Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
SLAPTAŽODŽIŲ STIPRUMAS, SUDĖTINGUMAS IR SAUGA

2020 m. liepos 7 d.

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos primena, kad yra itin svarbu pasirinkti saugų bei stiprų slaptažodį. Neretai slaptažodis yra vienintelis saugumo barjeras tarp vartotojo ir jo turimos informacijos. Egzistuoja daug programų, kurių pagalba piktavalis gali siekti sužinoti slaptažodį ir pasisavinti asmens saugomą informaciją. Tačiau pasirenkant tinkamą slaptažodį, galima labai apsunkinti kelią kitiems gauti prieigą prie jūsų duomenų.

Kam reikalingas stiprus slaptažodis?

Žmonės kasdien naudojasi slaptažodžiais ir tai yra pagrindinė autentifikavimo priemonė. Jos yra skirtos tam, kad tik įgalioti asmenys galėtų pasiekti jiems skirtą informaciją. Kad ir kaip būtų sunku atsiminti visus skirtingus slaptažodžius ir skaičių kombinacijas, reikia nepamiršti jog būtent jie saugo jūsų asmeninius duomenis nuo pašalinių asmenų. Kuo slaptažodis ilgesnis ir sudėtingesnis, tuo jis tampa stipresnis, tad natūralu, kad jį sunkiau atspėti piktavaliui.

Koks yra sudėtingas slaptažodis?

Sudėtingas slaptažodis yra tas, kurį sudarant laikomasi šių kriterijų:

- Slaptažodis netrumpesnis nei 12 simbolių (jei leidžiama – pageidautina 14 ir daugiau);
- Naudojamos didžiosios raidės, mažosios raidės, skaitmenys bei specialieji simboliai;
- Slaptažodis turi būti unikalus ir daugiau niekur kitur nenaudojamas.

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Kaip pasirinkti saugų slaptažodį?

1. Venkite dažnai pasitaikančių klaidų

Daugelis naudoja slaptažodžius, paremtus asmenine informacija, tad juos lengva įsiminti. Tačiau juos taip pat lengva ir atspėti. Kiti naudoja slaptažodžius, sudarytus iš paprastų žodžių. Tai taip pat yra nesaugu, kadangi egzistuoja tokio tipo atakos, kurios vadinasi žodyno parinkimo atakos (angl. *dictionary attack*), kai piktavalis slaptažodį bando „nulaužti“ automatiškai tikrindamas kiekvieną žodį iš žodyno. Vien pakeitus kelias raides į didžiąsias ar mažąsias bei pridėjus kelis skaitmenis ar specialiuosius simbolius galima stipriai pagerinti savo slaptažodžio saugumą.

Nr.	Slaptažodis
1	123456
2	123456789
3	qwerty
4	password
5	1234567
6	12345678
7	12345
8	iloveyou
9	111111
10	123123
11	abc123
12	qwerty123
13	1q2w3e4r
14	admin
15	qwertyuiop

Lentelė. 1. Top 15 dažniausia naudotų slaptažodžių 2019 m.

2. Kurkite ilgesnį ir sudėtingesnį slaptažodį

Šie du veiksniai yra pagrindiniai, kurie įtakoja, ar pasirinktas slaptažodis pakankamai saugus, ar ne. Natūralu, kad kuo slaptažodis ilgesnis ir kuo jame daugiau skirtingų ženklų, raidžių ir skaitmenų, tuo ilgiau užtrunka jį atspėti. Toks slaptažodis yra atsparesnis slaptažodžių parinkimo (angl. *brute force*) atakoms. Paprastas pavyzdys: tarkime jūsų slaptažodis yra sudarytas iš mažųjų raidžių (a-z) ir yra 4 simbolių ilgio. Vadinasi, galimų kombinacijų skaičius yra $26^4 = 456976$. Atrodo nemažas skaičius, tačiau, naudojantis kiek geresniu nei įprastu namų kompiuteriu, tokią kombinaciją „nulaužti“ galima per 0.2 milisekundės. Didinant slaptažodžio ilgį, didėja galimų kombinacijų skaičius ir ilgėja laikas, per kurį automatizuotos sistemos gali atspėti slaptažodį.

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Patarimai ir rekomendacijos

Susigalvoję stiprų ir patikimą slaptažodį daugelis jį pradeda naudoti visur. Tai yra bene didžiausia klaida. Naudojant net ir stiprų slaptažodį keliose skirtingose vietose, padidėja tikimybė jog jis bus atspėtas. Jeigu kažkas sužinos jūsų slaptažodį vienoje platformoje, piktavalis galės juo naudotis prisijungti prie kitų vietų, kurias esate apsaugojąs tuo pačiu slaptažodžiu. Reikia nepamiršti, jog tobulėjant technologijoms, net ir ilgą bei sudėtingą slaptažodį atspėti tampa paprasčiau ir greičiau.

Svarbiausia atminti jog reikia:

- Naudokite skirtingus slaptažodžius skirtingose platformose ar sistemose;
- Naudokite slaptažodžių saugojimo programines įrangas, kurios padės sekti jūsų slaptažodžius (daugiau informacijos apačioje);
- Nenaudokite slaptažodžių, kurie yra paremti jūsų asmenine informacija;
- Nenaudokite slaptažodžių randamų bet kurios kalbos žodynuose;
- Nenaudokite elementarių slaptažodžių, tokių kaip: „labas“, „password“, „slaptazodis“, „1234“ ir pan.;
- Periodiškai keiskite savo slaptažodį.

Kaip apsaugoti ir atsiminti savo slaptažodį?

Niekada neužsirašinėkite slaptažodžio ir nepalikite jo vietose, kur kiti galėtų jį rasti, pavyzdžiui, ant savo darbo stalo. Tokiu atveju žmonės, galintys patekti į jūsų darbo vietą, lengvai gali prisijungti prie jūsų paskyrų. Niekada niekam nesakykite savo slaptažodžio. Būkite budrūs, nes piktavaliai visokiais būdais stengiasi išvilioti slaptažodžius, ar tai būtų telefoninis skambutis ar elektroninis laiškas, kuriuo apsimetama tam tikrais žmonėmis ar įstaigomis ir prašoma atsiųsti savo slaptažodį. Taip pat reikia atminti, jog daugelyje naršyklių galima išsaugoti slaptažodžius, tačiau to daryti nereikėtų, nes bet kas, kas gali gauti prieigą prie jūsų kompiuterio, automatiškai gauna prieigą prie visų išsaugotų slaptažodžių. Naudodamiesi viešu kompiuteriu visada nepamirškite atsijungti nuo savo paskyrų. Venkite naudotis viešu Wi-Fi ryšiu jungdamiesi prie savo elektrinio pašto ar banko paskyrų. Naudodamiesi viešais tinklais, papildomai naudokite Virtualų privatų tinklą (angl. *Virtual private network (VPN*)).

Verta paminėti jog yra programinė įranga, skirta slaptažodžių saugojimui. Nors slaptažodžių užsirašinėti nederėtų, tačiau jeigu jų turite daug ir norite prisiimti tokią riziką, darykite tai teisingai. Specialios slaptažodžių tvarkyklės gali saugoti visus jūsų turimus slaptažodžius vienoje vietoje. Dažniausiai jie būna apsaugoti pagrindiniu (angl. *master*) slaptažodžiu, tačiau dauguma slaptažodžių tvarkyklių papildomai turi ir 2 žingsnių autentifikavimo funkciją (apie ją skaitykite žemiau). Slaptažodžiai būna saugomi lokaliai jūsų kompiuteryje arba debesyje (angl. *cloud-based*). Papildomai duomenų bazės, kuriose talpinami jūsų slaptažodžiai, tiek lokalios, tiek debesyje, yra šifruojamos. Tai tarsi slaptažodžių „seifas“ kuriuo galite naudotis, jei turite daug sudėtingų slaptažodžių ir juos visus atsiminti yra per sunku.

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Papildomai

Svarbu atminti paprastus saugumo pagrindus, kurie leis jums jaustis geriau dėl savo slaptažodžių saugumo:

- Visada pasitikrinkite ar naudojate naujausias operacinės sistemos, programinės įrangos bei naršyklės versijas;
- Naudokite ir atnaujinkite savo antivirusinę programinę įrangą, taip pat ugniasienę (angl. *„firewall“*);
- Reguliariai skenuokite savo kompiuterį dėl žalingo kodo;
- Sekite įtartiną veiklą savo paskyrose ir jei pastebėjote kažką, ko nedarėte ar nesate dėl to tikras, tuoj pat pasikeiskite savo slaptažodį;
- Neapsiribokite tik slaptažodžiu siekdami apsaugoti savo paskyras. Naudokite 2 žingsnių autentifikavimą. Papildomai prie slaptažodžio galima naudoti ir biometrinius duomenis (pirštų antspaudą, veido atpažinimą). Kiekviena papildoma autentifikavimo priemonė prie slaptažodžio prideda papildomą saugumo lygį.

Dviejų žingsnių autentifikavimas

Dviejų žingsnių autentifikavimas (angl. *Two-factor authentication - 2FA*) – tai prisijungimo procesas, kuris reikalauja ne tik prisijungimo vardo/el. pašto adreso ir slaptažodžio, bet kartu ir papildomo autentifikacijos būdo. Egzistuoja 3 pagrindiniai autentifikacijos būdai:

- Tai, ką žinote: jūsų slaptažodis, PIN, paskyros numeris ar betkokia kita skaitmenų ar raidžių seka;
- Tai, ką turite: USB saugos raktas, telefonas ar betkokia kita technologija kurią galite turėti fiziškai;
- Tai, kuo esate: jūsų pirštų antspaudas, akies, veido atvaizdas arba tiesiog – biometriniai duomenys.

Norint naudoti dviejų žingsnių autentifikaciją, būtina naudoti bent 2 iš 3 anksčiau paminėtų autentifikavimo būdų. Prisijungimui prie sistemų rekomenduojame visada naudoti dviejų žingsnių autentifikaciją, jeigu toks funkcionalumas įgalintas. Tai ženkliai padidins jūsų duomenų saugumą.