OUCH! 2023 - 01

SANS SECURITY AWARENESS

Biometrija — drošības vienkāršošana

Pārskats

Vai jums nepatīk paroles? Vai esat noguris no nemitīgas pieslēgšanās jaunām vietnēm vai nevarat atcerēties visas savas sarežģītās paroles? Jūs neapmierina nepieciešamība izdomāt jaunas paroles jauniem kontiem vai mainīt vecās paroles esošajiem kontiem? Mums jums ir lieliskas ziņas. Pastāv risinājums, ko sauc par biometriju, kas palīdz uzlabot kiberdrošību. Turpmāk rakstā skaidrosim, kas ir biometrija, kā tā atvieglo dzīvi un kāpēc ar to saskarsieties arvien biežāk.

Pirmkārt, kāpēc izmanto paroles?

Paroles ir daļa no tā sauktā autentifikācijas procesa, kurā tiek pierādīta jūsu identitāte. Lai pierādītu savu identitāti, parasti var izmantot divus elementus: kaut ko, ko jūs zināt (piemēram, paroles), un kaut ko, kas jums ir (piemēram, bankas karte vai mobilā ierīce). Tradicionāli autentifikācija tiek veikta, izmantojot paroles. Paroles sākotnēji tika ieviestas, jo tas bija viens no visvieglāk ieviešamajiem autentifikācijas risinājumiem. Tomēr gadu gaitā mūsu dzīve ir kļuvusi sarežģītāka un ar daudz vairāk kontiem, nekā kāds jebkad gaidījis. Bieži vien cilvēkam darba un personīgajā dzīvē ir vairāk nekā 100 paroļu.

Turklāt kiberuzbrucēji ir diezgan labi iemanījušies uzminēt, nozagt vai uzlauzt paroles. Tāpēc ir tik daudz noteikumu par paroļu lietošanu, piemēram, paroles ir jāveido garas (lai tās būtu grūti uzminēt) un katram kontam jāizmanto unikāla parole (lai gadījumā, ja kāds no jūsu kontiem tiek uzlauzts, pārējie konti joprojām būtu droši). Problēma ar visām paroļu prasībām ir tā, ka tās apgrūtina kiberdrošību. Paroļu pārvaldnieki ievērojami palīdz, jo tie droši atceras visas jūsu paroles un pieslēdzas tīmekļa vietnēm jūsu vietā, bet vai ir labāks risinājums? Te var palīdzēt biometrija, jo tas ir trešais elements, kas apliecina jūsu identitāti.

Biometrija

Tāpat kā paroles, arī biometriskie dati ir vēl viens veids, kā pierādīt, kas esat. Atšķirība ir tāda, ka tā vietā, lai kaut ko atcerētos (piemēram, paroles), jūs izmantojat kādu savu identitāti apliecinošu elementu, piemēram, pirksta nospiedumu, lai piekļūtu savam tālrunim.

Biometriskie dati ir daudz vienkāršāki, jo jums nekas nav jāatceras vai jāievada, jūs vienkārši autentificējaties ar savas identitātes palīdzību. Ir daudz dažādu biometrisko datu veidu, piemēram, jūsu balss, veids, kā staigājat, vai jūsu varavīksnene. Tomēr pirkstu nospiedumi un sejas atpazīšana ir divi visizplatītākie biometrijas elementi, jo īpaši mobilajās ierīcēs. Lai gan biometrijai ir ārkārtīgi daudz priekšrocību, tai ir arī daži trūkumi, un viens no lielākajiem ir tas, ka, ja jūsu pirksta nospiedumu vai seju nokopē kiberuzbrucēji, jūs to nevarat mainīt.

Ieejas atslēgas

Tuvāko mēnešu un gadu laikā biometriskie dati aizstās paroles ar jauno tehnoloģiju Passkeys (ieejas atslēgas). Šo tehnoloģiju izmanto Microsoft, Apple un Google, un gaidāms, ka laika gaitā to izmantos arvien vairāk vietņu. Ieejas atslēgas aizstāj paroles, ļaujot jums pierādīt, kas esat, vienkārši izmantojot biometriskos datus kopā ar mobilo ierīci. Kad vietnē (piemēram, Google vai Apple) izveidojat kontu, tā vietā, lai izveidotu paroli, jūs reģistrējat savu mobilo ierīci. Turpmāk jūs piesakāties šajā vietnē, autentificējoties ar savu mobilo ierīci, izmantojot biometriskos datus, piemēram, pirksta nospiedumu vai sejas atpazīšanu. Tīmekļa vietne uzticas jūsu mobilajai ierīcei, un jūsu mobilā ierīce apstiprina, ka tas esat jūs, izmantojot biometriskos datus. Turklāt jūsu biometriskie dati (pirksta nospiedums vai sejas atpazīšana) netiek nosūtīti nevienai vietnei. Tā vietā jūsu biometriskie dati tiek droši saglabāti lokāli jūsu ierīcē. Tie ir izmantoti tikai, lai atbloķētu katrai vietnei izveidoto unikālo atslēgu Passkey, ko jūsu ierīce nosūta vietnei, vienlaikus aizsargājot jūsu biometriskos datus. Lai gan neviens risinājums nav ideāls, biometrija un tādi risinājumi kā Passkeys var palīdzēt nodrošināt jūsu drošību, vienlaikus vienkāršojot drošības pasākumu īstenošanu.

Viesredaktors

Dr. Johanness Ulrihs (Johannes Ullrich) ir SANS Tehnoloģiju institūta koledžas pētniecības dekāns. Viņam ir vairāk nekā 20 gadu pieredze šajā nozarē, un pašlaik viņš uzrauga aktuālos draudus, vadot SANS Internet Storm Center. Viņš pasniedz SEC522 (tīmekļa lietotņu drošība) un SEC503 (ielaušanās atklāšana).
Twitter: @johullrich un LinkedIn: https://www.linkedin.com/in/johannesullrich/.

Resursi

Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/
Vairāk par ieejas atslēgām: https://www.sans.org/blog/what-is-phishing-proof-mfa/

Tulkojums: CERT.LV