Zabezpečenie WordPressu: Podrobný návod pre začínajúcich používateľov

Last updated 13 septembra, 2024

WordPress je dnes jedným z najpopulárnejších a najrozšírenejších systémov na správu obsahu na internete. S jeho rastúcou obľúbenosťou sa, bohužiaľ, zvyšuje aj riziko útokov a bezpečnostných hrozieb. Existuje však niekoľko opatrení, ktoré môžete prijať a uistiť sa tak, že váš WordPress web zostane bezpečný.

V tomto článku sa pozrieme na podrobný a štruktúrovaný návod, ktorý vám pomôže zabezpečiť váš WordPress web a chrániť ho pred neoprávneným prístupom a potenciálnymi hrozbami.

Preto sa tu budeme venovať:

- Aktualizáciám WordPressu, šablón a pluginov

Aktualizácia WordPressu, šablón a pluginov

Jedným z najdôležitejších opatrení na zabezpečenie vášho WordPress webu je pravidelná aktualizácia.

Vývojári WordPressu, šablón a pluginov pravidelne vydávajú aktualizácie, ktoré zabezpečujú opravy bezpečnostných chýb a zraniteľných miest, prostredníctvom ktorých by sa hackeri mohli nabúrať do vášho účtu.

- **Dôležitosť aktualizácií:**

Aktualizácie sú kľúčové na udržanie maximálnej bezpečnosti vášho webu. Neprehliadajte žiadne dostupné aktualizácie.

- **Aktualizácia WordPressu:**

Ak využívate náš WordPress hosting, staráme sa o pravidelné aktualizácie WordPressu za vás. Sami ich môžete uskutočniť jednoducho prostredníctvom administrátorského rozhrania.

- **Aktualizácia šablón:**

Uistite sa, že aj vaše WordPress šablóny sú vždy v najnovšej verzii a aktualizujte ich hneď, keď je to možné.

- **Aktualizácia pluginov**

WordPress pluginy sú častým cieľom útokov, preto je dôležité ich pravidelne aktualizovať na najnovšie verzie.

O aktualizáciách pluginov píšeme v článku Inštalácia WordPress pluginov.

Silné prihlasovacie údaje

Prihlasovacie údaje sú bránou k vášmu WordPress webu, a preto je dôležité postarať sa o to, aby boli dostatočne silné a odolné voči útokom.

Tu je pár tipov na vytvorenie bezpečných prihlasovacích údajov:

- **Unikátne používateľské meno:**

Používajte unikátne používateľské meno namiesto predvoleného „admin“. To útočníkom skomplikuje uhádnutie vašich prihlasovacích údajov.

- **Silné heslo:**

Vytvorte si silné heslo s kombináciou veľkých a malých písmen, čísel a špeciálnych znakov. Vyhnite sa jednoduchým a ľahko uhádnuteľným heslám.

Prečítajte si, ako si zmeniť prihlasovacie údaje do WordPressu.

- **Používanie dvojfaktorovej autentifikácie (2FA):**

Zapnite si dvojfaktorovú autentifikáciu, ktorá poskytuje ďalšiu vrstvu ochrany pri prihlasovaní.

Obmedzenie prístupu a ochrana súborov

Ďalším dôležitým krokom je obmedzenie prístupu k vášmu WordPress webu a zabezpečenie súborov.

Tu je zopár praktických tipov:

- **Prístupové práva súborov a zložiek:**

Nastavte si k súborom a zložkám vášho WordPress webu správne prístupové práva. Obmedzte editorské práva k nepotrebným súborom.

- **Obmedzenie prístupu k administrácii:**

Zabráňte neoprávnenému prístupu k administrátorskému rozhraniu pomocou IP obmedzení alebo presmerovaní z verejnej siete.

- **Skrytie súboru wp-config.php:**

Presuňte súbor wp-config.php na vyššiu úroveň, než je verejný adresár alebo využite plugin, ktorý soubor skryje.

- **Ochrana súborov pomocou .htaccess:**

Použite súbor .htaccess na ochranu dôležitých súborov a adresárov pred priamym prístupom.

- **Zálohovanie a obnova súborov:**

Pravidelne zálohujte svoje súbory, aby ste mali možnosť v prípade problémov obnoviť web.

Zabezpečenie databázy

Databáza WordPressu obsahuje cenné údaje, a preto je dôležité ju chrániť.

Tu je prehľad krokov, ktoré môžete podniknúť:

- **Unikátna predpona tabuliek:**

Pri inštalácii WordPressu použite unikátnu predponu pre tabuľky databázy, aby ste minimalizovali riziko útokov.

- **Silné heslo na prístup do databázy:**

Použite silné heslo na prístup do databázy. Malo by sa líšiť od ostatných prihlasovacích

údajov.

- **Obmedzenie prístupu k databáze z verejnej siete:**

Uistite sa, že prístup k databáze je povolený len z dôveryhodných IP adries a obmedzte prístup z verejnej siete.

Bezpečnostné pluginy a nástroje

Existuje množstvo bezpečnostných pluginov a nástrojov, ktoré vám môžu pomôcť chrániť váš WordPress web.

Niektoré z nich sú napríklad:

- **Používanie bezpečnostných pluginov:**

Inštalujte a aktivujte si bezpečnostný plugin, ktorý vám poskytne dodatočné funkcie na ochranu a monitorovanie webu. V našej verzii WordPressu je pre vás pripravený populárny a veľmi kvalitný plugin Wordfence.

Tu je návod na nastavenie Wordfence.

- **Firewall a blokovanie IP adries:**

Využite firewall a možnosť blokovania podozrivých IP adries, ktoré sa pokúšajú o neoprávnené prihlásenie.

- **Kontrola a detekcia škodlivého kódu:**

Použite nástroje na kontrolu škodlivého kódu a detekciu potenciálnych hrozieb na vašom webe.

- **Monitorovanie a auditovanie:**

Sledujte a monitorujte logy a auditné záznamy vášho webu, aby ste mohli identifikovať podozrivú činnost.

SSL certifikát a zabezpečené pripojenie

SSL certifikát poskytuje zabezpečené pripojenie medzi webovým prehliadačom a serverom.

- **Výhody SSL certifikátu:**

SSL certifikát zabezpečuje šifrované pripojenie, ktoré chráni citlivé dáta pri prenose medzi serverom a prehliadačom.

- **Nastavenie SSL certifikátu:**

Nainštalujte si SSL certifikát na svoj web.

- **Presmerovanie na HTTPS:**

Nastavte si presmerovanie z HTTP na HTTPS, aby sa zabezpečilo, že všetky pripojenia sú zabezpečené.

Pravidelné zálohy

Pravidelné zálohy sú zásadné pre obnovu webu v prípade útoku alebo technických problémov.

- **Dôležitosť pravidelného zálohovania:**

Pravidelné zálohovanie vám umožní obnoviť váš web späť do funkčného stavu v prípade problémov.

- **Voľba vhodného zálohovacieho riešenia:**

Vyberte si spoľahlivý zálohovací nástroj alebo plugin, ktorý vám umožní jednoduché zálohovanie a obnovu.

- **Ukladanie záloh na bezpečné miesto:**

Ukladajte si zálohy na externý server alebo cloudové úložisko, aby ste minimalizovali riziko straty dát.

Ovládnite WordPress

S našim úplne novým WordPress hostingom je tvorba webu hračka.

Zistiť viac