Parool on jätkuvalt üks suuremaid turvariske

6 aastat tagasi - 01.09.2020 Autor: Joosep Truu

123456, parool, iloveyou, printsess, draakon jne. 2019. aasta halvimate paroolide nimekiri tuletab meelde, et paljud interneti kasutajad endiselt alahindavad küberturvalisuse ohte. Edukad küberrünnakud saavad teoks enamasti tänu varastatud või nõrkadele paroolidele. Enim levinud oht on ühe parooli laialdane ja korduv kasutamine erinevate teenuste jaoks, selgitab IT haldusteenuseid pakkuva ettevõtte Iteraction OÜ juht Joosep Truu, miks on parool suur turvarisk ja annab nõu, kuidas seda vähendada.

Numbrite, tähtede ja erimärkide kombinatsioonide leiutamine ja meelde jätmine on paras peavalu. Keskmisel kasutajal on 100 kontot, mis vajavad paroole. Lihtne lahendus on kasutada sama parooli kõikjal, kuid ainult üks leke ühes kohas tähendab, et paljud kontod satuvad ohtu. Õnneks liiguvad autentimise tehnoloogiad selles suunas, et varsti ehk ei ole paroole enam vajagi.

Mis on mitmefaktoriline autentimine?

Mitmefaktoriline autentimine tähendab, et kasutaja peab oma identiteeti tõestama kahe või enama meetodi abil ühendades midagi, mida teab vaid tema (parool), midagi, mis tal on (PIN kalkulaator või telefonist kinnitatav sisse logimine või turvavõti) või midagi, mis ta on (biomeetria).

Midagi, mida sa tead

Kõige tavalisem autentimise vahend on olnud parool, PIN-kood, parool või küsimused ja vastused. Kasutaja sisestab info, mida programm võrdleb varem salvestatud andmetega.

Midagi, mis sul on

Enne nutitelefonide tulekut kandsid kasutajad paroolikaarte või PIN-kalkulaatoreid endaga kaasas. Täna kasutatakse valdavalt nutitelefoni ja mingit autentimisrakendust, mis võimaldab siseneda rakenduse loodud ainulaadse pääsukoodiga.

Midagi, mis/kes sa oled

Biomeetrilised tehnoloogiad aitavad sõrmejälgede, võrkkesta skaneerimise, näotuvastuse, hääletuvastuse või kasutaja käitumise abil kasutajat tuvastada.

Kas paroolide kasutamine kaob siis ära?

Enamik kasutajaid soovib kiiret ja hõlpsat autentimist ja juba praegu saab parooli kasutamist märkimisväärselt vähendada. Uutel tehnoloogiatel on eelised nii turvalisuse kui ka kasutajakogemuse osas.

Telefoni või sülearvuti lukust vabastamine näo või sõrmejälje abil on muutunud normiks.

Biomeetriline autentimine tähendab seda, et meie unikaalsed füsioloogilised ja anatoomilised omadused on taandatud arvutiparameetritele ehk muudetud digitaalseks koodiks. Ühest küljest on inimesi alati tuvastatud nende hääle, kõnnaku või näo järgi, aga mis võib muutuda häirivaks, on absoluutne usaldus algoritmide vastu. Tegelikult võivad ka nemad vigu teha, ka biomeetrial on puudusi. Seda tõestas Jan Krissler juba 2014. aastal, kui ta häkkis Euroopa Komisjoni presidendi Ursula Von der Leyeni sõrmejälje, kasutades tema pöidla HD-pilte pressikonverentsilt. Sõrmejälge on väga lihtne kuskilt jäetud jäljest kopeerida, eriti madala kvaliteediga andurite puhul. Kuid on juba ka keerukamaid tehnoloogiaid, mis võtavad arvesse selliseid tegureid nagu sõrme temperatuur ja hapnikuga varustatus.

Kaheastmelise autentimise saab panna peale nii MS 365 kontole, Gmaili kontole, Facebookile kui paljudele teistele teenustele. Kui kasutaja on oma kasutajanime ja parooli sisestanud, küsitakse kontrollkoodi, mis saadetakse SMS-iga.

Kontrollkood on ju veelgi tüütum kui paroolide meeldejätmine?

Sõnumi abil on natuke tüütu küll sisse logida. Aga spetsiaalsed rakendused nagu Microsoft Authenticator, Google Authenticator, LastPass ja teised teevad asja lihtsamaks. Ise kasutame tegelikult valdavalt äppi nimega Authy, mille eelisteks Microsoft Authenticatori ees on *multi-device* tugi ja *backup*'i teenus. See tähendab seda, et kui telefoni aku saab tühjaks, on võimalik autentimiseks kasutada ka mõnda muud seadet. Kui aga telefon peaks ära kaduma või ostad uue, on backup teenuse abil võimalik *master* koodi abil väga lihtsalt võimalik seadistada varasemalt loodud ligipääsud.

Samuti on võimalus end paroolideta autentida turvavõtme ehk *hardware token*'i abil. Miinus on see, et seade peab olema kogu aeg kaasas.

Mida peaksid ettevõtted tegema, et autentimine oleks murevaba, aga turvaline?

Näeme Microsoft 365 rünnakukatseid, kui kontosid proovitakse kaaperdada, igapäevaselt. Kaheastmeline autentimine on elementaarseim ja peamine MS 365 turva-element, mis tuleks igal ettevõttel peale panna. Microsofti statistika kohaselt väheneb kaheastmelise autentimisega kontode kaaperdamise oht 99,9%. Visalt, kuid tasapisi on see saamas suuremates organisatsioonides normiks.

Murekoht on täna see, et paljud portaalid, mis sisaldavad kriitilisi isikuandmeid või raamatupidamisinfot, ei ole varustatud nüüdisaegsete turvavõimalustega. Näiteks mõned väga paljusid puudutavad rakendused meditsiinisektorist, kus hoitakse patsientide tundlikke andmeid (isikuandmeid ja haigusluguside), ei toeta kaheastmelist autentimist.

Tugeva autentimise tagab erinevate tegurite kombinatsioon. Kuniks paroolid veel on olemas, on oluline, et neid ei kasutataks üksi. Microsoft ja teised töötavad uuenduslike ja kasutajasõbralike turvalahenduste kallal, nii et varem või hiljem saame kindlasti ka paroolideta hakkama.

- Lahendused
- Turvalisus

Pilt

