebno da je sami uključite i to za svaki od svojih važnih naloga, kao što su bankovni nalozi ili nalozi za elektronsku poštu. Iako se ovo na prvi pogled može učiniti zahtevnim, zapravo je veoma jednostavno za upotrebu.

Gost urednik

Lisandra Kapela ima više od 15 godina radnog iskustva u oblasti informacione bezbednosti i tehnologija. Ona je instruktorka SANS instituta za obuku SANS AUD507 na kojoj se izučava upravljanje rizikom i njegovo merenje. Kada ne predaje, Lisandra pruža podršku timovima izvršnih menadžera u izradi strategije, osiguravanju bezbednosti i IT upravljanju.
https://www.linkedin.com/in/lysandracapella/.

Dodatni materijal

Napravite lozinku na jednostavan način: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Menadžeri lozinki: https://www.sans.org/newsletters/ouch/password-managers/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović