OUCH! Januar 2023

SANS SECURITY AWARENESS

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Biometrija - bezbednost na jednostavniji način

Uvod

Ne volite lozinke? Da li ste umorni od zahteva za kreiranje naloga na novim sajtovima kojima pristupate i od činjenice da ne možete da zapamtite sve svoje složene lozinke? Frustrira li vas što neprestano morate da generišete nove lozinke za nove naloge ili da menjate stare lozinke za postojeće naloge? Imamo dobre vesti za vas. Postoji rešenje, zove se biometrija, koje pomaže da svoju bezbednost očuvate na jednostavniji način. U nastavku teksta je objašnjeno šta je biometrija, kako nam život čini jednostavnijim i zbog čega ćemo je upotrebljavati sve češće.

Čemu uopšte služe lozinke?

Lozinke su deo nečega što se zove autentifikacija, a predstavlja proces dokazivanja ko ste. Uobičajeno se koriste dva faktora koja možete da pružite kako biste dokazali svoj identitet: nešto što znate (poput vaših lozinki) i nešto što imate (poput vaše platne kartice ili vašeg mobilnog uređaja). Tradicionalno se za autentifikaciju koriste lozinke. One su usvojene prve jer je to rešenje za autentifikaciju bilo najlakše za implementaciju. Međutim, tokom godina su naši životi postali mnogo složeniji i mi danas upotrebljavamo mnogo više korisničkih naloga nego što je iko mogao da pretpostavi. Prilično je uobičajeno da osoba koristi preko 100 lozinki u svom poslovnom i privatnom životu.

Pored toga, sajber napadači su postali prilično vešti u pogađanju, krađi ili razbijanju lozinki. To je razlog zbog koga se u vezi sa lozinkama nameću brojna pravila, kao što je pravilo u vezi sa minimalnom dužinom lozinke (kako bi bile teže za pogađanje) i pravilo o korišćenju jedinstvene lozinke za svaki nalog (tako da ako jedan od vaših naloga bude hakovan, vaši drugi nalozi i dalje ostanu bezbedni). Problem sa svim tim različitim pravilima u vezi sa lozinkom je što ona usložnjavaju održavanje sajber bezbednosti. Menadžeri lozinki značajno pomažu u ovom domenu jer bezbedno pamte sve vaše lozinke i sami vas prijavljuju na veb lokacije, međutim ne možemo a da se ne zapitamo, postoji li možda i bolji način? Ovde nam može pomoći biometrija, koja omogućava korišćenje trećeg faktora kao nečega što vi jeste u cilju dokazivanja identiteta.

Biometrija

Biometrija, baš kao i same lozinke, predstavlja jedan od načina da dokažete svoj identitet. Razlika je u tome što umesto nečega što morate da pamtite (kao što su vaše lozinke), upotrebljavate faktor koji čini vas same, kao što je otisak prsta koji koristite kada pristupate svom telefonu.

Korišćenje biometrije je za korisnike mnogo jednostavnije jer ne moraju ništa da pamte ili kucaju, samo se autentifikuju koristeći nešto što je njihov deo. Postoji mnogo različitih tipova biometrijskih podataka, u njih spadaju i glas, način hoda, izgled dužice (irisa) oka. Ipak, otisak prsta i prepoznavanje lica su tipovi koji se najčešće koriste, posebno u slučaju mobilnih uređaja. Iako biometrija nudi veliki broj prednosti, ona takođe ima i neke nedostatke, a jedan od najznačajnijih je taj što ako vaš otisak prsta ili geometriju lica kopiraju sajber napadači, vi nećete moći da ih promenite (kao što ste mogli da promenite lozinku).

Pristupni ključevi

Tokom narednih meseci i godina, primetićete da biometrija zamenjuje lozinke i to putem nove tehnologije koja se zove pristupni ključevi. Ovu tehnologiju razvijaju Majkrosoft, Epl i Gugl i očekuje se da će sve veći broj veb sajtova uskoro početi da je primenjuje. Pristupni ključevi zamenjuju lozinke tako što vam omogućavaju da dokažete ko ste jednostavnim korišćenjem biometrijskih podataka u kombinaciji sa vašim mobilnim uređajem. Kada kreirate nalog na veb sajtu (kao što je Guglov ili Eplov), umesto da kreirate lozinku, registrujete svoj mobilni uređaj. Potom se prijavljujete na tu veb lokaciju tako što ćete se autentifikovati pomoću svog mobilnog uređaja koristeći biometriju, kao što je otisak prsta ili prepoznavanje lica. Veb lokacija veruje vašem mobilnom uređaju, a vaš mobilni uređaj potvrđuje da ste baš vi osoba koja na njemu koristi biometriju. Primetićete da se u tom postupku vaši biometrijski podaci (otisak prsta ili lice) ne šalju ni na jednu veb lokaciju. Umesto toga, vaša se biometrija bezbedno čuva lokalno, na vašem uređaju. Biometrija se u ovom postupku koristi samo za otključavanje pristupnih ključeva, kreiranih tako da budu jedinstveni za svaki sajt, koje vaš uređaj šalje sajtu dok istovremeno štiti vaše biometrijske podatke. Iako nijedno rešenje nije savršeno, biometrija i rešenja kao što su pristupni ključevi mogu da vam pomognu da ostanete bezbedni na jednostavniji način.

Gost urednik

Dr Johanes Ulrih je dekan Odseka za istraživanje koledža SANS tehnološkog instituta. Sa preko 20 godina iskustva u industriji, trenutno prati aktuelne pretnje upravljajući SANS Internet Storm centrom. Predaje na obukama SEC522 (Web Application Security) i SEC503 (Intrusion Detection).
Twitter: @johullrich & LinkedIn: https://www.linkedin.com/in/johannesullrich/.

Dodatni materijal

Menadžeri lozinki: https://www.sans.org/newsletters/ouch/password-managers/
Više o pristupnim ključevima: https://www.sans.org/blog/what-is-phishing-resistant-mfa/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović