Ako si lepšie zabezpečiť svoj hostingový účet

Last updated 11 októbra, 2024

V tomto článku si ukážeme niekoľko tipov, ktorými môžete zvýšiť nielen bezpečnosť svojho webhostingového účtu, ale aj svojich dát na sieti všeobecne. Než sa pozrieme bližšie na jednotlivé tipy, tak vás uistíme, že v tom rozhodne nie ste sami – vo Webglobe považujeme bezpečnosť za jeden z najdôležitejších pilierov webhostingových služieb vôbec. Robíme všetko pre to, aby naše servery boli bezpečným miestom pre vaše dáta.

Aké dodržiavame bezpečnostné pravidlá?

- nepretržite monitorujeme chod všetkých našich serverov a vyhodnocujeme prípadné anomálie sieťovej prevádzky
- starostlivo vyberáme, testujeme a aktualizujeme softvér a hardvér
- pravidelne dáta zálohujeme
- kontrolujeme dáta na prítomnosť škodlivého kódu
- vykonávame bezpečné zmeny majiteľa domény
- aktívne blokujeme pokusy o uhádnutie hesla
- riadime sa striktnými bezpečnostnými postupmi
- našich zamestnancov pravidelne školíme
- nasadzujeme nástroje, ktoré pomáhajú zvýšiť bezpečnosť webhostingových účtov

Čo môžete urobiť pre bezpečnosť vy?

Veľa aspektov zabezpečenia vášho účtu máte v rukách vy sami. V prvom rade ide o nástroje, ktoré máte k dispozícii v administrácii svojho účtu a môžete ich tak ľahko využívať, alebo o postupy, ktorých dodržiavaním môžete znížiť riziko straty či kompromitácie dát. Týmito základnými zásadami sa zvládne riadiť skutočne každý a ako sami uvidíte, ich aplikácia v praxi nie je vôbec zložitá.

Zabezpečenie FTP účtu

FTP je hlavnou cestou ako nahrať dáta na diskový priestor webhostingového účtu. Zároveň však môže ísť o cestu, ako sa k vašim dátam dostane útočník, pokiaľ by sa mu podarilo získať alebo uhádnuť prihlasovacie údaje účtu. Na to, ako chrániť heslá, sa pozrieme podrobnejšie nižšie. Teraz počítajme s tým, že útočník skutočne používateľské meno a heslo pozná. FTP účty pri Webglobe hostingu je však navyše možné chrániť povolením prístupu len z niektorých krajín, konkrétnych IP adries alebo rozsahu IP. Ak je ochrana

aktívna, útočník sa k vašim dátam nedostane ani so znalosťou prihlasovacích údajov.

FTP ochrana funguje jednoducho tak, že zabráni prístupu k vašim dátam zo všetkých IP adries mimo tých, ktoré máte v administrácii účtu povolené. Podrobnejšie informácie si môžete prečítať v našej nápovede.

Odhlásenie z administrácie účtu

Administrácia vás pri dlhšej nečinnosti automaticky odhlási. Vďaka tomu sa zníži pravdepodobnosť, že by váš účet niekto ovládol po tom, čo s ním už nejaký čas nepracujete.

Môžete však voliteľne zapnúť pre prihlásenie aj dvojfaktorovú autentifikáciu alebo ochranu prístupu len z povolených krajín, IP adries či rozsahov IP. Toto opatrenie zabráni prihláseniu útočníka, aj keby poznal vaše prístupové údaje. Ak by sa o prihlásenie z nepovolenej IP adresy pokúsil, administrácia tento prístup nepovolí.

Ako bezpečne pracovať s heslami

Určite ste už počuli množstvo poučiek o tom, ako si zvoliť čo najzložitejšie heslo, ktoré navyše musíte často meniť. Pomôžeme vám zorientovať sa v tom, kedy je starostlivosť o vaše heslo skutočne dôležitá a tiež odôvodníme prečo.

Tvorba hesla

Jednoznačne platí, že čím zložitejšie heslo, tým lepšie. Útočník totiž nemusí pri ľahkom hesle nič prelamovať, ale jednoducho ho skúsi uhádnuť. Pri založení účtu vám od nás dorazí možnosť nastavenia si hesla do administrácie. Účty a heslá pre prístup k FTP a databázam je ďalej možné zriadiť priamo v administrácii.

Nie je vhodné voliť rovnaké heslá pre viacero služieb. Keby sa k takému heslu útočník dostal, nemožno vylúčiť, že ho skúsi použiť všade možne.

Zhrnieme si niekoľko základných pravidiel pre heslá:

- čím dlhšie heslo a viac znakových sád použijete, tým lepšie
- ku každej službe voľte iné heslo
- pokiaľ je to možné, heslá pravidelne meňte

Dôrazne odporúčame nastaviť si dostatočne silné heslo predovšetkým pre vašu e-mailovú schránku. Dôvodom nie je len to, aby sa útočník nedostal k vašim správam, ale ani k službám, pri ktorých máte danú e-mailovú adresu nastavenú ako kontaktnú. Obvykle je totiž možné si pri zabudnutom hesle nechať vygenerovať nové práve na vašu e-mailovú adresu. Cesta k ovládnutiu ďalších služieb/účtov tak môže viesť „len" cez prelomenie prístupu k e-mailovej schránke.

Pri všetkých spomínaných opatreniach môžete samozrejme voliť rozumný kompromis medzi mierou požadovanej bezpečnosti a užívateľskou prívetivosťou. Prioritu dajte službám/loginom, ktoré sú dôležité a ktorých kompromitáciou vám môže vzniknúť väčšia škoda, teda napr. vyššie zmienená e-mailová schránka alebo samotná administrácia webhostingového účtu.

Čo sa pravidelného menenia hesiel týka, tak chápeme, že toto je asi najmenej obľúbené opatrenie. Ale aj napriek tomu má zmysel. Opäť môžete voliť kompromisnú stratégiu, kedy meníte heslá častejšie predovšetkým pri dôležitých službách.

Bezpečné uchovanie hesla

V predchádzajúcom odseku sme vám poradili používať dostatočne silné a pre každú službu odlišné heslo. Samozrejme nemožno očakávať, že by ste si mali takéto heslá pamätať. Heslá je vhodné niekde bezpečne „skladovať" a na to najlepšie poslúži správca hesiel (password manager). Nebudeme odporúčať žiadny konkrétny nástroj – na internete ich nájdete skutočne veľa. Od bezplatných až po platené s množstvom ďalších funkcií a pluginov do webových prehliadačov. Moderné operačné systémy už majú vlastný natívne integrovaný program pre správu hesiel. Nech použijete akýkoľvek, výrazne vám to môže zjednodušiť dodržiavanie vyššie uvedených zásad.

U nás vo Webglobe si prácu bez správcu hesiel už nedokážeme predstaviť.

Ak heslá nemeníte príliš často, môže sa vám hodiť nástroj Have I been pwned? Stránku vytvoril známy propagátor internetovej bezpečnosti Troy Hunt a môžete si na nej overiť, či vaša e-mailová adresa (ne)figuruje pri niektorej zo služieb, ktorá bola v minulosti úspešne napadnutá útočníkmi (a ktorí sa tak zmocnili aj hesiel). Pokiaľ sa vám takáto služba zobrazí, určite si u nej ihneď svoje heslo zmeňte. Stránka pracuje s verejnými databázami ukradnutých či uniknutých loginov as nimi porovnáva vami zadanú adresu. Podľa tvorcov sa hľadané otázky nikam neukladajú, ale určite nezadávajte nič iné ako vašu e-mailovú adresu.

Veľký pozor na phishing!

Jedným z častých spôsobov ako vymámiť z užívateľa napr. prihlasovacie údaje je tzv. phishing. Ide o útok spadajúci medzi metódy sociálneho inžinierstva, ktorý spočíva v tom, že útočník rozošle e-mailovú správu, v ktorej sa snaží vzbudiť dojem, že bola odoslaná napríklad vašou bankou alebo prevádzkovateľom webhostingového účtu. Obsahom takého e-mailu býva naliehavá výzva na akciu (napr. otvorenie prílohy alebo kliknutie na odkaz), kde sa väčšinou však skrýva škodlivý kód alebo podvrhnutá prihlasovacia stránka.

V posledných rokoch sa phishingové útoky zdokonalili a už zďaleka nejde len o e-maily plné „lámanej slovenčiny“ s jednoduchou výzvou na zaslanie hesla či so zjavne podozrivými odkazmi. Útočníci často vytvoria vernú napodobeninu prihlasovacích stránok prevádzkovateľa vybranej služby a pri pokuse o prihlásenie tak získajú vaše skutočné prihlasovacie údaje. E-maily sú často písané na mieru vytipované obete (tzv. spearphishing) a môžu tak pôsobiť veľmi vierohodne.

Ako spoznať phishingové e-maily a ako sa proti nim brániť si môžete prečítať v našom článku tu.

Nikdy od vás nebudeme chcieť heslo k vášmu účtu! Niektoré úkony, ako prevod domény alebo pomoc s presunom dát od konkurencie zaslanie hesla vyžadujú, ale celý proces je iniciovaný z vašej strany a máte ho plne pod kontrolou. Nikdy sa teda nestane, že by sme vám z ničoho nič napísali alebo zavolali (telefonický spôsob kontaktu vytipovanej obete je v poslednej dobe veľmi obľúbený) a požadovali od vás akékoľvek prístupové údaje k akýmkoľvek službám.

Či už sa budete riadiť všetkými vyššie uvedenými tipmi alebo využijete len niektoré z nich, vždy je dobré používať hlavne „zdravý rozum“. Čo to znamená? Tak napríklad neoznamovať svoje heslo nikomu, kto by ho mohol zneužiť alebo sa neprihlasovať k službám z miest, kde je nezabezpečená wifi sieť.