

Zabezpečení WordPressu: Podrobný návod pro začínající uživatele

Poslední aktualizace 15 listopadu, 2024

WordPress je dnes jedním z nejpoblárnějších a nejrozšířenějších systémů pro správu obsahu na internetu. S jeho rostoucí popularitou se bohužel zvyšuje i riziko útoku a bezpečnostních hrozeb. Nicméně, existuje řada opatření, která můžete přijmout, abyste zajistili, že váš WordPress web zůstane bezpečný.

V tomto článku se podíváme na podrobný a strukturovaný návod, který vám pomůže zabezpečit váš WordPress web a ochránit ho před neoprávněným přístupem a potenciálními hrozbami.

Budeme se zde věnovat:

- Aktualizacím WordPressu, šablon a pluginů

Aktualizace WordPressu, šablon a pluginů

Jedním z nejdůležitějších opatření pro zabezpečení vašeho WordPress webu je pravidelná aktualizace.

Vývojáři WordPressu, šablon a pluginů pravidelně vydávají aktualizace, které zajišťují opravy bezpečnostních chyb a zranitelných míst, jimiž by se hackeři mohli dostat do vašeho účtu.

- **Důležitost aktualizací:**

Aktualizace jsou klíčové pro udržení maximální bezpečnosti vašeho webu. Nepřehlížejte žádné dostupné aktualizace.

- **Aktualizace WordPressu:**

Využíváte-li náš WordPress hosting, staráme se o pravidelné aktualizujte WordPressu za vás. Sami je můžete provést jednoduše přes administrátorské rozhraní.

- **Aktualizace šablon:**

Ujistěte se, že i u WordPress šablony máte vždy nejnovější verzi a aktualizujte ji, jakmile je k dispozici.

- **Aktualizace pluginů:**

WordPress pluginy jsou častým cílem útoků, proto je důležité je pravidelně aktualizovat na nejnovější verze.

O aktualizacích pluginů se zmiňujeme v článku [Jak nainstalovat WordPress pluginy](#).

Silné přihlašovací údaje

Přihlašovací údaje jsou bránou k vašemu WordPress webu, a proto je důležité zajistit, že jsou dostatečně silné a odolné vůči útokům.

Zde je pár tipů pro vytvoření bezpečných přihlašovacích údajů:

- **Unikátní uživatelské jméno:**

Používejte unikátní uživatelské jméno místo výchozího „admin“. To ztěžuje útočnickům uhodnout vaše přihlašovací údaje.

- **Silné heslo:**

Vytvořte silné heslo s kombinací velkých a malých písmen, čísel a speciálních znaků. Vyhněte se jednoduchým a snadno uhodnutelným heslům.

Přečtěte si, [jak změnit přihlašovací údaje do WordPressu](#).

Konec s nebezpečnou metodou pokus – omyl

Vyvarujte se nejčastějších chyb, které vám rozbíjí WordPress. Zaregistrujte se ZDARMA do Endora Academy a staňte experty na tvorbu webu.

[Zjistit více](#)

- **Používání dvoufaktorové autentizace (2FA):**

Zapněte dvoufaktorovou autentizaci, která poskytuje další vrstvu ochrany při přihlašování.

Omezení přístupu a ochrana souborů

Dalším důležitým krokem je omezení přístupu k vašemu WordPress webu a zabezpečení souborů.

Zde jsou některé praktické tipy:

- **Přístupová práva souborů a složek:**

Nastavte správná přístupová práva pro soubory a složky vašeho WordPress webu. Omezte zápisová práva pro nepotřebné soubory.

- **Omezení přístupu k administraci:**

Zabraňte neoprávněnému přístupu k administrátorskému rozhraní pomocí IP omezení nebo přesměrování z veřejné sítě.

- **Skrytí souboru wp-config.php:**

Přesuňte soubor wp-config.php na vyšší úroveň než veřejného adresáře nebo využijte plugin, který soubor skryje.

- **Ochrana souborů pomocí .htaccess:**

Použijte soubor [.htaccess](#) pro ochranu důležitých souborů a adresářů před přímým přístupem.

- **Zálohování a obnova souborů:**

Pravidelně [zálohujte své soubory](#), abyste měli možnost obnovit web v případě problémů.

Zabezpečení databáze

Databáze WordPressu obsahuje cenná data, a proto je důležité ji chránit.

Zde je přehled kroků, které můžete podniknout:

- **Unikátní předpona tabulek:**

Při instalaci WordPressu použijte unikátní předponu pro tabulky databáze, abyste minimalizovali riziko útoků.

- **Silné heslo pro přístup k databázi:**

Použijte silné heslo pro přístup k databázi. Mělo by se lišit od ostatních přihlašovacích údajů.

- **Omezení přístupu k databázi z veřejné sítě:**

Ujistěte se, že přístup k databázi je povolen pouze z důvěryhodných IP adres a omezte přístup z veřejné sítě.

Bezpečnostní pluginy a nástroje

Existuje řada bezpečnostních pluginů a nástrojů, které vám mohou pomoci chránit váš WordPress web.

Některé z nich jsou například:

- **Používání bezpečnostních pluginů:**

Instalujte a aktivujte bezpečnostní plugin, který vám poskytne dodatečné funkce pro ochranu a monitorování webu. V naší verzi WordPressu je pro vás připraven populární a velmi kvalitní plugin [Wordfence](#).

Zde je návod pro [nastavení Wordfence](#).

- **Firewall a blokování IP adres:**

Využijte firewall a možnost blokování podezřelých IP adres, které se pokouší provádět neoprávněné pokusy o přihlášení.

- **Kontrola a detekce škodlivého kódu:**

Použijte nástroje pro kontrolu škodlivého kódu a detekci potenciálních hrozeb na vašem webu.

- **Monitorování a auditování:**

Sledujte a monitorujte logy a auditní záznamy vašeho webu, abyste mohli identifikovat podezřelou činnost.

SSL certifikát a zabezpečené připojení

[SSL certifikát](#) poskytuje zabezpečené připojení mezi webovým prohlížečem a serverem.

- **Výhody SSL certifikátu:**

SSL certifikát zajišťuje šifrované připojení, které chrání citlivá data při přenosu mezi serverem a prohlížečem.

- **Nastavení SSL certifikátu:**

[Nainstalujte si SSL](#) certifikát na svůj web.

- **Přesměrování na HTTPS:**

Nastavte přesměrování z HTTP na [HTTPS](#), aby bylo zajištěno, že všechna připojení jsou zabezpečená.

Pravidelná zálohování

Pravidelné zálohování je zásadní pro obnovu webu v případě útoku nebo technických problémů.

- **Důležitost pravidelného zálohování:**

Pravidelné zálohování vám umožní obnovit váš web zpět do funkčního stavu v případě potíží.

- **Volba vhodného zálohovacího řešení:**

Vyberte si spolehlivý zálohovací nástroj nebo plugin, který vám umožní snadné zálohování a obnovu.

- **Ukládání záloh na bezpečné místo:**

Ukládejte zálohy na externí server nebo cloudové úložiště, abyste minimalizovali riziko

ztráty dat.