Paroles spēks: kāpēc garāka parole ir labāka par gudrāku

Vienkārša parole, liela problēma

Daniels vienmēr sevi uzskatīja par "diezgan prasmīgu darbā ar datoriem". Viņš iepirkās tiešsaistē, pārvaldīja savas finanses digitāli un uzturēja saziņu ar draugiem sociālajos tīklos. Tāpat kā daudzi citi, viņš savu privāto e-pasta kontu aizsargāja ar paroli, kuru bija izmantojis gadiem ilgi. Tā bija īsa, viegli iegaumējama un iekļāva viņa iecienītās sporta komandas nosaukumu ar simbolu un skaitli. Viņam šķita, ka ar to pilnīgi pietiek.

Kādu rītu Daniels pamodās, ieraugot desmitiem paziņojumu. Paroles atiestatīšanas e-pasti, neveiksmīgu pieslēgšanās mēģinājumu brīdinājumi un ziņas no draugiem, kuri jautāja, kāpēc viņš viņiem sūta aizdomīgas saites. Viņa e-pasta konts naktī bija uzlauzts. Ielaužoties kontā, uzbrucējs nomainīja paroles viņa sociālo tīklu, iepirkšanās un mākoņuzglabāšanas kontiem. Dažu stundu laikā viņa kontaktpersonām tika nosūtītas viltus ziņas, viņa vārdā tika veikti pirkumi un lejupielādēti privāti fotoattēli.

Iemesls nebija sarežģīta hakeru uzbrukuma vai modernu ļaunatūru izmantošana. Visticamāk, iemesls bija vāja, atkārtoti izmantota parole, kas vai nu bija atklāta datu noplūdes laikā citā tīmekļvietnē, vai vienkārši uzminēta ar uzbrucēja automatizētajiem rīkiem. Tikai viena vāja parole deva kibernoziedzniekam piekļuvi visai Daniela digitālajai dzīvei.

Kāpēc paroles mūs pieviļ

Paroles joprojām ir visizplatītākais veids, kā mēs aizsargājam savus tiešsaistes kontus, taču tās ir arī viens no vājākajiem posmiem drošības sistēmā. Kibernoziedznieki parasti neuzmin paroles, izmēģinot vienu pēc otras, kā tas redzams filmās. Viņi izmanto automatizētus rīkus, kas ļoti ātri spēj pārbaudīt miljoniem vai pat miljardiem paroļu kombināciju. Viņi lielā mērā paļaujas arī uz zagtām paroļu datubāzēm no iepriekšējiem datu noplūdes gadījumiem. Ja atkārtoti izmantojat paroles vai izvēlaties īsas un paredzamas paroles, jūs būtiski atvieglojat darbu uzbrucējiem.

Spēcīgas paroles ir viens no galvenajiem veidiem, kā aizsargāt savus kontus un savu digitālo dzīvi internetā. Tomēr sarežģītu paroļu problēma ir tā, ka tās ir grūti atcerēties un ievadīt. Vēl labāks veids, kā izveidot spēcīgu un drošu paroli, ir tā sauktā "frāzveida parole". Frāzveida parole būtībā ir parole, kuru veido vairāki vārdiem, dažkārt apvienoti īsā frāzē. To stiprums slēpjas nevis sarežģītībā, bet garumā. Piemēram:

Laiks iedzert stipru kafiju!
pazudis-gliemežvāks-pludmalē

Garākas frāzveida paroles automatizētiem rīkiem ir ievērojami grūtāk uzlauzt, taču tās joprojām ir viegli atcerēties un ievadīt. Dažkārt frāzveida parole var būt jāpapildina ar sarežģītākiem elementiem, piemēram, simboliem, lielajiem burtiem vai cipariem.

Izmantojiet unikālas frāzveida paroles

Ar garumu vien nepietiek. Jūsu frāzveida parolei jābūt unikālai katram kontam. Ja izmantojat vienu un to pašu paroli vai frāzveida paroli vairākās vietnēs, viena konta uzlaušana var apdraudēt visus pārējos kontus. Uzbrucēji regulāri pārbauda nozagtos piekļuves datus e-pasta, banku un sociālo tīklu platformās – šo procesu sauc par nozagtu piekļuves datu masveida izmēģināšanu "credential stuffing".

Droša frāzveida paroļu glabāšana

Nespējat atcerēties visas šīs garās, unikālās frāzveida paroles katram kontam? Risinājums ir paroļu pārvaldnieki. Tās ir īpašas datorprogrammas, kas droši glabā visas jūsu paroles šifrētā seifā, kuru aizsargā galvenā parole. Lai tai piekļūtu, jāatceras tikai galvenā parole. Paroles pārvaldnieks var automātiski atrast jūsu paroles, kad vien tās ir nepieciešamas, un pieslēgties vietnēm jūsu vietā. Paroļu pārvaldnieki ir attīstījušies, iekļaujot arī citas funkcijas, tostarp atbilžu uz slepeniem jautājumiem glabāšanu, brīdināšanu, ja atkārtoti izmantojat paroles vai nokļūstat viltus tīmekļvietnē, ģeneratoru izmantošanu, kas jūsu vietā izveido spēcīgas vai frāzveida paroles, un daudzas citas funkcijas. Lielākā daļa paroļu pārvaldnieku nodrošina drošu sinhronizāciju gandrīz jebkurā datorā vai ierīcē, tāpēc neatkarīgi no tā, kādu sistēmu izmantojat, jums ir ērta un droša piekļuve visām savām parolēm.

Soli tālāk

Pat visstiprākā frāzveida parole nav nevainojama. Tāpēc, kad vien iespējams, jāiespējo daudzfaktoru autentifikācija (MFA). MFA pievieno papildu aizsardzības līmeni, pieprasot kaut ko, kas jums ir (piemēram, vienreizējs kods citā ierīcē), vai kaut ko, kas esat (piemēram, biometriska pārbaude). Tas nozīmē, ka pat tad, ja frāzveida parole tiek nozagta, uzbrucēji joprojām tiek bloķēti.

Vienkārši ieradumi, spēcīga aizsardzība

Daniela stāsts varēja beigties pavisam citādi, ja viņš būtu izmantojis garu, unikālu frāzveida paroli un, iespējams, arī ieslēdzis MFA. Vājas vai atkārtoti izmantotas paroles joprojām ir ļoti izplatītas un ļauj kibernoziedzniekiem apdraudēt jūs neatkarīgi no tā, cik piesardzīgs vai pieredzējis esat.

Viesredaktore

Taruns Prītems Bula (Tarun Preetham Bulla) ir kiberdrošības pasniedzējs un praktiķis ar pieredzi reaģēšanā uz incidentiem, digitālajā ekspertīzē un draudu noteikšanā. Taruns pasniedz bakalaura līmeņa kiberdrošības kursus, vada kiberdrošības laboratorijas, uzrauga noslēguma projektus un koncentrējas uz studentu sagatavošanu darba tirgum, integrējot reālās nozares pieredzi izglītībā.

Resursi

Paroļu pārvaldnieku spēks: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
Kā kibernoziedznieki nozog jūsu paroles: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Piekļuves (passkeys) atslēgas: https://www.sans.org/newsletters/ouch/passkeys-simpler-safer-way-sign-in

Tulkoja: **CERT.LV**

Vairāk informācijas par Ouch! Varat atrast šajā saitē: https://www.sans.org/newsletters/ouch