Jak si lépe zabezpečit svůj hostingový účet

Poslední aktualizace 10 října, 2024

V tomto článku si ukážeme několik tipů, kterými můžete zvýšit nejen bezpečnost svého webhostingového účtu, ale také svých dat na síti obecně. Než se podíváme blíže na jednotlivé tipy, tak vás ujistíme, že v tom rozhodně nejste sami – ve Endora považujeme bezpečnost za jeden z nejdůležitějších pilířů webhostingových služeb vůbec. Děláme tedy vše pro to, aby naše servery byly bezpečným místem pro vaše data.

Jaká dodržujeme bezpečnostní pravidla?

- nepřetržitě monitorujeme chod všech našich serverů a vyhodnocujeme případné anomálie síťového provozu
- pečlivě vybíráme, testujeme a aktualizujeme software a hardware
- pravidelně data zálohujeme
- kontrolujeme data na přítomnost škodlivého kódu
- provádíme bezpečné změny majitele domény
- aktivně blokujeme pokusy o uhodnutí hesla
- řídíme se striktními bezpečnostními postupy
- naše zaměstnance pravidelně školíme
- nasazujeme nástroje, které pomáhají zvýšit bezpečnost webhostingových účtů

Co můžete pro bezpečnost udělat vy?

Mnoho aspektů zabezpečení vašeho účtu máte v rukou vy sami. Jednak jde o nástroje, které máte k dispozici v administraci svého účtu a můžete je tak snadno využívat, nebo o postupy, jejichž dodržováním můžete snížit riziko ztráty či kompromitace dat. Těmito základními zásadami se zvládne řídit skutečně každý a jak sami uvidíte, jejich aplikace v praxi není vůbec složitá.

Zabezpečení FTP účtu

FTP je hlavní cestou jak nahrát data na diskový prostor webhostingového účtu. Zároveň však může jít o cestu, jak se k vašim datům dostane útočník, pokud by se mu podařilo získat nebo uhodnout přihlašovací údaje účtu. Na to, jak chránit hesla, se podíváme podrobněji níže. Nyní počítejme s tím, že útočník skutečně uživatelské jméno a heslo zná. FTP účty u Endora hostingu je však navíc možné chránit povolením přístupu jen z některých zemí, konkrétních IP adres nebo rozsahu IP. Je-li ochrana aktivní, útočník se

k vašim datům nedostane ani se znalostí přihlašovacích údajů.

FTP ochrana funguje jednoduše tak, že zabrání přístupu k vašim datům ze všech IP adres mimo ty, které máte v administraci účtu povoleny. Podrobnější informace si můžete přečíst v naší nápovědě.

Odhlášení z administrace účtu

Administrace vás při delší nečinnosti automaticky odhlásí. Díky tomu se sníží pravděpodobnost, že by váš účet někdo ovládl poté, co s ním už nějakou dobu nepracujete.

Můžete však volitelně zapnout pro přihlášení i dvoufaktorové přihlášení nebo ochranu přístupu jen z povolených zemí, IP adres či rozsahů IP. Toto opatření zabrání přihlášení útočníka, i kdyby znal Vaše přístupové údaje. Pokud by se o přihlášení z nepovolené IP adresy pokusil, administrace tento přístup nepovolí.

Jak bezpečně pracovat s hesly

Určitě jste už slyšeli spoustu pouček o tom, jak si zvolit co možná nejsložitější heslo, které navíc musíte často měnit. Pomůžeme vám zorientovat se v tom, kdy je péče o vaše heslo skutečně důležitá a také zdůvodníme proč.

Tvorba hesla

Jednoznačně platí, že čím složitější heslo, tím lépe. Útočník totiž nemusí při snadném hesle nic prolamovat, ale prostě ho zkusí uhodnout. Při založení účtu vám od nás dorazí možnost nastavení hesla k administraci. Účty a hesla pro přístup k FTP a databázím je dále možné zřídit přímo v administraci.

Není vhodné volit shodná hesla pro vícero služeb. Kdyby se k takovému heslu útočník dostal, nelze vyloučit, že ho zkusí použít všude možně.

Shrneme si několik základních pravidel pro hesla:

- čím delší heslo a více znakových sad použijete, tím lépe
- ke každé službě volte jiné heslo
- pokud je to možné, hesla pravidelně měňte

Důrazně doporučujeme nastavit dostatečně silné heslo především u vaší e-mailové schránky.

Důvodem není jen to, aby se útočník nedostal k vašim zprávám, ale i ke službám, u kterých máte danou e-mailovou adresu nastavenou jako kontaktní. Obvykle je totiž možné si při zapomenutém hesle nechat vygenerovat nové právě na vaši e-mailovou adresu. Cesta k ovládnutí dalších služeb / účtů tak může vést „jen" přes prolomení přístupu k e-mailové schránce.

U všech zmíněných opatření můžete samozřejmě volit rozumný kompromis mezi mírou požadované bezpečnosti a uživatelskou přívětivostí. Prioritu dejte službám / loginům, které jsou důležité a jejichž kompromitací vám může vzniknout větší škoda, tedy např. výše zmíněná e-mailová schránka nebo samotná administrace webhostingového účtu.

Co se pravidelného měnění hesel týče, tak chápeme, že tohle je asi nejméně oblíbené opatření. Ale i přesto má smysl. Opět můžete volit kompromisní strategii, kdy měníte hesla častěji především u důležitých služeb.

Bezpečné uchování hesla

V předešlém odstavci jsme vám poradili používat dostatečně silné a pro každou službu odlišné heslo. Samozřejmě nelze očekávat, že byste si měli taková hesla pamatovat. Hesla je vhodné někde bezpečně „skladovat" a na to nejlépe poslouží správce hesel (password manager). Nebudeme doporučovat žádný konkrétní nástroj – na internetu jich najdete skutečně mnoho. Od bezplatných až po placené se spoustou dalších funkcí a pluginů do webových prohlížečů. Moderní operační systémy už mají vlastní nativně integrovaný správce hesel. Ať použijete jakýkoliv, výrazně vám to může zjednodušit dodržování výše uvedených zásad.

U nás ve Endora si práci bez správce hesel už nedokážeme představit.

Pokud hesla neměníte příliš často, může se vám hodit nástroj Have I been pwned? Stránku vytvořil známý propagátor internetové bezpečnosti Troy Hunt a můžete si na ní ověřit, zda-li vaše e-mailová adresa (ne)figuruje u některé ze služeb, která byla v minulosti úspěšně napadena útočníky (a kteří se tak zmocnili i hesel). Pokud se vám taková služba zobrazí, určitě si u ní ihned své heslo změňte. Stránka pracuje s veřejnými databázemi ukradených či uniklých loginů a s nimi porovnává vámi zadanou adresu. Dle tvůrců se hledané dotazy nikam neukládají, ale určitě nezadávejte nic jiného než vaši e-mailovou adresu.

Velký pozor na phishing

Jedním z častých způsobů jak vymámit z uživatele např. přihlašovací údaje je tzv. phishing.

Jde o útok spadající mezi metody sociálního inženýrství, který spočívá v tom, že útočník rozešle e-mailovou zprávu, ve které se snaží vzbudit dojem, že byla odeslána například vaší bankou nebo provozovatelem webhostingového účtu. Obsahem takového e-mailu bývá naléhavá výzva k akci (např. otevření přílohy nebo kliknutí na odkaz), kde se většinou však skrývá škodlivý kód nebo podvržená přihlašovací stránka.

V posledních letech se phishingové útoky zdokonalily a už zdaleka nejde jen o e-maily plné „lámané češtiny“ s jednoduchou výzvou k zaslání hesla či se zjevně podezřelými odkazy. Útočníci často vytvoří věrnou napodobeninu přihlašovacích stránek provozovatele vybrané služby a při pokusu o přihlášení tak získají vaše skutečné přihlašovací údaje. E-maily jsou často psané na míru vytipované oběti (tzv. spearphishing) a mohou tak působit velmi věrohodně.

Jak poznat phishingové e-maily a jak se proti nim bránit si můžete přečíst v našem článku zde.

Nikdy po vás nebudeme chtít heslo k vašemu účtu! Některé úkony, jako převod domény nebo pomoc s přesunem dat od konkurence *zaslání hesla vyžadují, ale celý proces je iniciován z vaší strany a máte ho plně pod kontrolou. Nikdy se tedy nestane, že bychom vám z ničeho nic napsali nebo zavolali (telefonický způsob kontaktu vytipované oběti je v poslední době velmi oblíbený) a požadovali od vás jakékoliv přístupové údaje k jakýmkoliv službám.*

Ať už se budete řídit všemi výše uvedenými tipy nebo využijete jen některé z nich, vždy je dobré používat hlavně „zdravý rozum“. Co to znamená? Tak například nesdělovat své heslo nikomu, kdo by jej mohl zneužít nebo se nepřihlašovat ke službám z míst, kde je nezabezpečená wifi síť.