Návod na aktivaci licence bezpečnostního pluginu WordFence Security

Poslední aktualizace 15 listopadu, 2024

WordFence Security patří mezi špičku mezi bezpečnostními WordPress pluginy. Proto jsme jej vybrali mezi ty pluginy, které na váš WordPress hosting instalujeme automaticky. Po instalaci je však ještě třeba jej aktivovat a nastavit.

Zde si povíme:

- jak aktivovat bezplatnou licenci WordFence Security
- jak tento WordPress plugin nastavit
- tipy na lepší zabezpečení webových stránek
- něco o pluginu WordFence na závěr

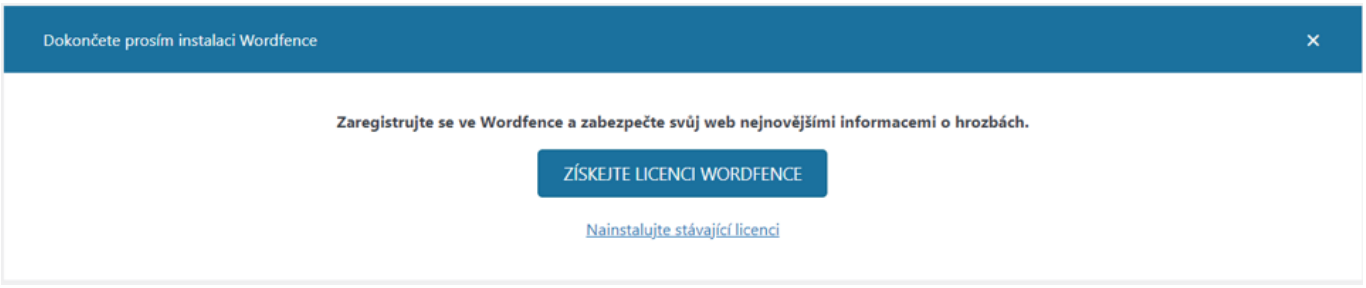
Chcete-li mít **WordFence v češtině** bude možná nutné jej nejprve aktualizovat. Po jeho instalaci si zkontrolujte, zda máte povolenou automatickou aktualizaci.

Aktivace bezplatné licence WordFence

Ve vašem WP adminu na vás po instalaci pluginu bude svítit upozornění, že je třeba instalaci ještě dokončit. WordFence totiž ještě vyžaduje registraci a aktivaci licence na stránkách výrobce.

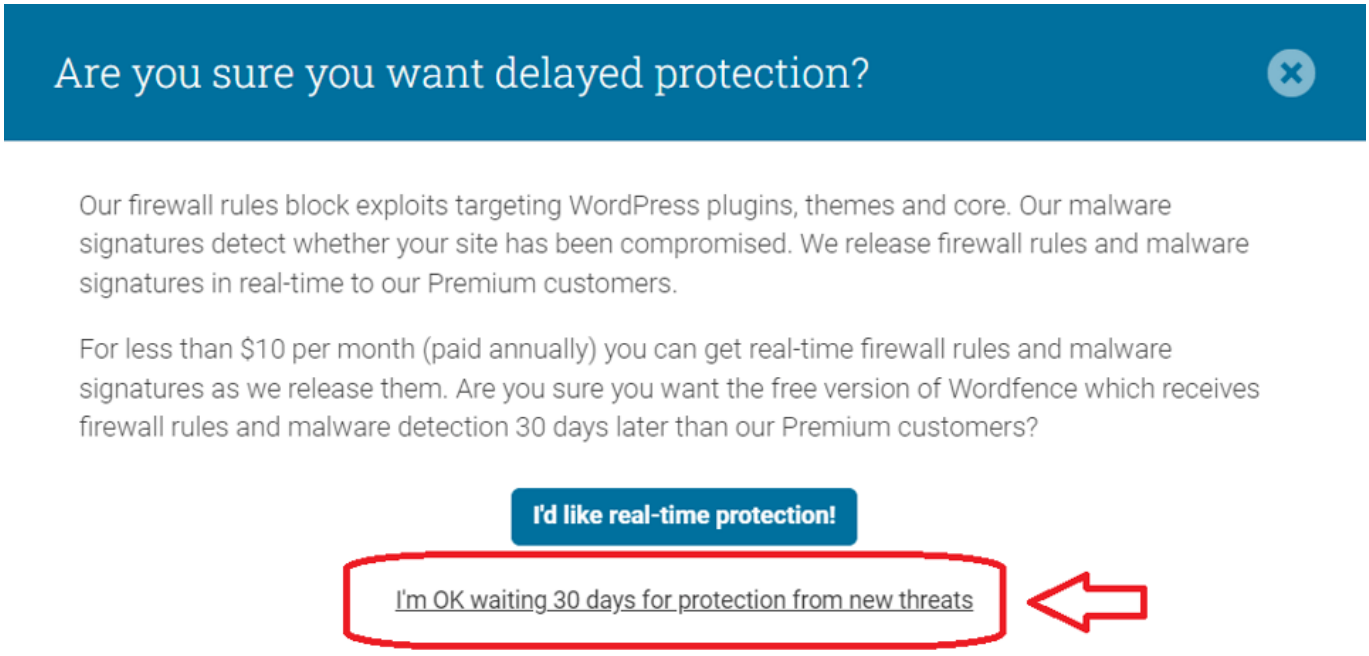
K využívání pluginu vám ale vystačí bezplatná licence. Pro její získání stačí kliknout na modré tlačítko **Získejte licenci WordFence.**

Následně budete přesměrováni na stránky pluginu.

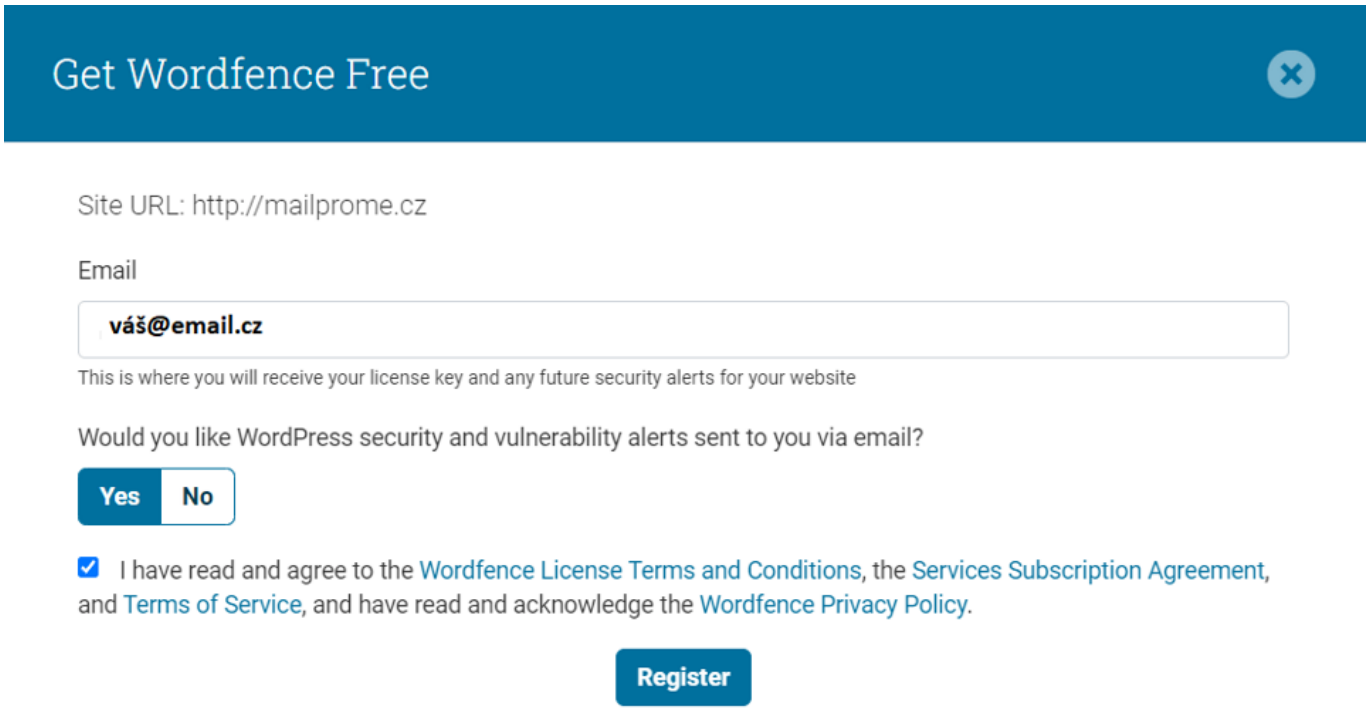


1. Na webu pluginu pokračujte kliknutím na tlačítko **Get a Free licence**.

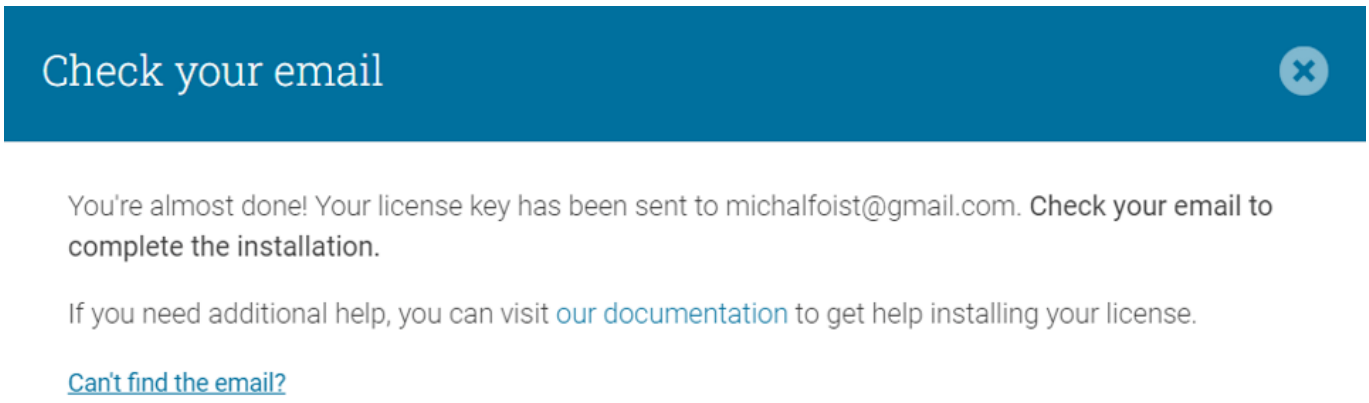
2. Klikněte na souhlas se 30 denním zpožděním aktualizací databáze pluginu, což je vlastnost verze zdarma.

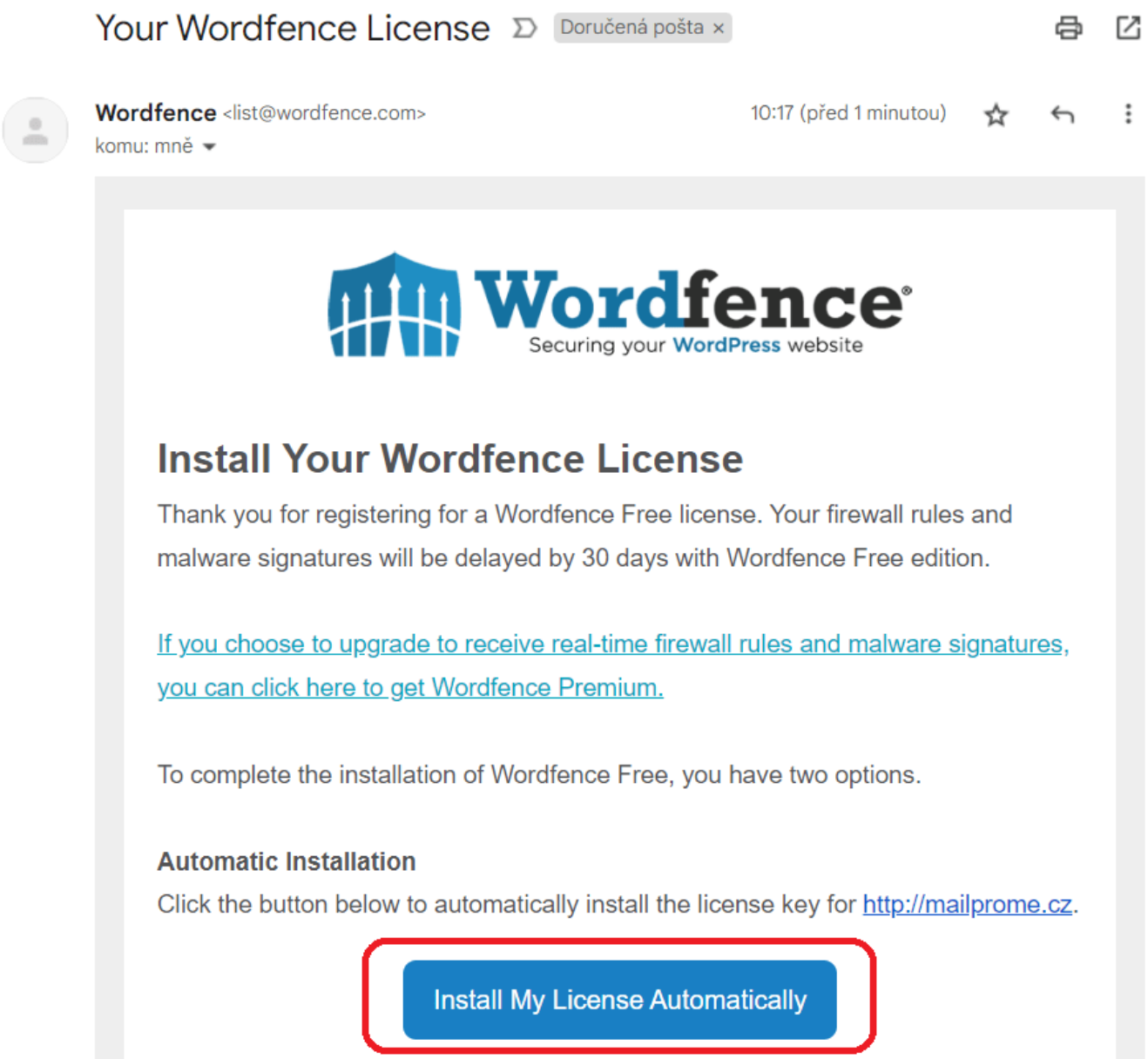


3. Zadejte svůj e-mail, na který se naváže FREE licence Wordfence a potvrďte akceptaci s pravidly a klikněte na tlačítko **Register**

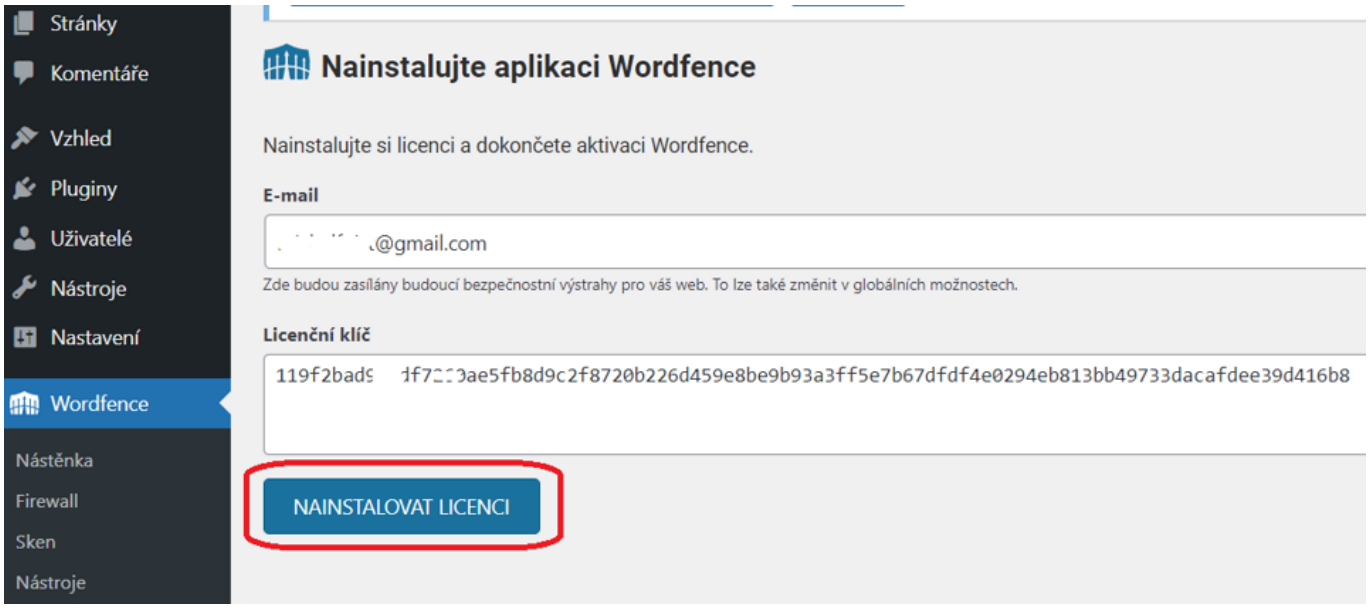


4. Do vaší e-mailové schránky vám od WordFence přijde potvrzovací e-mail. V e-mailu klikněte na **Install my license automatically**, to vás přenese zpět do Vašeho WordPressu.

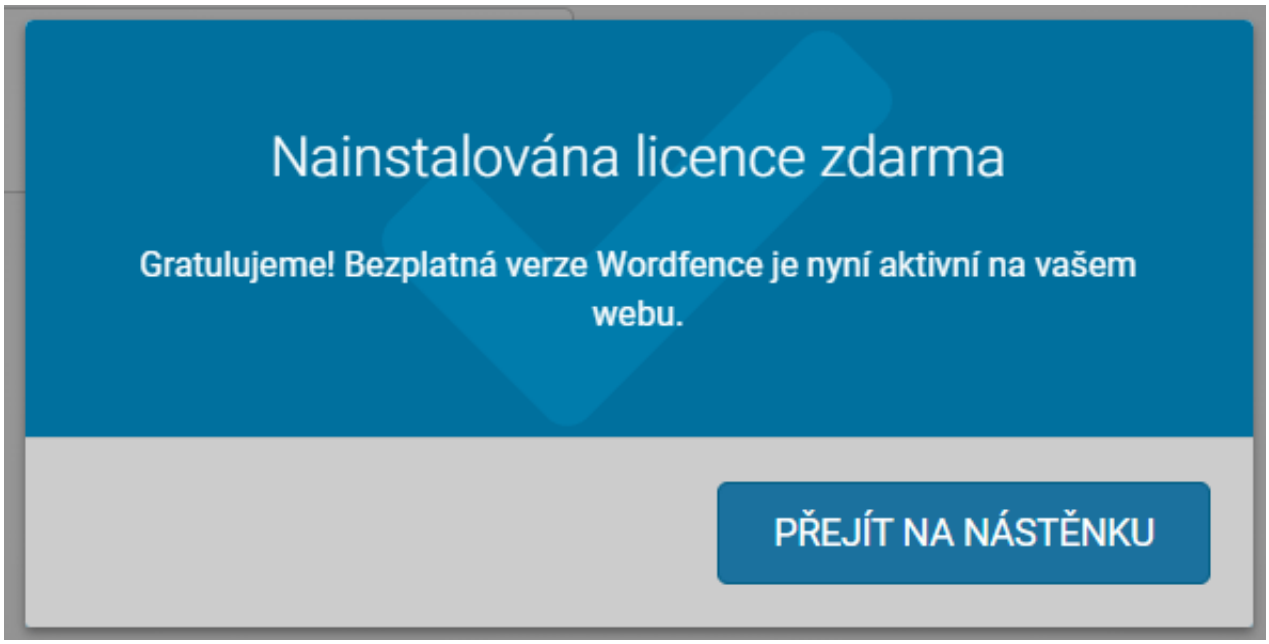




5. Zde již jen potvrdíte instalaci licence kliknutím na **Nainstalovat licenci**.



6. Hotovo, máte nainstalovanou free licenci pluginu Wordfence.



Nyní můžeme přejít k základnímu nastavení pluginu.

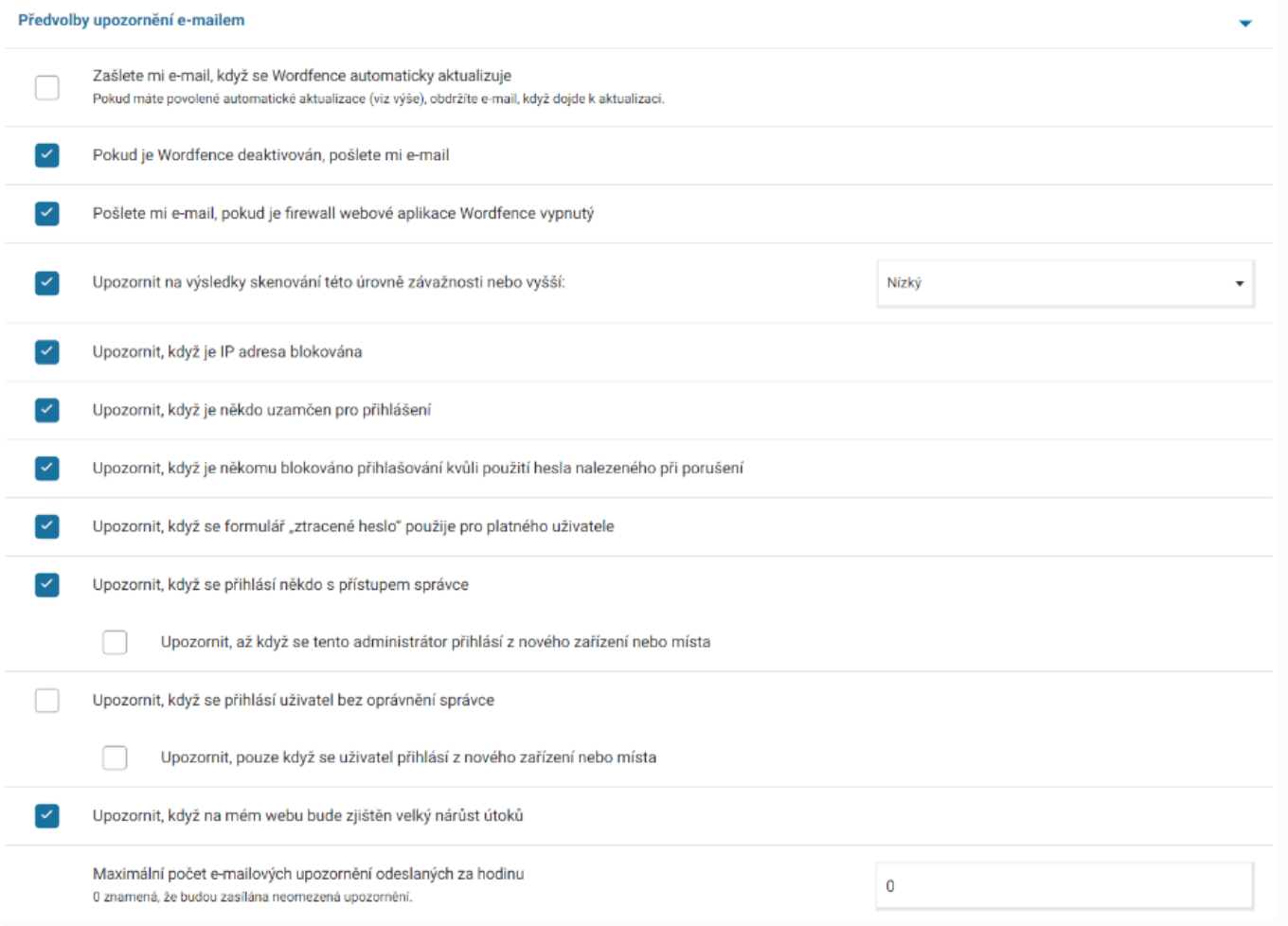
Nastavení pluginu WordFence Security

Po nainstalování pluginu Wordfence a jeho aktivaci, která je popsána výše, doporučujeme pouze drobné přenastavení.

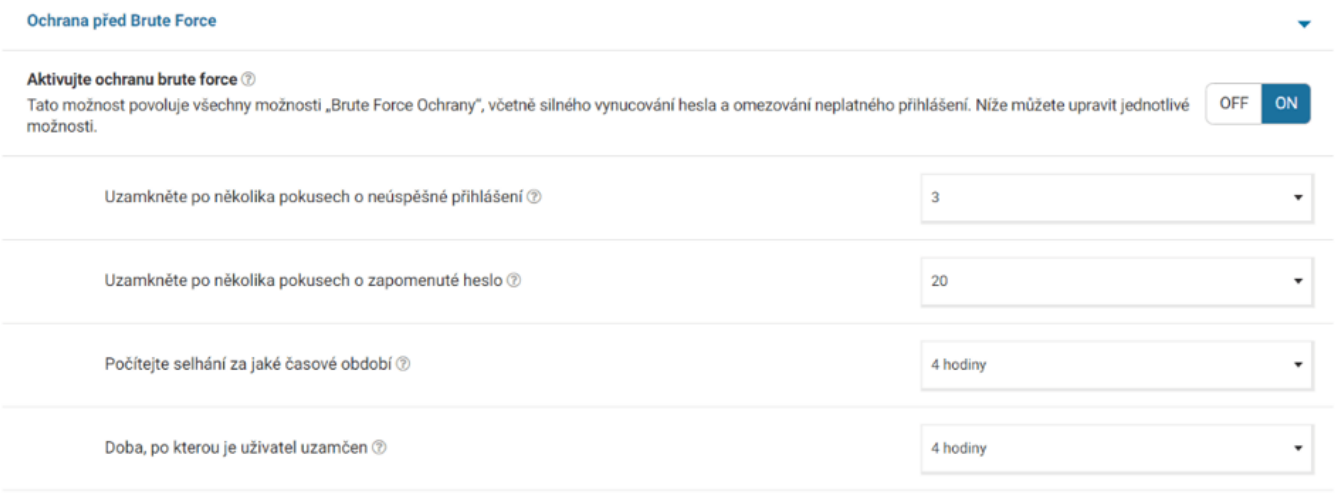
V základním nastavení je plugin také funkční, ale s drobnými úpravami dosáhnete lepší bezpečnosti.

Vše zvládnete sami, není to nijak složité.

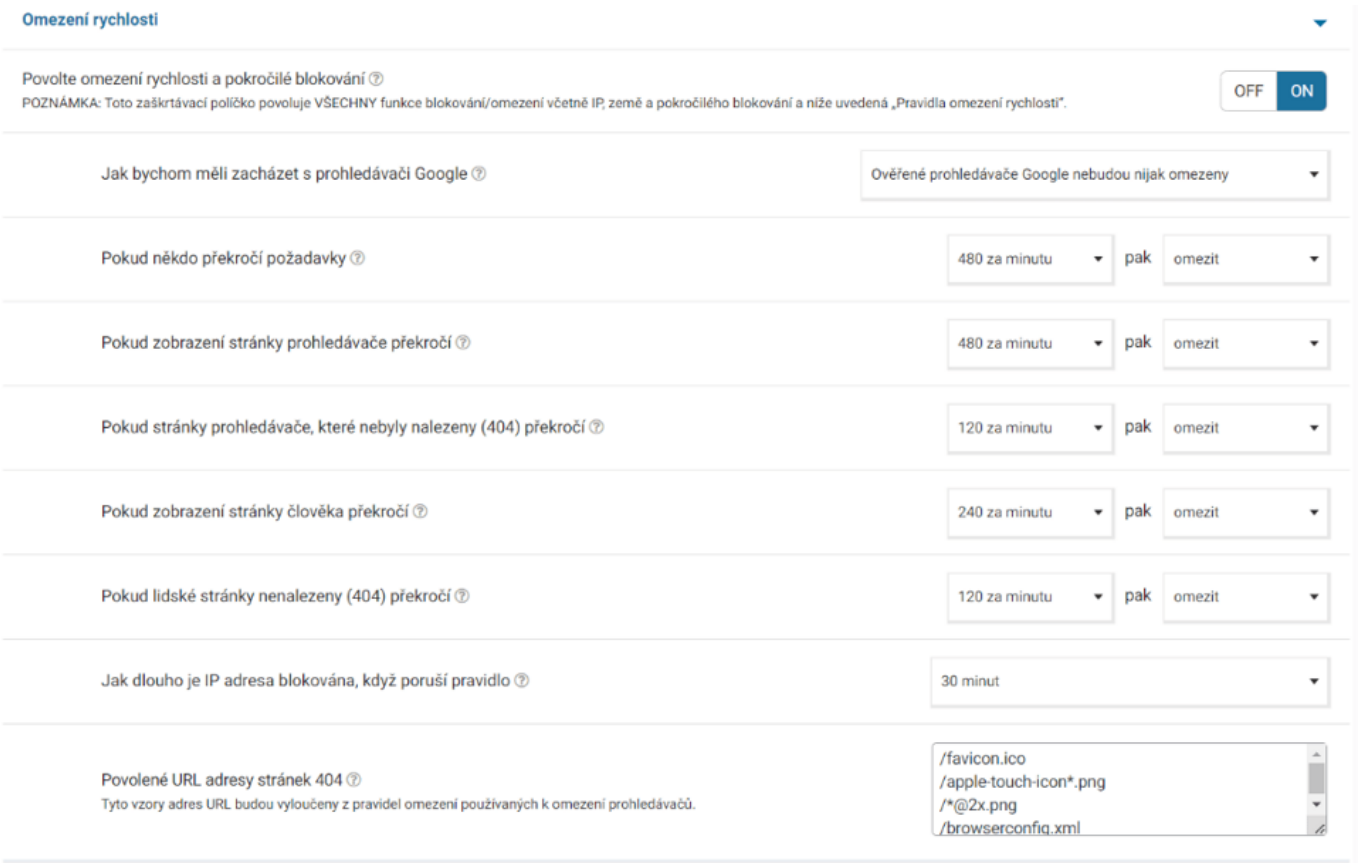
1. Přejděte v levém menu Wordfence do nastavení **Všechny možnosti**.
2. Zde si můžete nastavit, jak chcete aby vám byly zasílány e-maily o různých aktivitách. Níže zobrazené nastavení je jedna z možností.



3. Další nastavení je ochrana proti strojovému a robotickému prolamování hesel, tzv. **brute force attack**. Oproti původnímu nastavení lze například zvolit přísnější režim, tedy 3 pokusy a 1 hodinové zablokování.

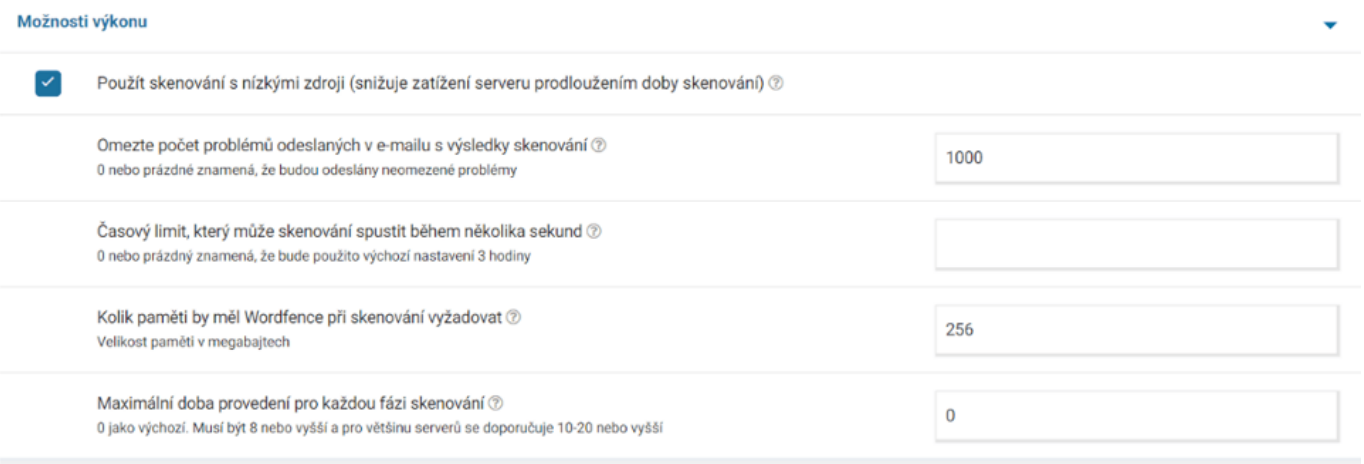


4. Další část, kterou doporučujeme upravit je **Rate limit**. Opět se jedná o zvolení přísnějších hodnot, než je výchozí nastavení.



5. Nastavení skenování WordFence doporučujeme přepnout na **standardní scan**, ne menší (to je vhodné zejména pro ty, kteří se technicky příliš neorientují v nastavení svého webhostingu a aktuální zátěže webových stránek).

6. Dále upravte **Možnosti výkonu** na zaškrtlou hodnotu Použít **skenování s nízkými zdroji**, ať si nepřetěžujete svůj webhosting.



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

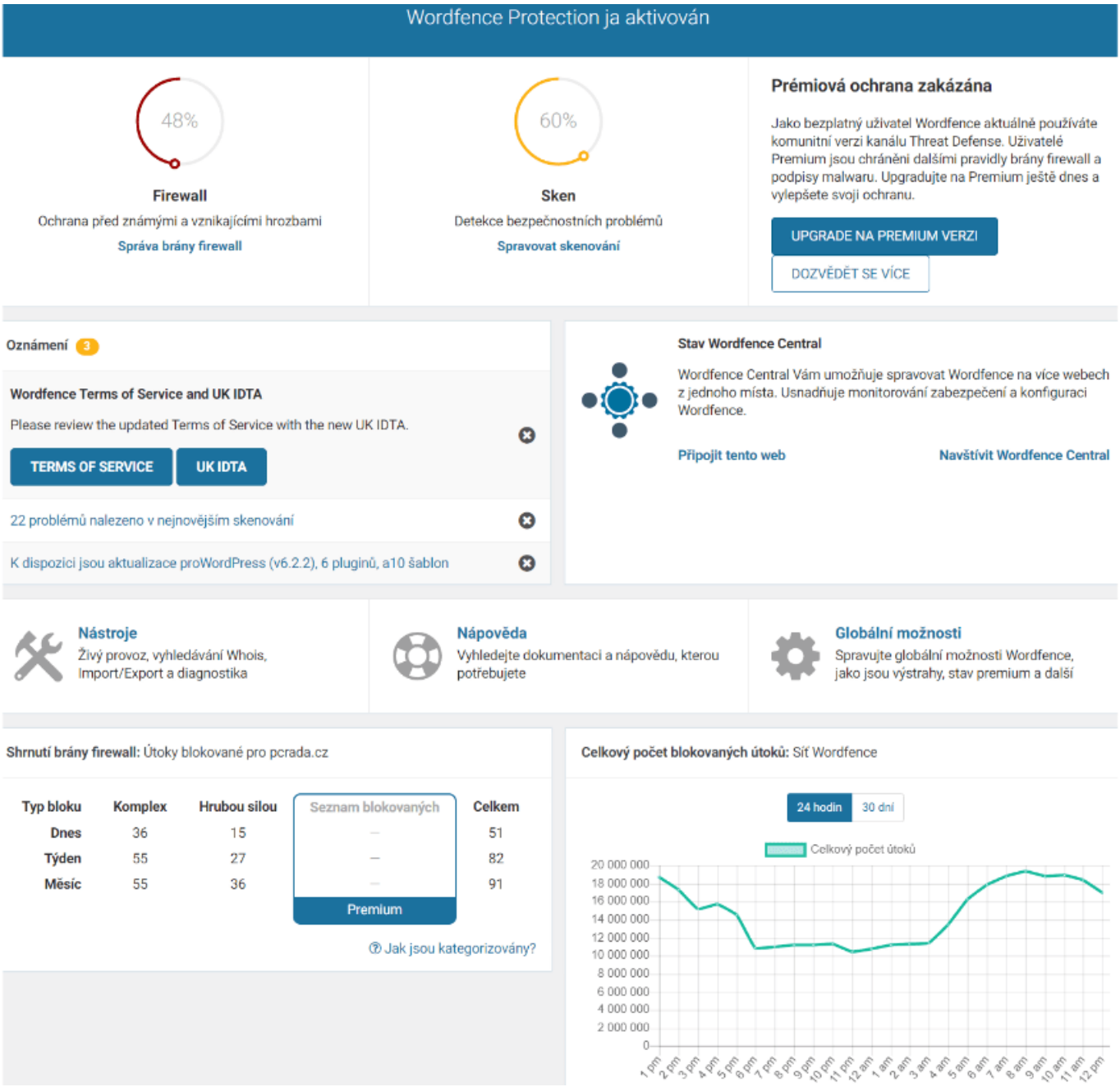
A to je vše!

Po prvních dnech a týdnech se neděste stavu, který uvidíte. Procenta Firewall a Scan zřejmě nebudou 100%, ale to nevadí.

Zjistíte, že na váš web útočí desítky hackerů a robotů týdně (a stovky až tisíce měsíčně). To je na internetu bohužel normální.

WordFence vám tyto útoky jednak reportuje, a jednak chrání váš web, aby útočníci nepronikli do jádra vašich webových stránek.

Drtivou většinu běžných internetových útoků plugin WordFence odvrátí a váš web ubrání.



Placené verze WordFence vám nabídnou rozšířené možnosti funkcí, nastavení, reportingu i ochrany.

Tipy pro zabezpečení webových stránek obecně

Za prioritní bezpečností faktory pro WordPress weby považujeme:

- Pravidelné aktualizace WordPressu.
- Používání ověřených a dobře hodnocených šablon a pluginů.
- Aktualizace šablony.
- Aktualizace pluginů.
- Používání unikátního uživatelského jména a hesla pro přihlášení.
- Neukládání hesel kamkoliv do PC ani do internetových prohlížečů (typicky Chrome nabízí uložení). Používejte Password manager (např. 1password.com).
- Přihlašování do WordPressu z bezpečných WiFi. V kavárnách atp. používejte minimálně VPN.
- Používejte službu Cloudflare (vyžaduje trochu více technických znalostí při nastavování).
- Nainstalujte, aktivujte a používejte plugin WordFence Security.

A především, pravidelně své webové stránky zálohujte.

Svůj web nikdy neukládejte na bezplatné webhostingy. Vždy používejte spolehlivý a bezpečný WordPress hosting.

K čemu slouží Plugin WordFence Security

WordPress je nejrozšířenější redakční systém, a to je v tomto případě jeho nevýhodou – existuje více útočníků a robotů, kteří jsou zaměřené právě na webové stránky běžící na WordPressu.
Bezpečnostní WordPress plugin WordFence se vám postará o to, aby váš web byl chráněný proti hackerům, robotům a řadě dalších „útočných“ nástrojů.
Slouží jako firewall a malware scanner, jehož úkolem je chránit váš WordPress před napadením.

WordFence je zdarma a při základním nastavení nemá zvýšené nároky na webhosting, takže nemusíte platit ani nic extra za webhostingový tarif.

Má miliony stažení – jedná se o jeden z nejstahovanějších pluginů v celé knihovně WordPress vůbec.

WordFence navíc umí česky.

Nejdůležitější funkce pluginu WordFence

- 2FA: 2 fázová autentifikace
- Ověřování Captcha, ochrana formulářů
- Filtrování dle IP (zamezení přístupu dle IP, z různých zemí, atp.)
- Testování na napadení webu malwarem
- Firewall 24/7