Workforce Security and Risk Training

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Kā sabojāt uzbrucējam dienu? Ar MFA (daudzfaktoru autentifikāciju)!

Kas ir vienkārši jums, ir vienkārši arī uzbrucējam

Džeims atpūtās mājās, kad viņa tālrunī pēkšņi parādījās virkne paziņojumu. Viņa personīgā e-pasta parole bija nomainīta, taču viņš neatcerējās, ka būtu kaut ko mainījis. Drīz pēc tam sekoja paziņojumi arī no sociālo mediju kontiem, informējot, ka ir nomainītas to paroles, un pēc tam banka brīdināja par aizdomīgiem pirkumiem. Panikā Džeimss mēģināja piekļūt savam e-pastam, taču viņa parole vairs nedarbojās. Kāds viņam bija liedzis piekļuvi! Dažas nākamās dienas Džeimss pavadīja atgūstot piekļuvi kontiem, apstrīdot maksājumus un mainot paroles. Visvairāk viņu mulsināja tas, ka viņš bija darījis visu, ko, viņaprāt, vajadzēja darīt. Viņš izmantoja spēcīgu paroli un nekad to nevienam neatklāja!

Taču problēma nebija parole – problēma bija paļaušanās tikai uz paroli. Džeimss neapzinājās, ka steidzamā īsziņa, ko viņš pagājušajā nedēļā saņēma no šķietamā e-pasta pakalpojumu sniedzēja, patiesībā bija kibernoziedznieka sūtīta, kurš ar viltu bija izmānījis viņa paroli. Tiklīdz kibernoziedznieks ieguva Džeimsa e-pasta paroli, viņš pilnībā pārņēma kontroli pār viņa e-pasta kontu. Viņš ne tikai ieguva piekļuvi visiem Džeimsa e-pastiem, bet varēja izmantot e-pasta kontu, lai atiestatītu paroles daudziem citiem viņa kontiem.

Džeimsa māsa Ariela saņēma tieši tādu pašu īsziņu, un tāpat kā viņas brālis, arī viņa tika maldināta, lai noklikšķinātu uz krāpnieciskas saites un ievadītu savu paroli Tomēr atšķirībā no Džeimsa Ariela sava e-pasta konta aizsardzībai izmantoja daudzfaktoru autentifikāciju (MFA). Tas nozīmēja, ka uzbrucējam trūka otrā faktora, kas nepieciešams pieteikšanās procesam (papildus parolei), un viņam nācās veikt nesekmīgus pieteikšanās mēģinājumus. Ariela apturēja uzbrucēju un viņai izdevās nosargāt savu e-pastu. Drīz pēc tam viņa palīdzēja arī brālim aktivizēt MFA.

Kas ir daudzfaktoru autentifikācija (MFA)?

Daudzfaktoru autentifikācija jeb MFA ir vienkāršs veids kā bezmaksas pievienot papildu drošības līmeni saviem kontiem. Tā vietā, lai paļautos tikai uz paroli, daudzpakāpju autentifikācija (MFA) izmanto otro līmeni (vai faktoru), lai pārliecinātos, ka tiešām esat jūs. Izmantojot MFA, lai pieteiktos, parasti ir nepieciešami vismaz divi no šiem elementiem:

- **kaut kas, ko zināt** - jūsu parole.
- **kaut kas, kas jums pieder** - vienreizlietojams kods, kas ir nosūtīts uz jūsu tālruni vai ģenerēts lietotnē.
- **kaut kas, kas jūs raksturo** - pirksta nospiedums vai sejas atpazīšana.

Pat ja kibernoziedznieks nozog jūsu paroli, viņš joprojām nevar piekļūt jūsu kontam bez otrā faktora. Tāpēc MFA ieslēgšana bieži tiek uzskatīta par **vienu no svarīgākajām darbībām, ko varat veikt, lai aizsargātu savus kontus**.

Kā pareizi izmantot MFA

Labā ziņa ir tā, ka daudzfaktoru autentifikācija (MFA) ir vienkārši lietojama un plaši pieejama. To bez maksas piedāvā lielākā daļa populāro pakalpojumu (e-pasts, internetbanka, sociālie mediji un iepirkšanās vietnes). Bieži vien katrā vietnē ar MFA jāpiesakās tikai vienu reizi. Pēc tam vietne atpazīst un "atceras" jūsu pārlūkprogrammu, padarot autentifikāciju ne tikai drošāku, bet arī ērtāku. Lūk, kā sākt:

1. Ieslēdziet MFA saviem svarīgākajiem kontiem: sāciet ar e-pastu, internetbanku, ieguldījumu kontiem un citiem svarīgiem kontiem. Ņemiet vērā, ja kāds iegūst piekļuvi jūsu e-pastam, viņš parasti var atiestatīt piekļuvi arī citiem jūsu kontiem.

2. Ja iespējams, izmantojiet autentifikācijas lietotni: viens no izplatītākajiem veidiem, kā saņemt otro faktoru, ir vienreizlietojama koda saņemšana īsziņā. Tomēr autentifikācijas lietotnes izmantošama ir vēl drošāks un uzticamāks risinājums. Autentifikācijas lietotne tiek instalēta jūsu tālrunī un tā ģenerē vienreiz lietojamus kodus, kas ir redzami lietotnē, nevis īsziņā.

3. Izmantojiet MFA kopā ar spēcīgām parolēm: MFA ir ļoti efektīva, taču vislabāk darbojas kopā ar spēcīgām un unikālām parolēm. Papildus MFA vienmēr izmantojiet katram kontam spēcīgu un unikālu paroli. Ja vietnes piedāvā jūsu kontam izmantot piekļuves atslēgas (passkeys), ziniet, ka piekļuves atslēga ir droša MFA versija.

4. Aizsargājiet savas mobilās ierīces: mobilā ierīce tagad ir kļuvusi par būtisku MFA izmantošanas daļu. Tajā bieži atrodas gan daudzfaktoru autentifikācijas (MFA) lietotnes, gan paroļu pārvaldnieks. Viedtālrunis nodrošina piekļuvi lielai daļai jūsu digitālās dzīves, tāpēc tās drošība ir īpaši svarīga. Pasargājiet savu mobilo ierīci, ieslēdzot ekrāna bloķēšanu un automātiskos atjauninājumus.

Kontrolējiet savu drošību

MFA ieslēgšana ir viens no efektīvākajiem veidiem, kā pasargāt sevi tiešsaistē. Negaidiet, līdz jūsu konti tiks apdraudēti, kā tas notika ar Džeimsu. Esiet kā Ariela un parūpējieties, lai slikta diena būtu uzbrucējam, nevis jums.

Viesredaktore

Beta Laiona-Delsordo (Betta Lyon Delsordo) ir AWS ielaušanās testētāja, kura specializējas lietotņu, mākoņdatošanas un MI drošībā. Viņai ir Džordžijas Tehnoloģiju institūta maģistra grāds kiberdrošībā, kā arī GPEN sertifikāts. Beta ir uzstājusies DEF CON, Pasaules Bankas, WiCyS pasākumos un konferencēs visā ASV un Eiropas Savienībā.

Resursi

Kā kibernoziedznieki nozog jūsu paroles: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions
Frāžveida paroļu spēks: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
Paroļu pārvaldnieka spēks: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager

Tulkoja: **CERT.LV**

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