Jak zabezpečit WordPress – kompletní průvodce pro rok 2025 (blog.jirivanek.eu)

Obsah knihy:

WordPress je jedním z nejoblíbenějších a nejrozšířenějších platforem pro tvorbu webových stránek na světě. Aktuálně pohání více jak 40 % všech webů napříč celým světem. Jeho jednoduché rozhraní a bohaté možnosti přizpůsobení ho činí oblíbenou volbou pro jednotlivce i firmy. Nicméně, popularita WordPressu přináší také výzvy, zejména v oblasti bezpečnosti. Jak zabezpečit WordPress je otázka, kterou si klade mnoho tvůrců webu a na kterou neexistuje jednoduchá odpověď. Bezpečnost webu je totiž komplexní záležitost, která vyžaduje čas a práci.

V dnešní době jsou webové stránky častým terčem útoků hackerů a škodlivého softwaru. A právě proto je důležité, aby majitelé webů byli obezřetní a přijímali kroky k zabezpečení svých stránek. Tento článek se zaměří na klíčové aspekty zabezpečení WordPressu a poskytne Vám praktické tipy a doporučení, jak chránit vaši webovou stránku před potenciálními hrozbami. Těchto 16 tipů a rad Vám pomůže zabezpečit WordPress do takové úrovně, kdy bude velmi obtížné, možná až nemožné do takového webu proniknout.

Bezpečnost WordPressu by měla být prioritou pro každého správce webové stránky. V tomto článku Vám pomůžu pochopit, jak ji dosáhnout a jak můžete svůj WordPress udělat nedobytným.

Vše začíná webhostingem

Výběr webhostingu je z hlediska bezpečnosti důležitým prvním krokem jak zabezpečit WordPress hned na startu. Mnoho poskytovatelů klasického sdíleného webhostingu již na WordPress myslí jako na důležitou součást ekosystému internetu a mají své Linuxové operační systémy z části zabezpečené proti různým typům útoků. Můžete se tak setkat s tím, že poskytovatel webhostingu má již implementovanou ochranu proti vícenásobnému pokusu o prolomení hesla do administrace, nebo má také implementovanou ochranu pomocí Geo-IP.

Hosting je základní a klíčová komponenta pro Váš web. Od jeho kvality se bude odvíjet nejen rychlost webu, ale také právě i samotná bezpečnost. Nebojte se tedy před nákupem webu zeptat poskytovatele na parametry poskytované služby.

Měly by Vás zajímat primárně tyto parametry:

- Zda Vám webhoster poskytne SSL certifikát k webu zdarma.
- Verze PHP na webu (optimálně ke dni napsání této knihy **8.3.** a **8.4.**).
- Velikost memory limitu (paměť přidělená Vašemu webu -> minimálně 256 MB jako základ, ideálně pak 512 MB a více).
- Velikost max execution time (doba, po kterou běží skript, než jej násilně ukončí server – důležité např. při migraci webu pomocí pluginů).
- Zda můžete nějaké directivy měnit pomocí souborů .htaccess nebo pomocí souboru .user.ini.
- Jaké základní bezpečnostní prvky web poskytuje (Geo-IP ochrana, ochrana proti brute Force útoku, ochrana proti DDOS …).

Jak vidíte, už samotný poskytovatel webhostingu může pro bezpečnost WordPressu udělat hodně a už samotný Linuxový systém, na kterém Váš web poběží může mít základní bezpečnost vyřešenou nativně. Ptejte se. Cena webu nemusí být rozhodující, protože ne vždy platí pravidlo, že nejlevnější webhosting bude nejlepší volbou. Tím, že se zároveň zeptáte zákaznické podpory na klíčové údaje ohledně provozu Vašeho nového webu, snadno zjistíte, jak rychle taková podpora reaguje na Vaše dotazy a případné budoucí problémy, které budete v průběhu času řešit. Kvalitní zákaznická podpora je základ pro úspěšný chod Vaší webové prezentace i pro její bezpečnost.

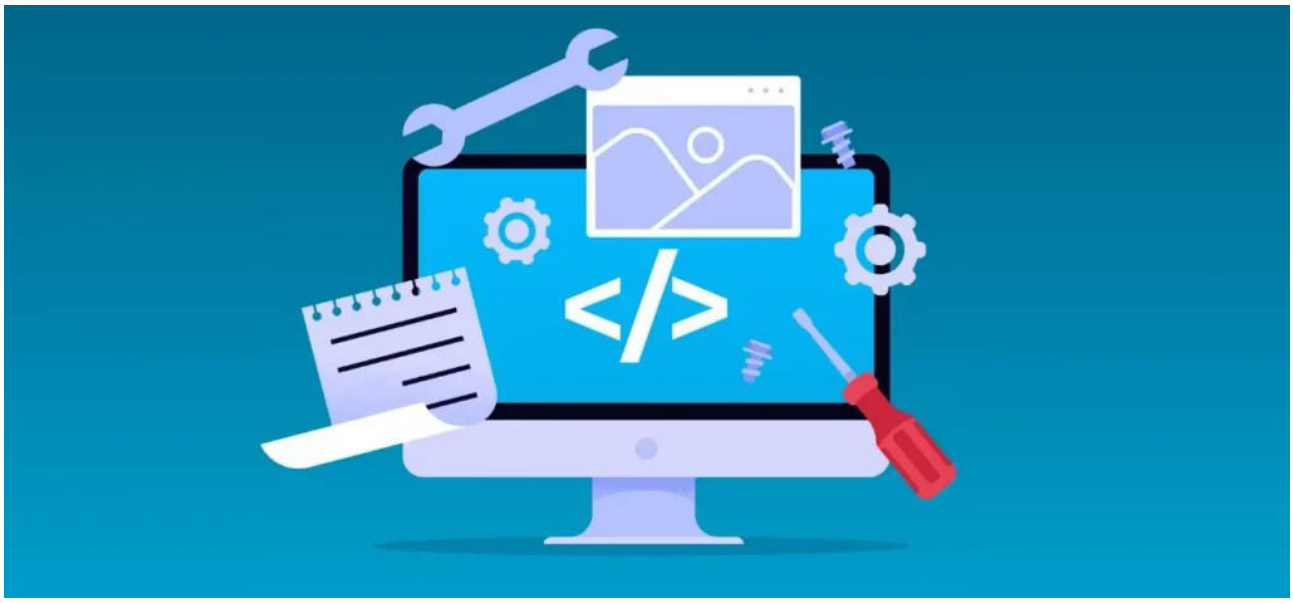
Proč je bezpečnější používat HTTPS

SSL a protokol HTTPS je v dnešní době nutnou podmínkou. Z mnoha důvodů. Nejprve si pojďme říct, k čemu SSL a HTTPS slouží. HTTPS protokol zajišťuje šifrovanou komunikaci mezi Vaším webem a počítačem uživatele, který se na tento web dívá. To zjednodušeně znamená, že tyto dva stroje si mezi sebou data vyměňují zašifrovaně. Pokud někdo mezi těmito stroji data zachytával, dostane je pouze v zašifrované podobě a nebude schopen zjistit, jaká data si tyto stroje mezi sebou vyměňují.

Z pohledu bezpečnosti je to důležité např. v momentě, kdy se přihlašujete do administrace WordPressu. Data, jako login a heslo se na server díky HTTPS odesílají v nečitelné formě, kterou není nikdo uprostřed schopen dešifrovat. To je pro zabezpečení WordPressu i Vašeho webu klíčové. Nechcete na server posílat heslo a login v plain text podobě, kterou může kdokoliv snadno odhalit.

V neposlední řadě na HTTPS kouká i samotný Google, který jeho používání hodnotí. Pokud na webu HTTPS nepoužíváte, bude Vás velmi pravděpodobně penalizovat a Vaše výsledky ve vyhledávání nebudou dobré. Samotný Google kontroluje zabezpečení WordPressu, které používáte a HTTPS je pro něj klíčový parametr. Dbejte tedy na to, aby HTTPS protokol byl součástí Vašeho webu a podle toho také vybírejte i poskytovatele webhostingu (viz. výše).

Instalace – uživatel, heslo a prefix (jak zabezpečit WordPress hned na začátku)



Pro zabezpečení WordPressu může mnoho základních kroků provést již při samotné instalaci tohoto redakčního systému. Jako základní bezpečnostní pravidlo mohu ihned zmínit opravdu silné heslo do MySQL databáze. Nepoužívejte slovní hesla, dají se velmi snadno odhalit. Použijte heslo, které bude mít minimálně osm znaků. Používejte malá i velká písmena, číslice a také nějaký speciální znak (**? ! #** apod.). Díky této praktice mnohonásobně zvýšíte počet pokusů, které by musel potenciální útočník vykonat, aby takové heslo dokázal odhalil. Díky této praktice se pak brute force útok na MySQL stává prakticky nemožný.

Další tři prvky, které můžete z hlediska bezpečnosti ovlivnit již při instalaci jsou prefix tabulek, jméno uživatele a jeho heslo. WordPress při základní instalaci používá prefix tabulek wp_. Změňte jej na svůj vlastní. Jakýkoliv útočník automaticky počítá s tím, že Váš prefix tabulek bude základní, tedy wp_. Neulehčujte mu práci a změňte prefix tabulek na libovolný svůj (**abc**_, **muj**_, **blog**_ …).

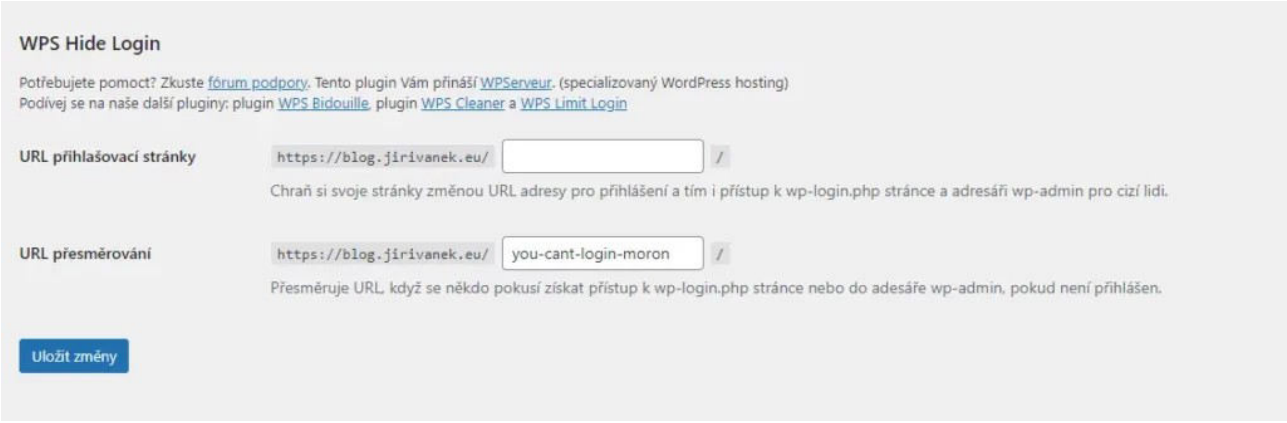
Co se dále zabezpečení WordPressu týče, potažmo hlavně administrace, je klíčový uživatel a jeho heslo. Opět narážím na defaultní hodnoty, kdy mnoho uživatelů při instalaci ponechá WordPressem předvyplněného uživatele admin. Upravte si login a uživatele admin nepoužívejte. Použijte např. své vlastní jméno. admin bude totiž první uživatel, kterého útočník při pokusu o prolomení hesla vyzkouší. Co se hesla týče, použijte stejnou praktiku popsanou výše u MySQL. Alespoň osm znaků a kombinace čísel, malých a velkých písmen a speciálních znaků.

Ideální stav po instalaci z pohledu bezpečnosti vypadá takto

- vlastní prefix tabulek
- unikátní uživatelské jméno (určitě ne admin, nebo administrator)
- kvalitní heslo o minimálně osmi znacích

Ochraňte přístup do administrace pomocí změny URL

WordPress má pro přístup do administrace dvě možné cesty. Jedna je **domena.tld/wp-admin** a druhá je **domena.tld/login.php**. Útočník, který bude chtít napadnout Váš web pomocí brute force útoku jako první použije jednu z těchto dvou adres. Proto, pokud budete řešit, jak zabezpečit WordPress a jeho administraci, je dobré toto ošetřit a URL změnit. Ke změně URL adresy můžete použít plugin WPS Hide Login. Je velmi jednoduchý a po jeho aktivaci Vám do nastavení WordPressu a do karty obecné přidá položku, kde můžete definovat vlastní url adresu administrace. Zároveň můžete nastavit druhou adresu, kam bude přesměrovaný uživatel, který se pokusí dostat do administrace klasickou cestou. To může být např. stránka 404 nebo jakákoliv jiná informativní stránka.

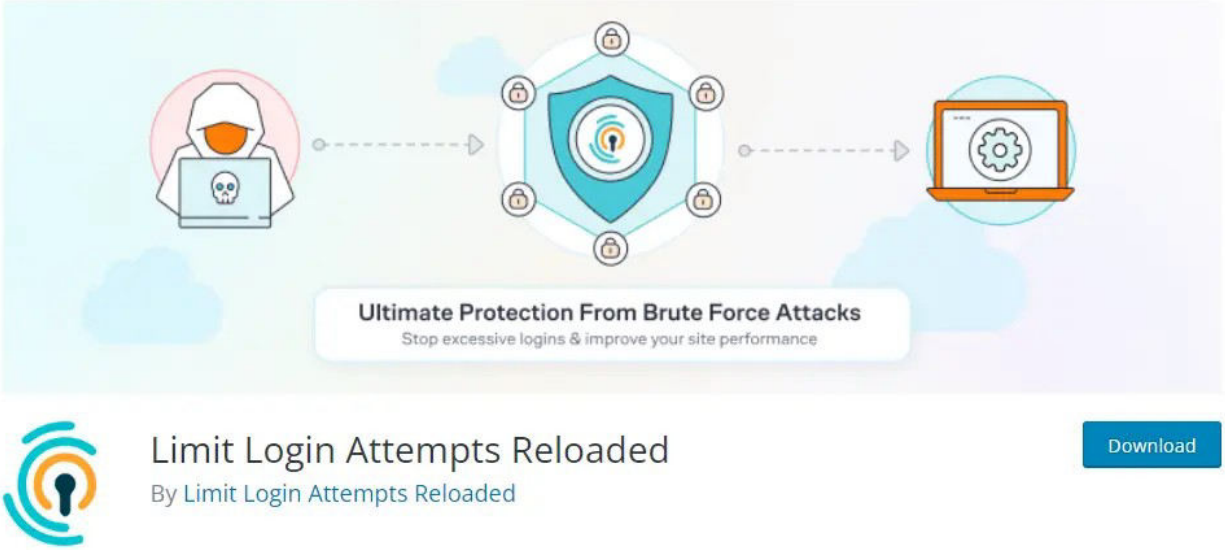


Opět, z pohledu toho, jak zabezpečit WordPress a administraci, znesnadníte potenciálnímu útočníkovi práci. Nebude vědět, jaká je adresa Vaší administrace, na které by mohl zkusit provést brute force útok a hádat hesla k přístupu.

Nastavte limit pokusů o přihlášení do administrace

Metoda, která ztíží možnost odhalit Vaše heslo také spočívá v omezení počtu pokusů o přihlášení. Toho opět můžete dosáhnout velmi pohodlně pomocí pluginu Limit Login Attempts Reloaded. Ten Vám mimo jiné dovolí nastavit následující:

- Omezení přihlášení – Omezíte počet pokusů pro přihlašování (pro každou IP adresu).
- Nastavitelná doba uzamčení – Upravíte dobu, po kterou musí uživatel nebo IP adresa čekat po uzamčení.
- Zbývající pokusy
- Informuje uživatele o zbývajících pokusech, nebo době uzamčení na přihlašovací stránce.
- Oznámení emailem o uzamčení
- Informuje správce emailem o uzamčení.
- Záznamy neúspěšných pokusů
- Zobrazíte si záznamy všech odmítnutých pokusů a uzamčení.
- Whitelist/Blacklist IP adres a uživatelských jmen – Kontrola přístupu k uživatelským jménům a IP adresám.
- Zabezpečení brány XML-RPC.
- Zabezpečení přihlašovací stránky Woocommerce.



Jak vidíte, pomocí tohoto pluginu dokážete nastavit opravdu hodně. Pokud by Vám nevyhovoval, jsou v repozitáři WordPressu k dispozici i další pluginy, které mají podobné funkce. Důležité je, zablokovat uživatele, který bude vytvářet nesmyslný počet požadavků pro přihlášení hned zkraje. Díky tomu nedáte útočníkovi šanci prolomit Vaše heslo, protože mnohem dříve jej plugin zablokuje.

Dvou faktorové ověření přístupu do administrace

Otázka, jak zabezpečit WordPress se minimálně hned zkraje opravdu hodně točí okolo administračního rozhraní. Proto, pokud chcete, můžete na web nasadit druhou vrstvu ochrany pro případ, že by někdo prolomil všechny prvky zabezpečení, které jsem popsal výše. Tou další vrstvou je dvou faktorové ověření. Dvou faktorové ověření přidává další vrstvu do procesu přihlášení se a eliminuje riziko, že by se do systému mohl dostat člověk, který z nějakého důvodu bude znát Vaše přihlašovací údaje.

Tato metoda přidá na přihlašovací obrazovku další pole, kam musíte zadat i kód, který si vygenerujete pomocí aplikace ve Vašem mobilním telefonu. To jistě znáte např. při ověřování plateb ve své bance, kde platbu musíte schválit ještě nějakou dodatečnou metodou ověření. Zde je to stejné. Napojíte si administraci WordPressu na aplikaci Google Authenticator, která Vám bude generovat přístupové kódy. Pokud by někdo z nějakého důvodu odhalil Váš login i heslo, pak se bez Vašeho mobilního telefonu do administrace stejně nedostane. Bude mu totiž chybět ten druhý faktor ověření. Kód z Vašeho mobilního zařízení.

Pokud byste chtěli zabezpečení WordPressu povýšit na další úroveň i pomocí tohoto, dvou faktorového ověření, napsal jsem na to samostatný článek, kde najdete podrobný návod jak na instalaci, tak na aktivaci této druhé vrstvy bezpečnosti: Jak nastavit dvoufaktorové ověření administrace WordPressu.

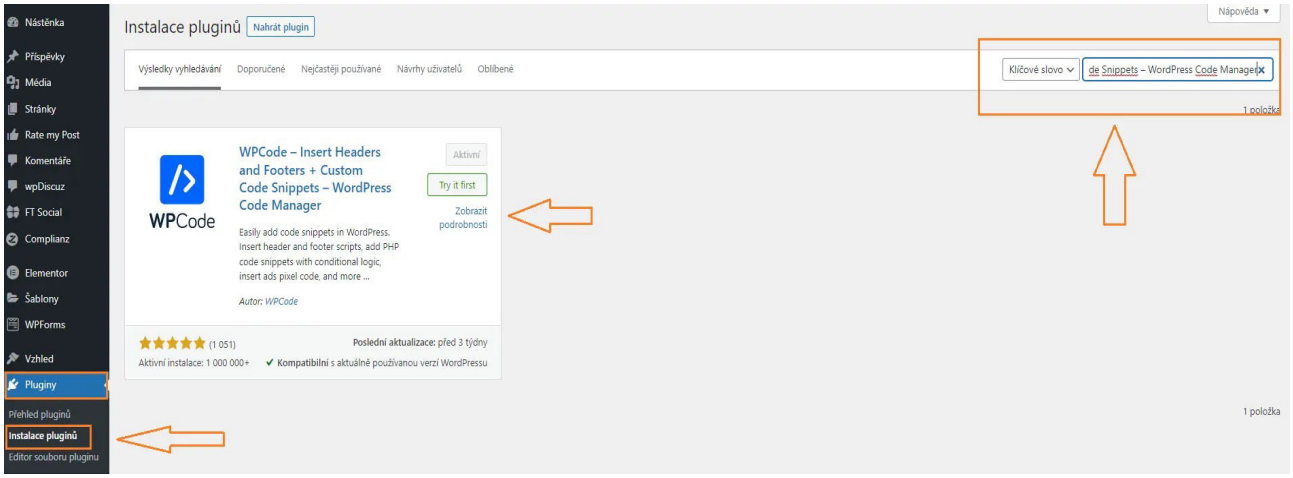
Zakažte XML-RPC

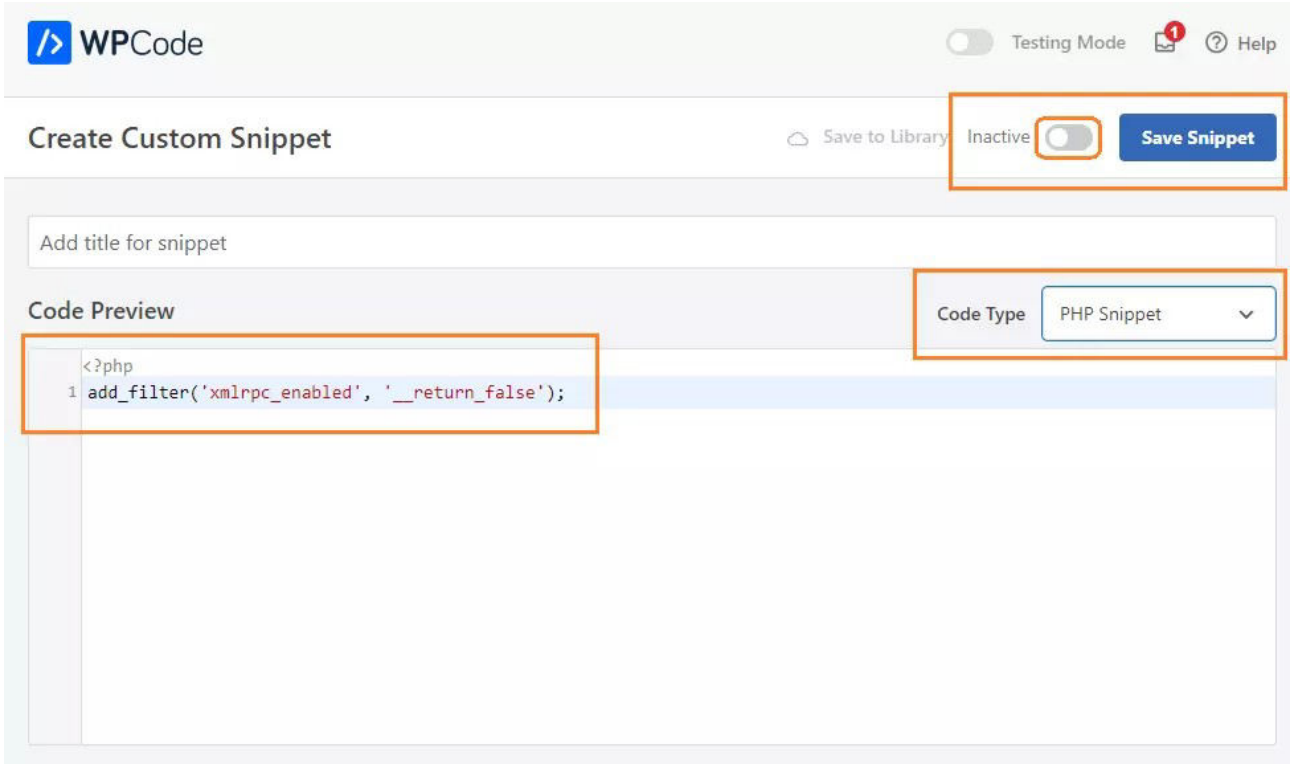
XML-RPC je jedno ze základních API WordPressu, které je povolené v defaultním stavu již od verze 3.5. Ta vyšla v roce 2012. Od té doby má tedy každá nová instalace WordPressu XML-RPC automaticky aktivní. Tato funkcionalita WordPressu umožňuje velmi zjednodušeně řečeno připojení k Vašemu webu a interakci s ním. Např. pomocí mobilní aplikace pro správu WordPressu, nebo pomocí různých automatizačních služeb. Pokud XML-RPC na webu nevyužíváte, je z pohledu zabezpečení WordPressu lepší jej na webu vypnout.

Vypnutí XML-RPC je opravdu velmi jednoduché a provádí se pomocí tohoto krátkého snippetu:

#Jak zabezpečit WordPress - vypnutí XML-RPC
add_filter('xmlrpc_enabled', '__return_false');

Pokud nevíte přesně, jak tento snippet do svého webu vložit, napsal jsem pro tento účel samostatný, relativně krátký článek, kde se naučíte používat plugin WPCode. Určitě se tedy podívejte sem: Jak jednoduše zakázat XML-RPC ve WordPressu.





Automatické odhlašování uživatelů

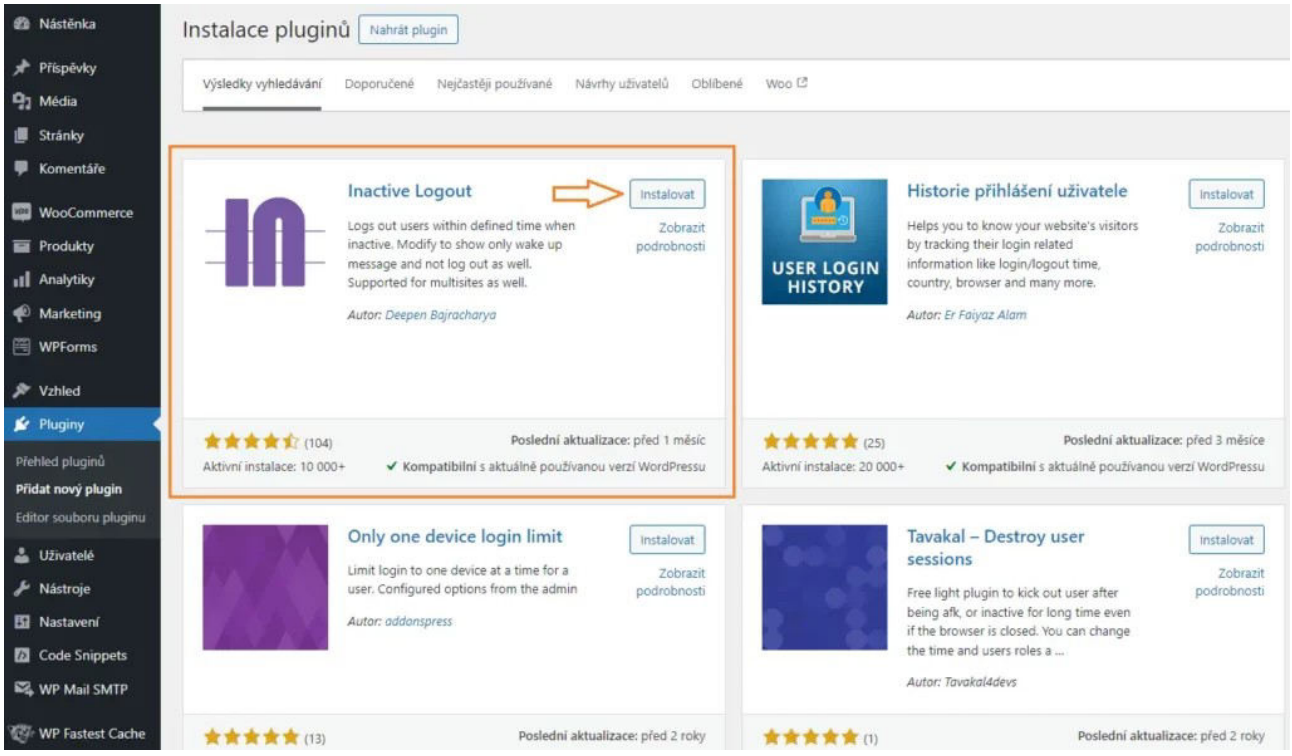
Jak zabezpečit WordPress je dost často také otázkou malých detailů, které mohou být pro někoho sice bezvýznamné, nicméně v celkovém ohledu poté dělají web stabilní a opravdu bezpečný. Jedním z takových detailů může být právě i automatické odhlašování z administrace. To je důležité hlavně v momentě, kdy je web multiuživatelský. Tedy kromě jednoho administrátora na webu pracuje i více uživatelů v různých rolích.

Patrně si dokážete představit situaci, kdy uživatel odejde od svého notebooku, na kterém zůstane přihlášený do administrace WordPressu. Takový notebook, nebo stolní počítač s otevřeným přístupem k citlivým údajům může napáchat velké množství problémů. WordPress nativně automatické odhlášení uživatelů neřeší. Proto mu s tím trochu pomůžeme.

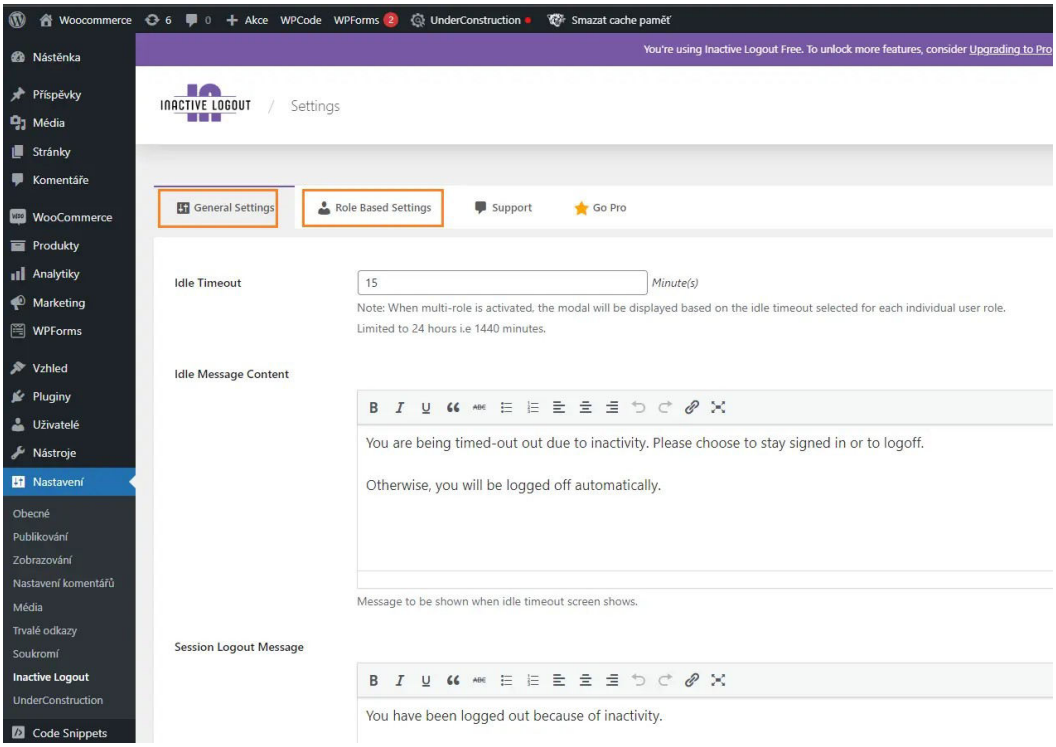
Vše, co k tomu budete potřebovat je plugin Inactive Logout, který se nachází v oficiálním repozitáři WordPressu.

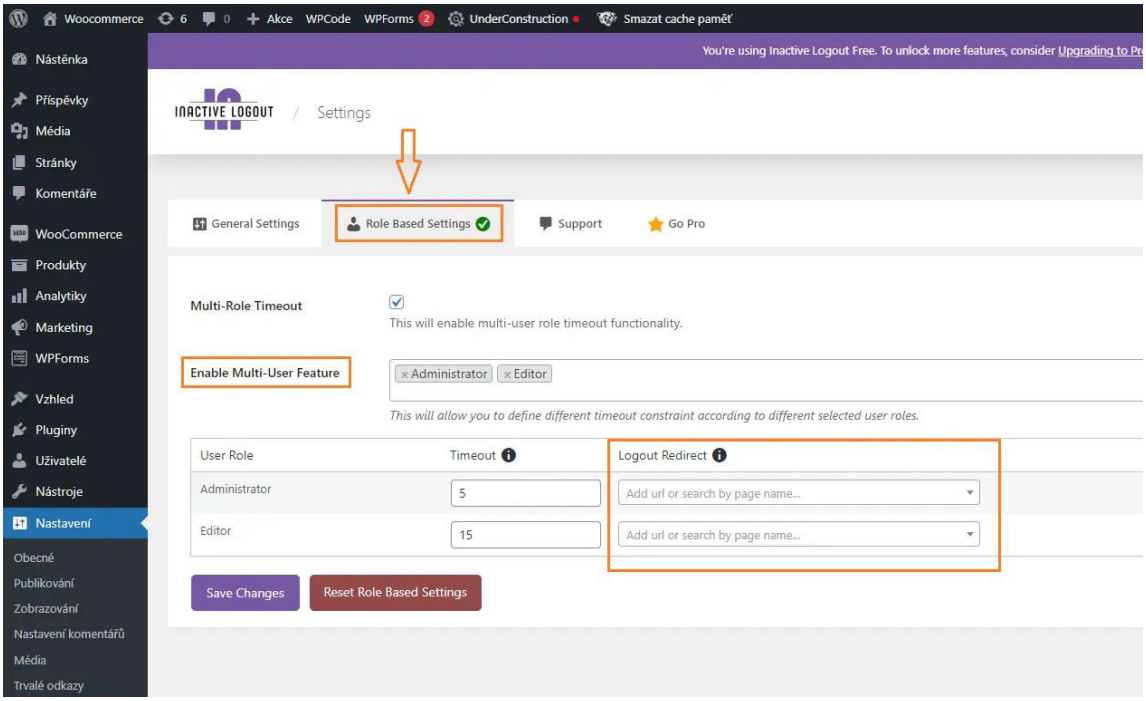
Instalaci pluginu provedete takto:

- V levém menu WordPressu si klikněte na tlačítko „Pluginy“.
- V novém menu klikněte na položku „Přidat nový plugin“.
- Nyní, v pravém horním rohu napište do vyhledávacího pole klíčovou frázi „Inactive Logout“.
- WordPress plugin vyhledá.
- Plugin nainstalujte a poté aktivujte.



Jakmile plugin aktivujete, přejděte do jeho nastavení. Tento plugin má nastavení schované v menu pod položkou Nastavení -> Inactive Logout. Tento plugin nabízí několik možností zabezpečení WordPressu. První možností je nastavit časový limit pro všechny stejný (doporučeno), druhá možnost zabezpečení je podle uživatelských rolí. To znamená, že administrátorovi můžete nastavit nižší čas než například kolegovi, který má roli přispěvatele. Zároveň vždy můžete nastavit vlastní upozornění uživatelům, kteří se blíží k limitu, nebo již byli odhlášeni. Pokud nastavujete odhlášení na základě uživatelských rolí, můžete nastavit redirect na stránku, na kterou mají být daní uživatelé odhlášení.





Správce hesel – bezpečnější uložení citlivých dat

Nyní se tak trochu od zabezpečení WordPressu odkloníme k bezpečnosti chování uživatele. Konkrétně k heslům a loginům. To se týká obecné práce s citlivými daty. Běžná praxe mnoha lidí je taková, že si ukládají hesla a loginy do prohlížeče. Z důvodu pohodlnosti. Prohlížeč vyplňuje login i heslo za ně. Je to rychlejší a pohodlné, ale velmi nebezpečné. Pak totiž nemá velký smysl vymýšlet dlouhá, složitá a těžko zapamatovatelná hesla, když se do systému přihlásí každý, kdo má přístup k Vašemu prohlížeči. Berte takové chování jako velmi nebezpečnou praxi obecně.

Pro zabezpečení WordPressu jako takového, ale i pro zabezpečení svého celkového portfolia účtů na internetu uděláte to nejlepší v momentě, kdy od této praxe upustíte a začnete používat správce hesel. Je to stejně pohodlné a stejně rychlé, avšak diametrálně bezpečnější. Všechna hesla a loginy máte schované ve správci hesel, který je navíc krytý další vrstvou zabezpečení.

Jak to vlastně funguje? Do počítače si nainstalujete program pro správu hesel a do prohlížeče poté jeho doplněk. Doplněk v prohlížeči zařídí, že bude hesla nadále vyplňovat za Vás. Podmínkou ale je, že musíte nejprve spustit program pro správu hesel a do něj se přihlásit. A jakou že obrovskou výhodu to vlastně má? Pamatujete si pouze jedno jediné heslo a to do svého správce hesel. Zbytek si pamatuje tento program. Můžete tak zcela bez problémů do všech svých online aplikací vkládat opravdu velmi složitá hesla a díky a správci hesel je nikdy nezapomenete.

Mezi nejlepší a mnou prověřené správce hesel řadím KeePassXC. Stáhnout jej můžete zde: KeePassXC.

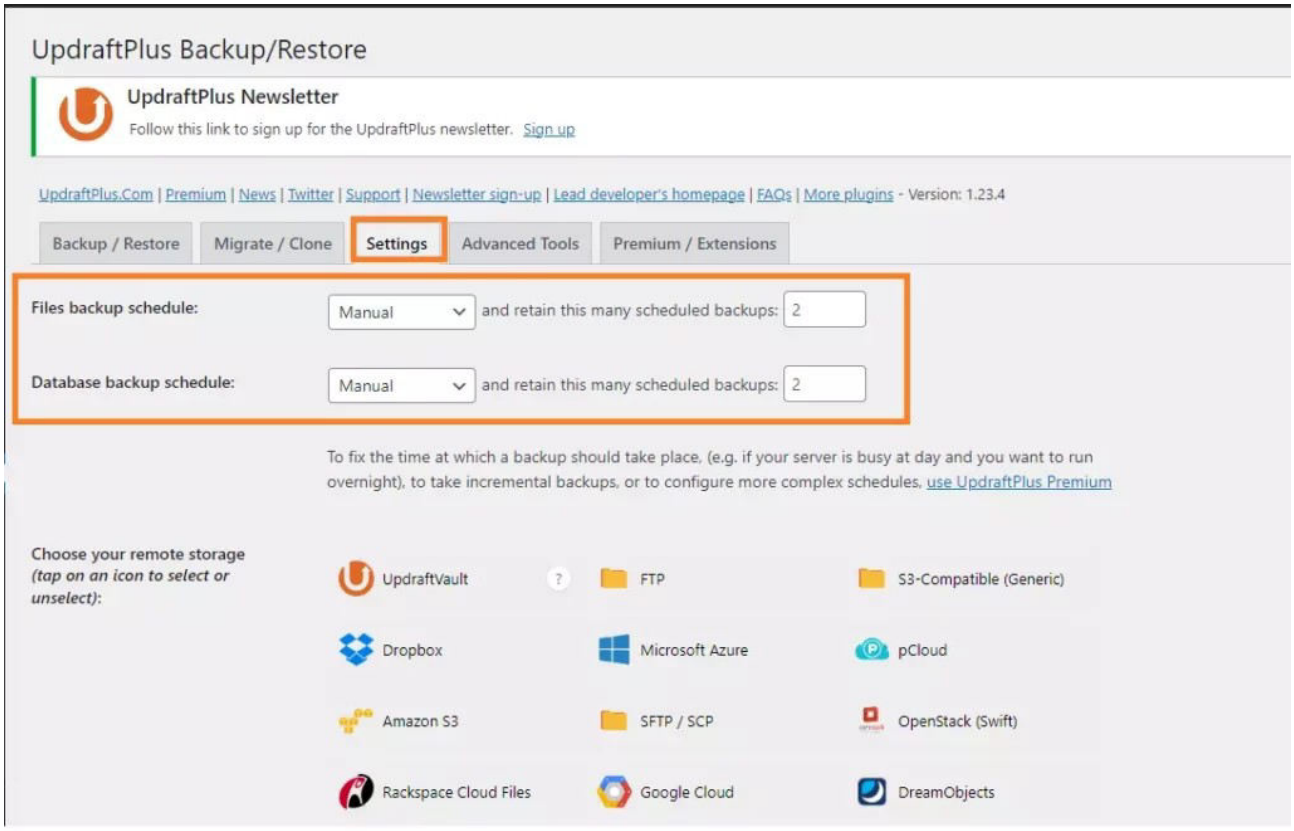
Jak zabezpečit WordPress pomocí automatické zálohy dat

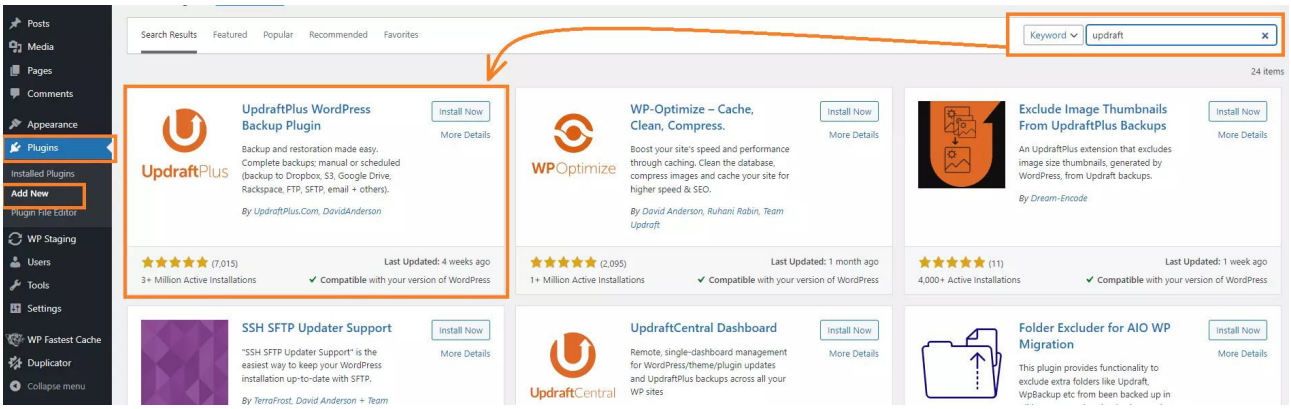
Zálohování dat je věčné téma, které opravdu ale málokdo dodržuje. Bezpečí Vašeho webu začíná tam, kde máte jistotu, že jsou Vaše data v pořádku. To znamená, že nejlepší situace nastává v momentě, kdy máte data čistého webu zálohovaná na nějakém místě, ke kterému se útočník jen tak nedostane. Mohou to být šifrovaná cloudová úložiště jako OneDrive nebo Google Disk, nebo to může být Váš soukromý SSD disk uložený off-line doma, v šuplíku pracovního stolu.

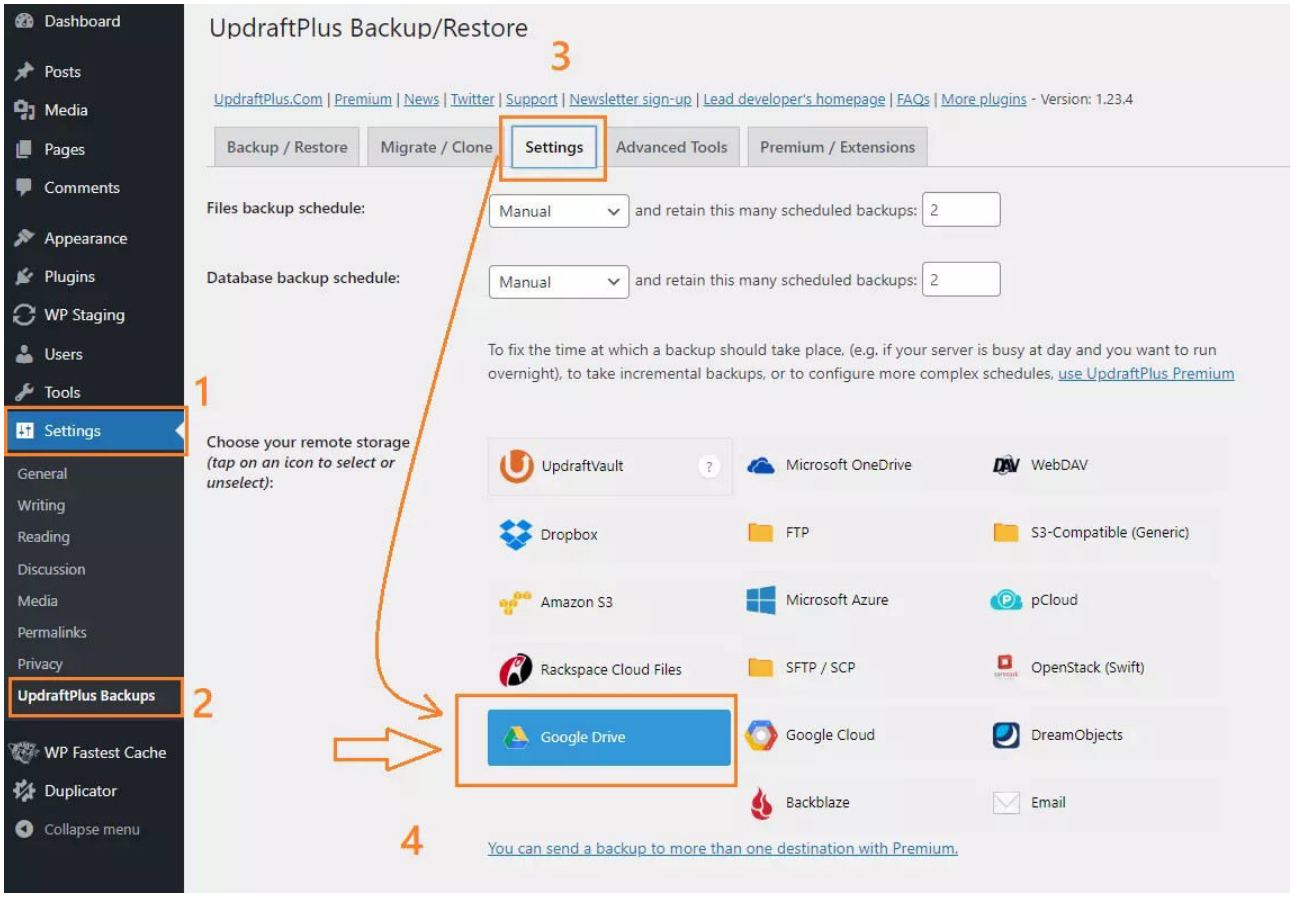
Co se týče zabezpečení WordPressu, nejlepší metoda zálohování je taková, která se děje sama, automaticky. K tomuto účelu existuje mnoho pluginů a mezi ty nejlepší pak mohu doporučit Updraft. V něm můžete nastavit zálohování periodicky a také

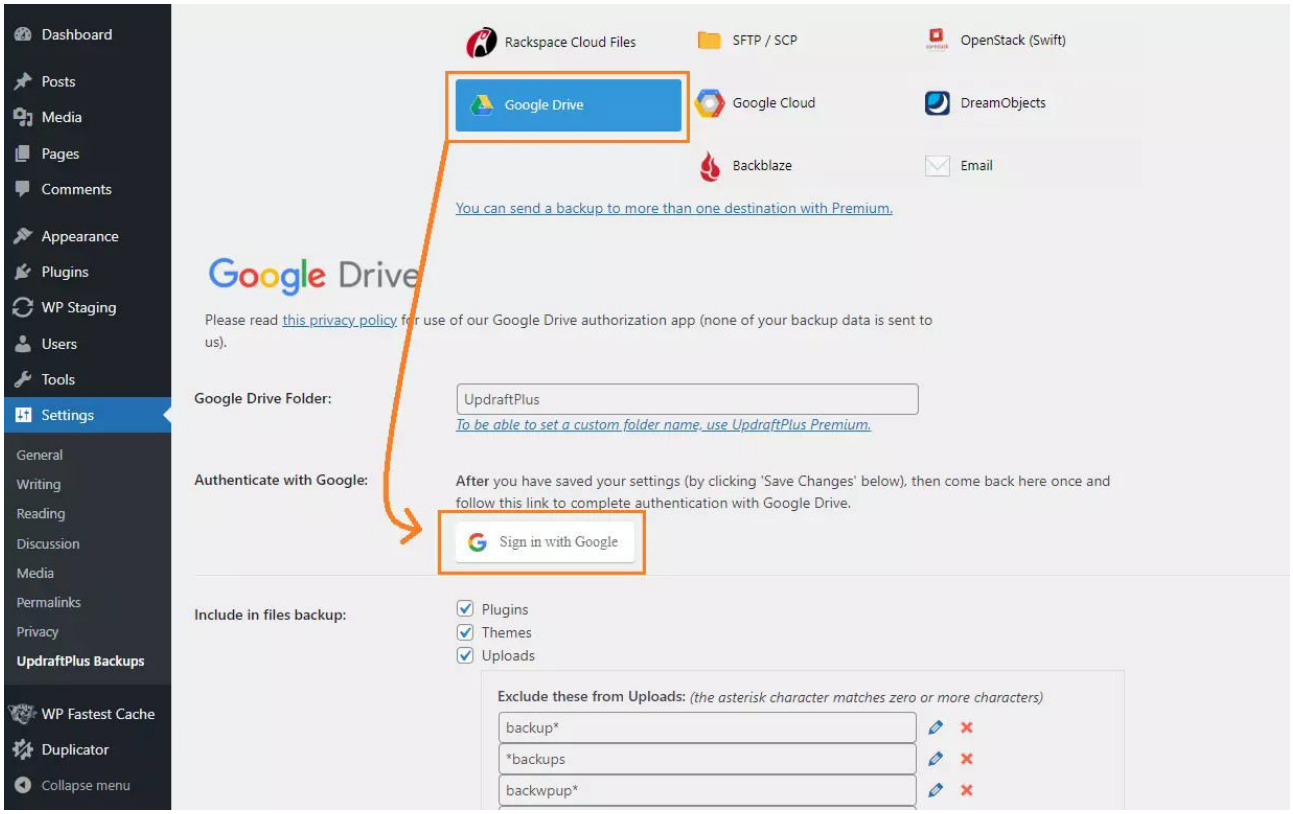
můžete vzniklé zálohy odesílat rovnou na vzdálené cloudové disky. Nikdy neukládejte zálohu webu na FTP. Za prvé to časem začne vadit poskytovateli webhostingu, kterému zaplníte kvótu, za druhé, ukládat zálohu na stejné místo, kde se nachází web je hloupost. Zálohy musí být od webu oddělené jak geolokačně, tak i serverově. To znamená že záloha musí být na jiném místě, stroji a nejlépe i datacentru.

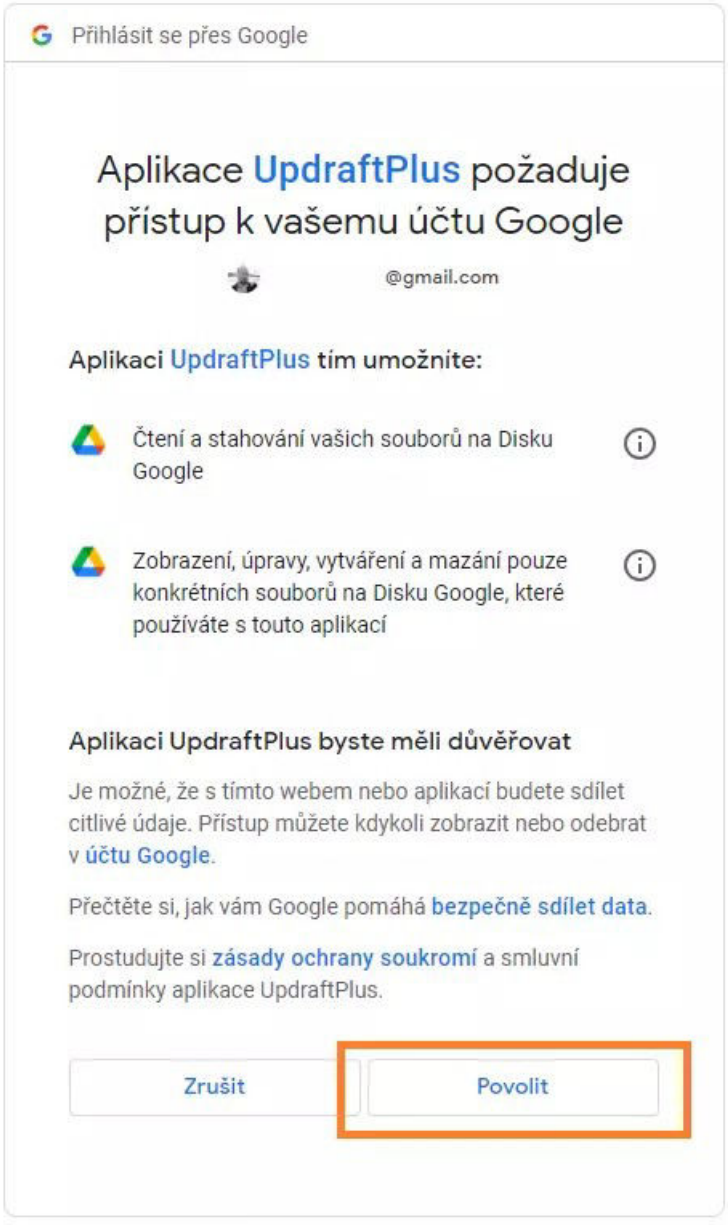
Pokud Vás zajímá, jak můžete plugin Updraft aktivovat a nastavit cyklické zálohy na Google disk, napsal jsem na toto téma samostatný článek: Chraňte svá data a zálohujte si WordPress. Věřte, že pro zabezpečení WordPressu jsou zálohu klíčovým prvkem a rozhodně je nepodceňujte. Nespoléhejte se nikdy na zálohy svého poskytovatele. Jsou obvykle maximálně 14 dní staré a to, že je Váš web napadený můžete zjistit klidně i po měsíci. Záloha od Vašeho poskytovatele webhostingu Vám pak bude k ničemu.

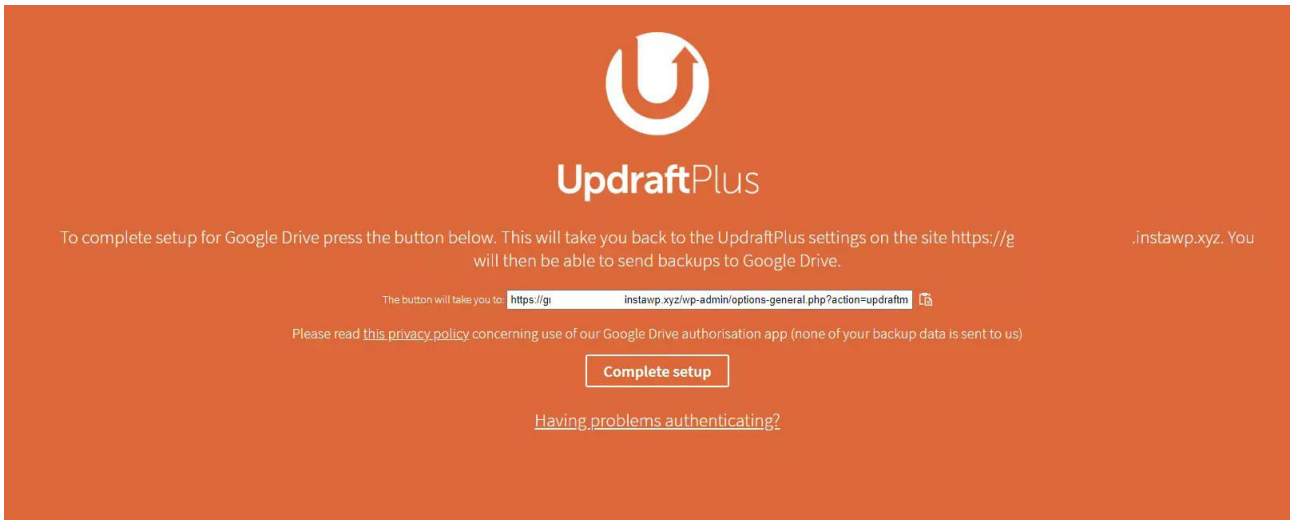


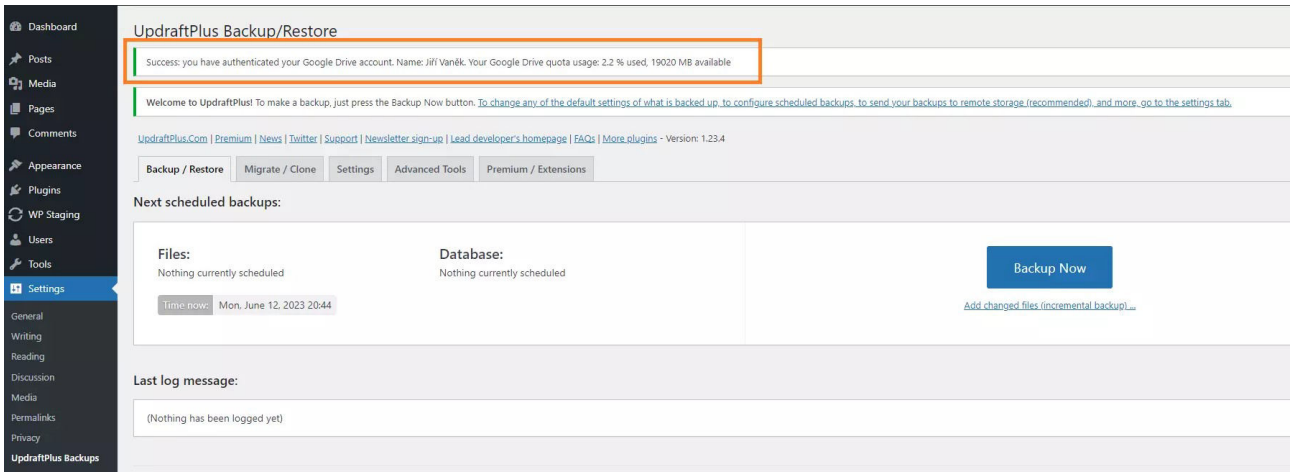

Posts
Media
Pages
Comments
Appearance
Plugins
Installed Plugins
Add New
Plugin File Editor
WP Staging
Users
Tools
Settings
WP Fastest Cache
Duplicator
Collapse menu
Search Results
Featured
Popular
Recommended
Favorites
Keyword
updraft
24 items
UpdraftPlus WordPress Backup Plugin
Install Now
More Details
Backup and restoration made easy. Complete backups; manual or scheduled (backup to Dropbox, S3, Google Drive, Rackspace, FTP, SFTP, email + others).
By UpdraftPlus.Com, DavidAnderson
(7,015)
3+ Million Active Installations
Last Updated: 4 weeks ago
Compatible with your version of WordPress
WP-Optimize – Cache, Clean, Compress.
Boost your site's speed and performance through caching. Clean the database, compress images and cache your site for higher speed & SEO.
By David Anderson, Ruhani Rabin, Team Updraft
(2,095)
1+ Million Active Installations
Last Updated: 1 month ago
Compatible with your version of WordPress
Exclude Image Thumbnails From UpdraftPlus Backups
An UpdraftPlus extension that excludes image size thumbnails, generated by WordPress, from Updraft backups.
By Dream-Encode
(11)
4,000+ Active Installations
Last Updated: 1 week ago
Compatible with your version of WordPress
SSH SFTP Updater Support
"SSH SFTP Updater Support" is the easiest way to keep your WordPress installation up-to-date with SFTP.
By TerraFrost, David Anderson + Team
UpdraftCentral Dashboard
Remote, single-dashboard management for WordPress/theme/plugin updates and UpdraftPlus backups across all your WP sites
Folder Excluder for AIO WP Migration
This plugin provides functionality to exclude extra folders like Updraft, WpBackup etc from been backed up in

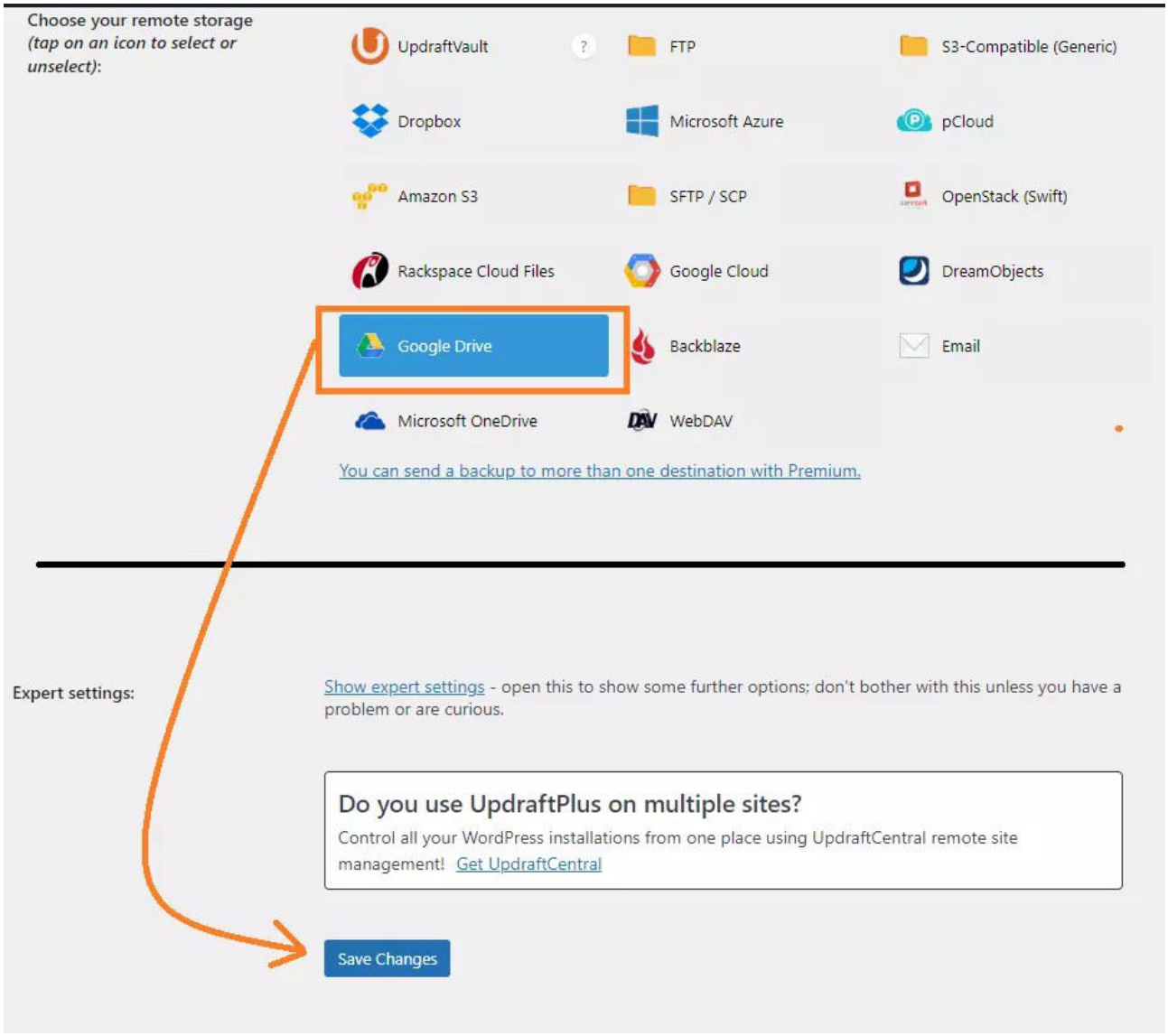

Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
WP Staging
Users
Tools
Settings
General
Writing
Reading
Discussion
Media
Permalinks
Privacy
UpdraftPlus Backups
WP Fastest Cache
Duplicator
Collapse menu
1
2
3
4
UpdraftPlus Backup/Restore
UpdraftPlus.Com | Premium | News | Twitter | Support | Newsletter sign-up | Lead developer's homepage | FAQs | More plugins - Version: 1.23.4
Backup / Restore
Migrate / Clone
Settings
Advanced Tools
Premium / Extensions
Files backup schedule:
Manual
and retain this many scheduled backups:
2
Database backup schedule:
Manual
and retain this many scheduled backups:
2
To fix the time at which a backup should take place, (e.g. if your server is busy at day and you want to run overnight), to take incremental backups, or to configure more complex schedules, use UpdraftPlus Premium
Choose your remote storage (tap on an icon to select or unselect):
UpdraftVault
Microsoft OneDrive
WebDAV
Dropbox
FTP
S3-Compatible (Generic)
Amazon S3
Microsoft Azure
pCloud
Rackspace Cloud Files
SFTP / SCP
OpenStack (Swift)
Google Drive
Google Cloud
DreamObjects
Backblaze
Email
You can send a backup to more than one destination with Premium.


Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
WP Staging
Users
Tools
Settings
General
Writing
Reading
Discussion
Media
Permalinks
Privacy
UpdraftPlus Backups
WP Fastest Cache
Duplicator
Collapse menu
Rackspace Cloud Files
SFTP / SCP
OpenStack (Swift)
Google Drive
Google Cloud
DreamObjects
Backblaze
Email
You can send a backup to more than one destination with Premium.
Google Drive
Please read this privacy policy for use of our Google Drive authorization app (none of your backup data is sent to us).
Google Drive Folder:
UpdraftPlus
To be able to set a custom folder name, use UpdraftPlus Premium.
Authenticate with Google:
After you have saved your settings (by clicking 'Save Changes' below), then come back here once and follow this link to complete authentication with Google Drive.
Sign in with Google
Include in files backup:
Plugins
Themes
Uploads
Exclude these from Uploads: (the asterisk character matches zero or more characters)
backup*
*backups
backwpup*


Přihlásit se přes Google
Aplikace UpdraftPlus požaduje přístup k vašemu účtu Google
@gmail.com
Aplikaci UpdraftPlus tím umožnite:
Čtení a stahování vašich souborů na Disku Google
Zobrazení, úpravy, vytváření a mazání pouze konkrétních souborů na Disku Google, které používáte s touto aplikací
Aplikaci UpdraftPlus byste měli důvěřovat
Je možné, že s tímto webem nebo aplikací budete sdílet citlivé údaje. Přístup můžete kdykoli zobrazit nebo odebrat v účtu Google.
Přečtěte si, jak vám Google pomáhá bezpečně sdílet data.
Prostudujte si zásady ochrany soukromí a smluvní podmínky aplikace UpdraftPlus.
Zrušit
Povolit


UpdraftPlus
To complete setup for Google Drive press the button below. This will take you back to the UpdraftPlus settings on the site https://g .instawp.xyz. You will then be able to send backups to Google Drive.
The button will take you to: https://g instawp.xyz/wp-admin/options-general.php?action=updraftm
Please read this privacy policy concerning use of our Google Drive authorisation app (none of your backup data is sent to us)
Complete setup
Having problems authenticating?


Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
WP Staging
Users
Tools
Settings
General
Writing
Reading
Discussion
Media
Permalinks
Privacy
UpdraftPlus Backups
UpdraftPlus Backup/Restore
Success: you have authenticated your Google Drive account. Name: Jiří Vaněk. Your Google Drive quota usage: 2.2 % used, 19020 MB available
Welcome to UpdraftPlus! To make a backup, just press the Backup Now button. To change any of the default settings of what is backed up, to configure scheduled backups, to send your backups to remote storage (recommended), and more, go to the settings tab.
UpdraftPlus.Com | Premium | News | Twitter | Support | Newsletter sign-up | Lead developer's homepage | FAQs | More plugins - Version: 1.23.4
Backup / Restore
Migrate / Clone
Settings
Advanced Tools
Premium / Extensions
Next scheduled backups:
Files:
Nothing currently scheduled
Database:
Nothing currently scheduled
Time now: Mon, June 12, 2023 20:44
Backup Now
Add changed files (incremental backup) ...
Last log message:
(Nothing has been logged yet)


Choose your remote storage
(tap on an icon to select or unselect):
UpdraftVault
FTP
S3-Compatible (Generic)
Dropbox
Microsoft Azure
pCloud
Amazon S3
SFTP / SCP
OpenStack (Swift)
Rackspace Cloud Files
Google Cloud
DreamObjects
Google Drive
Backblaze
Email
Microsoft OneDrive
WebDAV
You can send a backup to more than one destination with Premium.
Expert settings:
Show expert settings - open this to show some further options; don't bother with this unless you have a problem or are curious.
Do you use UpdraftPlus on multiple sites?
Control all your WordPress installations from one place using UpdraftCentral remote site management! Get UpdraftCentral
Save Changes

DNS a ochrana proti DDOS útoku

Nyní si pojďme něco říct o DDOS útoku. Je to útok, kdy někdo použije velké množství počítačů v síti tím způsobem, že vyšle na Váš web či server obrovský počet požadavků. To způsobí, že web i server bude přetížený a služba bude nedostupná. Jak se tomu bránit? Mnohdy mají vlastní řešení již samotní poskytovatelé webhostingu, ale nelze se na něj spoléhat. Pokud situaci nezvládnou, může se stát, že Váš webhosting pro přetěžování serveru vypnou. To je kritické v momentě, kdy Vám webhosting vydělává peníze (např. e-shop).

Proto vždy a každému doporučuji přenést DNS servery domény na společnost CloudFlare a používat jejich služby. Placené, ale i ty zdarma. CloudFlare má již v tarifu zdarma docela dobře propracovanou obranu proti DDOS útoku. A jak to vlastně celé funguje?

CloudFlare skryje Vaší cílovou IP adresu web serveru za proxy server. To znamená, že pokud někdo bude chtít zjistit IP adresu stroje, na kterém běží Váš webhosting, dostane jako odpověď IP adresu proxy serveru CloudFlare. DDOS útok tedy bude mířit na tuto IP adresu, namísto Vašeho serveru. A s takovým útokem si již CloudFlare velmi dobře poradí a vyfiltruje ho. Na Váš server, nebo na server Vašeho poskytovatele webhostingu se útok vůbec nedostane.

Pokud Vás zajímá, jak velkým DDOS útokům dokáže CloudFlare čelit, podívejte se na tento článek: Největší kybernetický útok v historii. Hackeři napadli Amazon, Cloudflare i Google.

Podobnou službu nabízí aktuálně i česká společnost WEDOS. Jmenuje se WEDOS Global Protection a je to placená služba. Nemám s ní bohužel aktuálně žádné zkušenosti, protože po celou dobu používám služby společnosti CloudFlare. Je dobré ji zde ale zmínit jako alternativu.

Chraňte svá data proti krádeži

Otázka ochrany duševního vlastnictví je dnes poměrně zásadní. A proto, pokud máte vlastní web nebo blog, měla by pro Vás být ochrana Vašeho vlastnictví prioritní. Co se týče webové prezentace, je zcela běžné, že ze strany ostatních subjektů dochází ke kopírování textu či vizuálního obsahu. Proto je vhodné, chcete-li, zavést určité metody k zabezpečení obsahu Vašeho webu proti krádeži. Ruku na srdce, kdo bude obsah na webu chtít ukrást, cestu si najde, nicméně, proč to zlodějům obsahu dělat jednoduché.

Jsou dvě věci, které byste měli na svém webu chránit. Jsou to texty a obrázky.

Co se týče ochrany textu na webu, psal jsem na toto téma podrobný článek zde: Jak zabránit kopírování textu z WordPress webu.

Co se týče obrázků, je potřeba zakázat tzv. hotlinking. To znamená, že obrázek se z webu fyzicky neukradne, ale cizí weby na něj odkazují a zobrazují jej z Vašeho umístění. Zjednodušeně řečeno, zadají do svého kódu URL adresu Vašeho obrázku a ten zobrazují přímo z Vašeho webu, potažmo serveru. Nejenom že Vám tím kradou Váš autorský obsah, ale také zatěžují výkon Vašeho webu, či serveru. Hotlinking na obrázky zakážete tak, že do svého .htaccess souboru na FTP vložíte následující kód:

```
#jak zabezpečit WordPress proti hotlinkingu obrázků
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?vase-domena.koncovka [NC]
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?google.com [NC]
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?bing.com [NC]
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?yandex.com [NC]
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?seznam.cz [NC]
RewriteRule \.(jpg|jpeg|png|gif|webp)$ – [NC,F,L]
```

V pravidlech nahraďte položku vase-domena.koncovka za jméno Vaší domény. Tento kód zakazuje odkazovat na obrázky Vašeho webu všem, kromě Vaší domény a vyhledávačů Google, Bing, Yandex a Seznam. Díky tomu nezakážete vyhledávačům odkazovat na Vaše obrázky. Zloději ale budou mít smůlu.

Jak zabezpečit WordPress proti spamu

Pokud máte web na WordPressu, pravděpodobně budete také používat formuláře. Těch může být několik typů. Může jít formulář pro komentáře pod příspěvkem, kontaktní formulář, nebo nebo také formulář pro přihlášení do systému. A všechny tyto formuláře je potřeba zabezpečit proti spamovým robotům. Existuje mnoho řešení, jak se vyhnout spamovým robotům. Osobně používám řešení, které zahrnuje v jednom pluginu ochranu všech těchto formulářů najednou. Jedná se o plugin WP Armour – Honeypot Anti Spam. Používám tento plugin již více jak dva roky na všech webech, které jsem vytvořil a zatím jsem nezaznamenal u jediného z webů ani jeden spam.

Mohu tak plugin oprávněně považovat za velmi kvalitní. Navíc, ocení ho i začátečníci protože se nijak nenastavuje. Tento plugin se pouze nainstaluje do systému a aktivuje. Instalaci pluginu provedete takto:

- V levém menu WordPressu si klikněte na tlačítko „Pluginy“.
- V novém menu klikněte na položku „Přidat nový plugin“.
- Nyní, v pravém horním rohu napište do vyhledávacího pole klíčovou frázi „honeypot“ nebo „WP Armour“.
- WordPress plugin vyhledá.
- Plugin nainstalujte a poté aktivujte.

Tento plugin Vám zabezpečí proti spamovým robotům konkrétně:

- Komentáře WordPressu
- Registrační formulář WordPressu
- Fórum BBPress (bbpress.org)
- plugin Contact Form 7 (wordpress.org/plugins/contact-form-7)
- plugin Gravity Forms
- nejlepší plugin pro komentáře WPForms (wpforms.com)
- Formidable Forms (formidableforms.com)
- Caldera Forms (calderaforms.com)
- Formuláře nástroje Toolset (toolset.com)
- Formuláře Elementoru (elementor.com)
- Fluent Forms (fluentforms.com)
- Kontaktní formulář tématu Divi (elegantthemes.com)
- Theme My Login (https://wordpress.org/plugins/theme-my-login/)
- WooCommerce Reviews Pro

Jako velkou výhodu také vnímám to, že je WP Armour plně GDPR kompatibilní. Neobsahuje žádné sledování, ukládání cookie nebo volání externího serveru. Pokud tedy chcete zabezpečit WordPress proti nechtěnému spamu, doporučuji jako první volbu tento plugin. Udělá více práce a je mnohem efektivnější jak Google reCAPTCHA.

Aktualizujte – zabezpečení WordPressu to výrazně posílí

WordPress je modulární systém. Vy jej dostanete v nějakém základním stavu a pomocí modulů, u WordPressu nazývaných pluginy, si systém dále rozšiřujete o funkce, které v systému nativně nejsou. To samé se obvykle děje u šablony vzhledu. Pokud nechcete defaultní sadu šablon, obvykle sáhnete po nějaké externí z oficiálního, či neoficiálního repozitáře WordPressu a tu na web nainstalujete.

Pro všechny tyto doplňky WordPressu se vydávají aktualizace. A nejen pro ně. I samotný WordPress čas od času vydá balíček pro aktualizaci. Buď jako minoritní update při malých změnách (**6.3.1 -> 6.3.2**), nebo jako majoritní update, když se mění celá verze (**6.3 -> 6.4** apod.). Aktualizovat tedy můžete:

- Jádro WordPressu
- Pluginy
- Šablony

Aktualizace se vydávají z prostého důvodu. Buď přináší do systému nebo doplňku nové funkce, nebo opravují nalezené chyby. Pro nás je klíčový ten druhý důvod. Oprava chyb. Pokud se v pluginu, šabloně vzhledu nebo samotném jádru systému objeví bezpečnostní chyba, reaguje vývojář dané části opravou takové chyby. Systém Vás upozorní na novou aktualizaci dané části a Vy tím, že aktualizaci provedete také opravíte nalezenou chybu. Pokud aktualizace neprovádíte, vystavujete svůj web obrovskému riziku potenciálních problémů s napadením.

Proč jsou aktualizace důležité v kontextu toho, jak zabezpečit WordPress?

Pojďme se podívat, jak bych postupoval jako hacker já, pokud bych chtěl napadnout Váš web. Pomocí online nástrojů jako je např. https://builtwith.com bych si nejprve zjistil, na čem je Váš web postavený a jaké doplňky používá. Zjistil bych mimo jiné i pluginy, které na webu máte. U pluginů bych se poté podíval, jaké bezpečnostní chyby u nich byly objeveny a ty bych se pokusil zneužít. Pokud neaktualizujete, nechali byste mi otevřená vrátka k útoku. Pokud ale aktualizace provádíte, nalezené chyby už budete mít opravené aktualizací a já pravděpodobně půjdu hledat „štěstí“ jinam.

Co tedy z toho plyne? Že celý systém je pouze natolik pevný, jako je jeho nejslabší část. Aktualizace Vám pomáhají chránit Váš systém před nalezenými bezpečnostními problémy a zabezpečení WordPressu je celé primárně postaveno hlavně na tom, že aktualizace nebudete ignorovat.

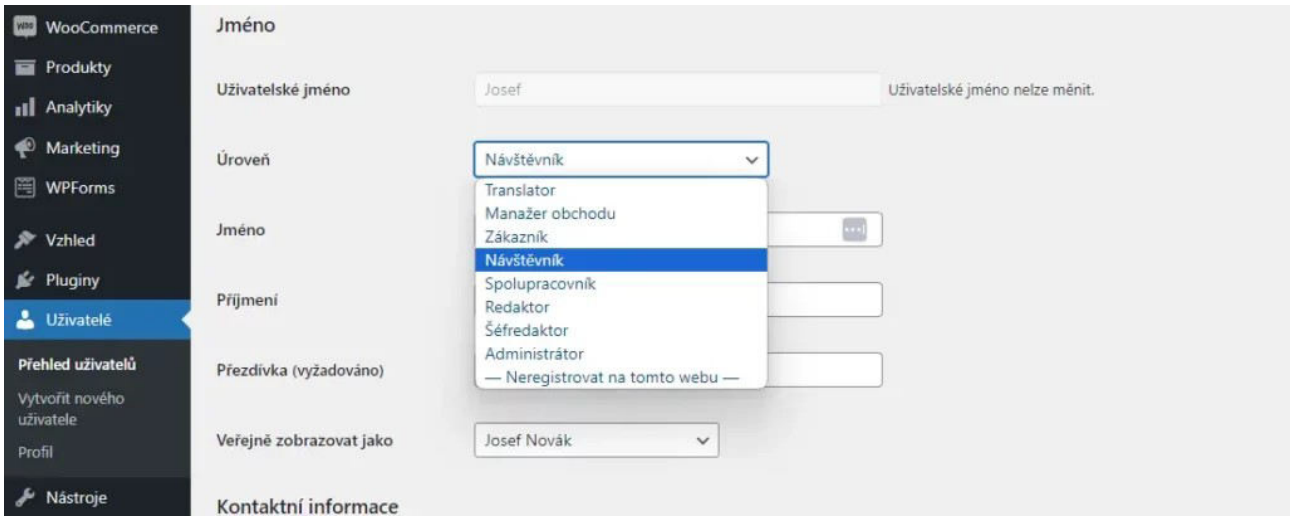
Máte více uživatelů? Zvažte rozdělení uživatelských rolí. Zabezpečení WordPressu to výrazně posílí.

Stejně tak, jako jsem před chvílí psal o tom, že je WordPress modulární systém, tak stejnou měrou je to i systém multiuživatelský. To znamená, že v něm může existovat mnoho uživatelů a ti by při správném řešení měli mít správně nastavené role. Každá role má v systému určitá práva. Nejvyšší role je administrátor webu se všemi právy, nejmenší role je pak návštěvník (ten nemá vůči systému skoro žádná práva). WordPress nativně rozlišuje tyto uživatelské role:

**Role	Správa uživatelů	Správa pluginů a šablon	Změna nastavení webu	Vytváření a úprava obsahu	Schvalování a publikování příspěvků	Správa kategorií a tagů
Administrátor	Ano	Ano	Ano	Ano	Ano	Ano
Šéfredaktor	Ne	Ne	Ne	Ano	Ano	Ano
Redaktor	Ne	Ne	Ne	Ano	Ne	Ne
Spolupracovník	Ne	Ne	Ne	Ano	Ne	Ne
Návštěvník	Ne	Ne	Ne	Ne	Ne	Ne
Předplatitel	Ne	Ne	Ne	Ne	Ne	Ne
Autor	Ne	Ne	Ne	Ano	Ne	Ne

Proto je nadmíru důležité, abyste posoudili všechny uživatele svého systému i to, co pro daný web vykonávají za činnost. Podle toho jim rozdělte uživatelské role. Z hlediska zabezpečení WordPressu praktikujte metodu nejnižšího oprávnění. To znamená, že uživateli vždy nastavte nejnižší možné oprávnění, které mu ale nebude bránit v jeho činnosti. Jakákoliv další oprávnění nad rámec jeho práce jsou zbytečná a potenciálně nebezpečná.

Pokud by Vás zajímaly uživatelské role a konkrétní oprávnění, která poté mohou uživatelé v systému vlastnit, podívete se na tento článek, kde tyto role popisuji detailněji: Uživatelé a uživatelská oprávnění ve WordPressu.



Bezpečnostní pluginy (jak zabezpečit WordPress pomocí Sucuri nebo WordFence)

Jako poslední záležitost na téma jak zabezpečit WordPress jsem nechal pluginy. Proč jsou až na posledním místě? Protože mnoho lidí, aniž by provedlo základní zabezpečení WordPressu popsané výše, spoléhá na to, že jim web ochrání plugin. Bohužel, tak tomu ale rozhodně není. Pluginy jako **Sucuri** nebo **WordFence** mohou zvýšit bezpečnost webu, to určitě ano, ale nejsou samospasitelné, pokud neprovede nic z toho, o čem jsem psal v tomto článku.

Tyto pluginy tedy berte pouze jako doplněk bezpečnosti a to ještě ne nutný. Pokud se budete řídit výše popsanými kroky, troufám si tvrdit, že takovéto pluginy nikdy potřebovat nebudete.

Sucuri

Plugin Sucuri Security – Auditing, Malware Scanner and Security Hardening můžete najít v oficiálním repozitáři zde: Sucuri Scanner. Instalaci pluginu provedete klasickým postupem z administrace WordPressu přes sekci pluginů. Tento plugin umí konkrétně tyto činnosti:

- Bezpečnostní audit činnosti
- Monitorování integrity souborů
- Vzdálené skenování malware
- Monitorování blocklistu
- Efektivní zabezpečení
- Akce v oblasti zabezpečení po hackerském útoku
- Oznámení o bezpečnosti
- Firewall pro webové stránky (prémiový)

WordFence

Plugin WordFence můžete získat na této URL adrese: Wordfence Security – Firewall, Malware Scan, and Login Security. Tento bezpečnostní plugin podobně jako Sucuri výše umí řešit tyto činnosti:

- WAF (Web Aplication Firewall)
- Real time firewall (premium)
- Malware scanner
- Ochrana proti Brute Force útoku
- Oprava souborů přepsaných mallwarem
- Kontrola bezpečnosti obsa

Oba pluginy mohou řešit situaci, kdy je web napadený a potřebujete jej vyčistit od zákeřného kódu. Nicméně osobně si myslím, že nikdy nemůžete výsledku věřit natolik, jako když budete k dispozici nenapadenou zálohu webu. To je vždy to nejsnazší a nejjednodušší řešení vzniklé situace. Mnoho funkcí obou pluginů je navíc placených a tudíž se dostanete do situace, že budete za tyto pluginy muset buď platit, nebo je používat v jejich základní variantě zdarma. A ta neposkytuje takovou ochranou webu, jako když si zabezpečení WordPressu provedete sami již od začátku. Proto oba pluginy zmiňuji na konci článku a pouze jako jednu z možností.

Jak zabezpečit WordPress – závěrem

Jak vidíte, je zabezpečení WordPressu opravdu velmi komplexní akce, která zahrnuje mnoho parametrů ochrany. Ta se týká nejen administrace, ale také uživatelů a jejich chování, souborů na FTP a databázi a celého systémů. Jak jste mohli pochopit z článku výše, klíčové je, abyste se o svůj systém pravidelně starali. Klíčové jsou aktualizace. Neaktualizovaný systém je obrovské riziko, které láká mnoho hackerů k útoku na Váš web.

Dnes je velmi jednoduché zjistit, na jaké technologii Váš web běží a jaké komponenty web používá. Např. služba https://builtwith.com řekne o Vašem webu potenciálnímu útočníkovi opravdu mnoho. Ten se může soustředit na Vaše pluginy a hledat jejich potenciální chyby ve starších, neaktualizovaných verzích. Výše uvedená pravidla, pokud je aplikujete a budete dodržovat, udělají z Vašeho WordPressu relativně nedobytnou pevnost. Nicméně i tak se může stát, že nějakému poškození dojde. Nic není samospasitelné. Proto zálohujte svá data a dělejte to pravidelně. Záloha nepoškozeného a nenapadeného webu může vyřešit mnoho dlouhých nocí

strávených nad tím, že budete hledat zákeřný kód ve svém webu. Obnova webu ze zálohy je otázkou několika minut a problém je vyřešený.

FAQ – často kladené dotazy – Jak zabezpečit WordPress

Jaký je nejčastější způsob, jak hackeři pronikají do WordPress stránek?

Hackeři často využívají slabá hesla, zastaralé pluginy, nebo šablony s bezpečnostními chybami. Také používají útoky typu brute-force na přihlašovací formuláře administrace.

Jak mohu zvýšit zabezpečení WordPress webu?

Bezpečnost svého webu můžete posílit pomocí silných hesel, pravidelných aktualizací WordPressu, pluginů a šablon vzhledu. Bezpečnosti také pomůžete instalací bezpečnostních pluginů, zabezpečením souborů a databáze. Pravidelně zálohujte obsah svého webu.

Co dělat v případě, že je můj WordPress napaden?

Pokud je váš web napaden, uveďte svůj WordPress do režimu údržby, aby nepoškozoval potenciální uživatele Vašeho webu. Poté analyzujte zranitelnost a přijměte opatření k zajištění, aby se podobný incident neopakoval. Pokud máte zálohu webu, která napadená není, obnovte web ze zálohy a poté ošetřte zabezpečení WordPressu podle výše uvedených kroků v tomto článku.

Jaké jsou nejlepší praktiky pro správu hesel uživatelů ve WordPressu?

Nejlepší praktiky zahrnují:

- používání silných a unikátních hesel
- aktivaci dvou faktorové autentizace
- pravidelné změny hesla
- omezení počtu pokusů o přihlášení
- používání password managera namísto ukládání hesla do prohlížeče

Je důležité pravidelně aktualizovat WordPress a jeho pluginy?

Ano, pravidelné aktualizace WordPressu a pluginů jsou zásadní pro zajištění zabezpečení vašeho webu. Aktualizace často zahrnují opravy bezpečnostních chyb a zranitelností.

Jak mohu chránit svůj WordPress web před útoky typu "brute-force"?

Můžete chránit svůj web před útoky brute-force pomocí pluginů, které omezují počet neúspěšných pokusů o přihlášení, používáním silných hesel a implementací dvou faktorové autentizace.

Jak mohu ověřit, zda jsou pluginy a témata, které používám, bezpečné?

Můžete použít online nástroje, jako je Sucuri nebo WordFence, k ověření zabezpečení WordPressu, pluginů i šablon. Také je důležité sledovat aktualizace a recenze od uživatelů.

Je důležité zálohovat WordPress a data na webu?

Ano, pravidelné zálohování je důležité pro případ, že váš web bude napaden, nebo dojde k jeho selhání. Měli byste zálohovat nejen soubory na FTP, ale i databázi. Existuje mnoho pluginů, které budou pravidelnou zálohu provádět za Vás a tuto zálohu uloží na cloudové úložiště jako je např. Google disk, One Drive apod. Mezi nejlepší patří např. plugin Updraft.

Jak mohu zabezpečit svůj administrátorský účet v WordPressu?

Svůj administrátorský účet můžete ochránit pomocí silného hesla, aktivace dvou faktorové autentizace, omezení počtu pokusů o přihlášení a používáním bezpečného připojení k internetu. Také zvažte změnu URL administrace svého WordPressu

Co dělat, když mám podezření, že je na mém webu škodlivý kód?

V případě podezření na škodlivý kód byste měli okamžitě provést kontrolu a odstranění infekce. To může zahrnovat skenování pomocí bezpečnostního pluginu Sucuri nebo Wordfence. Také proveďte ruční kontrolu souborů na FTP a tabulek

databáze pomocí phpMyAdmin nástroje. Pokud problematice zabezpečení WordPressu nerozumíte, vyhledejte odbornou pomoc. Ceny za odvirování webu se aktuálně pohybují od 1500 Kč do 6000 Kč v závislosti na velikosti poškození webu a odbornosti člověka, který bude odvirování provádět. Požadujte záruku, aby se nestalo, že na webu budou tzv. zadní vrátka a infekce se vrátí. Pokud máte čistou zálohu webu, obnovte ji a proveďte zabezpečení WordPressu podle bodů ve článku.