Kaip sužinoti, kad jūsų paskyra „nulaužta“?

Programišiai išpuolius rengia kas 39 sekundes, rodo tyrimų duomenys, tad vartotojai yra nuolatiniame kibernetinių atakų pavojuje. Jų metu gali būti pavogti asmens duomenys, jautri asmeninė informacija, prisijungimai prie paskyrų, kurias atgauti – sudėtinga. Atpažinti atakas padės neįprastas dažniausiai naudojamų paslaugų veikimas, o apsisaugoti – tinkami slaptažodžiai, dvigubos autentifikacijos funkcija ir prevencinės priemonės.

„Įprastai kibernetinės atakos būna nutaikytos į svarbias pareigas einančius arba žinomus žmones, turtingas organizacijas, ar net valstybes. Taip yra todėl, kad šie „taikiniai“ sėkmingos atakos atveju turi tai, ko programišiams labiausiai reikia – arba svarbios, naudingos, skandalingos informacijos, arba pakankamai pinigų išpirkai už ją. Bet tai visiškai nereiškia, kad atakos negali būti nukreiptos į „paprastus“ žmones – jos taip pat dažnos, skiriasi tik jų mastas ir forma – dažniausiai siekiama ne gauti pinigų, bet naudojantis vartotojo paskyra dalintis kenkėjiškomis nuorodomis, reputacijai kenkiančia informacija, apgaulingomis žinutėmis“, – sako Saulius Skirmantas, „Bitės“ kibernetinio ir IT saugumo vadovas, bei paaiškina, kaip atpažinti kibernetinės atakos ženklus ir nuo programišių apsisaugoti.

Ar sunku atpažinti atakas?

Dažniausiai apie įsilaužimą sužinome tuomet, kai žala jau padaryta – vartotojo socialiniuose tinkluose atsiranda neįprasti įrašai, draugai informuoja apie gautas keistas žinutes, banko sąskaitoje pastebime pinigų trūkumą ir kitais atvejais.

„Viena ryškiausių detalių, nurodančių galimą įsilaužimą, yra neįprastas įprastų paskyrų veikimas. Pavyzdžiui, įtarimų turėtų kelti situacija, kai su savo prisijungimo duomenimis negalite pasiekti dažniausiai naudojamų paskyrų, ar banko sąskaitoje matote kad ir mažus, bet niekada jūsų neatliktus pavedimus. Visa tai gali nurodyti, kad į jūsų paskyras įsilaužta arba pavogti jūsų asmeniniai duomenys, leidžiantys prisijungti prie šių paskyrų ir jomis naudotis be jūsų leidimo“, – sako „Bitės“ ekspertas.

Apie įsilaužimus ar neteisėtus prisijungimus praneša ir pačios programėlės – pavyzdžiui „Facebook“ ir „Google“ siunčia pranešimus ir elektroninius laiškus apie tai, kad paskyrą buvo bandoma pasiekti be savininko žinios. Gavus tokią žinutę ir iš karto sureagavus, įmanoma užkirsti kelią programišiams dar iki tol, kol nepadaryta didesnė žala. „Tokios įspėjamosios žinutės turi tik vieną trūkumą – jos nurodo tiek bandymą jungtis prie paskyros, tiek sėkmingą prisijungimą. Antruoju atveju paskyros apsaugoti galite ir nespėti, nes gali būti pakeisti prisijungimai prie jos ar kiti svarbūs nustatymai, neleidžiantys jos pasiekti teisėtam savininkui“, – sako S. Skirmantas.

Apie įsilaužimus ir duomenų vagystes dažniausiai tiek viešai, tiek asmeniškai vartotojams praneša ir juos patyrusios kompanijos ar programėlės. Gavus tokią žinutę galima iš karto patikrinti, ar nuo atakos nenukentėjote ir imtis saugumo priemonių, kurias įprastai pateikia apie ataką pranešusios kompanijos.

Kaip paskyras susigrąžinti?

Pastebėjus, kad paskyra nulaužta, pirmiausia būtina atgauti jos valdymą tam, kad būtų galima ją iš naujo apsaugoti ir pakeisti prisijungimo duomenis. „Pirmiausia, susisiekite su kompanijomis, kurių produktus naudojate. Pavyzdžiui, jei negalite prisijungti prie „Google“ paskyros, keliaukite į jos atkūrimo puslapį ir atlikite visas reikiamas procedūras. Jei manote, kad įsilaužta į jūsų „Facebook“ paskyrą, taip pat pagalbos ieškokite tam skirtame puslapyje. Pastebėję įtartinus pavedimus iš jūsų banko sąskaitos, kreipkitės pagalbos į banką“, – sako S. Skirmantas.

Negalėdami prisijungti prie savo paskyros ir turėdami įtarimų, kad ji gali būti užgrobta, venkite keisti slaptažodį, naudojant kiekviename puslapyje esančią funkciją „Forgot my password“ (liet. Pamiršau slaptažodį), prideda ekspertas. Naujasis slaptažodis dėl programišių pakeistų paskyros nustatymų gali būti išsiųstas ne į jūsų el. pašto dėžutę, tad toks veiksmas susigražinti paskyros nepadės. „Jei vis tik prie užgrobtos paskyros prisijungti galite, tuoj pat pakeiskite jos slaptažodį nauju – tokiu būdu senasis, kurį pagrobė programišiai, nebeteks prasmės. Jei senąjį slaptažodį naudojote ir kitose paskyrose, jį pakeiskite ir ten“, – prideda S. Skirmantas.

Kitas svarbus žingsnis – tik atsiradus galimybei, nedelsiant apie paskyros užgrobimą ir visą situaciją informuoti žmones, kurie galėjo ar gali nuo to tiesiogiai nukentėti. „Dažnai programišiai iš jūsų paskyros gali išsiųsti užkratą turinčias žinutes, jas paspaudę jūsų draugai pateks į pavojingą interneto puslapį, kur ir jų duomenys gal būti pavogti. Jei pastebėjote, kad tokios žinutės išsiųstos, nedelsiant informuokite jų gavėjus, kad atsiųstų nuorodų neatvertų“, – sako S. Skirmantas. Esant reikalui, apie įsilaužimą galima informuoti ir Lietuvos policiją, tačiau skubių saugumo priemonių rekomenduojama imtis patiems.

Kaip apsisaugoti iš naujo?

Atgavus užgrobtų paskyrų kontrolę, jas reikia iš naujo tinkamai apsaugoti, kad būtų užkirstas kelias tolimesniems nesklandumams ateityje.

„Pirmiausia, paskyros turi būti apsaugotos tinkamais slaptažodžiais. Kurdami naują, venkite naudoti savo gimimo datą, itin paprastą skaičių seką – 111111, 123456, ar stulpelį

sudarančią kombinaciją, pavyzdžiui, 7410 ir panašias. Verčiau rinkitės logikos neturinčių ženklų kombinaciją, sudarytą iš raidžių, simbolių ir skaičių. Idealiu atveju, kiekvienai paskyrai naudokite skirtingus slaptažodžius, o juos saugokite tam skirtose, užraktus turinčios programėlėse, pavyzdžiui, „LastPass“, – pataria S. Skirmantas.

Paskyras rekomenduojama papildomai apsaugoti naudojant dvigubą autentifikaciją (angl. Two-factor authentification arba 2FA) – dviejų žingsnių prisijungimo prie paskyros paslaugą. „Tai būdas patvirtinti vartotojo tapatybę, naudojant dviejų apsaugos veiksmų derinį. Pirmasis veiksmas – toks, kuriam naudojame mums žinomą informaciją, pavyzdžiui, apsaugos slaptažodį. O antrajam naudojame tai, ką automatiškai kiekvieno jungimosi metu sugeneruoja puslapis, prie kurio jungiamės, ar papildomos programėlės. Funkciją aktyvuoti galite paskyrų, kurias norite apsaugoti, nustatymuose“, – sako S. Skirmantas.

Tokia registracija gerokai saugesnė ir sunkiau „nulaužiama“. Pavyzdžiui, jei nevykdydami jokio prisijungimo vis tiek gausite pranešimą, kad kodas sugeneruotas, tai reikš, kad prie jūsų paskyros bandoma neteisėtai jungtis. Tokiu atveju jums tereikės kodo generavimo etape procesą sustabdyti ir įtartinas prisijungimas bus iškart nutrauktas.

Kaip neužkibti ant programišių kabliuko?

Tinkamai apsaugojus paskyras slaptažodžiais, verta galvoje turėti keletą saugumo patarimų, kurie padės nepakliūti į programišių pinkles. Pirmiausia, būtina pasirūpinti tinkamomis programėlėmis ir jų atnaujinimais.