Jak zabezpieczyć Wordpressa? Poznaj 6 sposobów

Posiadasz stronę internetową na WordPressie, jesteś świadomy zagrożeń występujących w dzisiejszej dobie internetu i chciałbyś się dowiedzieć jak możesz zabezpieczyć swoją stronę opartą na Wordpressie?

W dzisiejszej erze cyfrowej coraz więcej firm decyduje się na prowadzenie swojej działalności w internecie i tak samo duża ilość przedsiębiorców postanawia prowadzić swoją stronę opartą na WordPressie. Ponad 500 witryn jest tworzonych każdego dnia za pomocą tej platformy, a tylko 60-80 witryn dziennie jest tworzonych na platformach takich jak Shopify i Squarespace.

Trudno się dziwić. **WordPress jest jednym z najpopularniejszych systemów zarządzania treścią (CMS) i najszybciej rozwijającą się platformą na świecie.** Niestety tak duża popularność tego systemu niesie za sobą także większe **ryzyko ataku cyberprzestępców.**

W tym artykule przekażę Tobie wszystkie najważniejsze wskazówki, które pomogą Ci zwiększyć bezpieczeństwo Twojej strony internetowej.

STOSOWANIE CERTYFIKATÓW SSL - KOMUNIKACJA PROTOKOŁEM HTTPS

Pierwszą rzeczą, którą należy zrobić, jest wdrożenie szyfrowanej komunikacji, która zapewni ochronę odwiedzającym Twoją stronę przed oszustwami i znacznie zmniejszy ryzyko oraz utrudni ''szpiegowanie'' i kradzież informacji takich jak: dane pozostawione przez potencjalnych klientów w formularzach kontaktowych czy dane logowania.

W jaki sposób zainstalować certyfikat SSL i odpowiednią wtyczkę?

- Zaloguj się do swojego panelu
- Przejdź do zakładki ''wtyczki'', wyszukaj i zainstaluj odpowiednią wtyczkę o nazwie

''Really Simple SSL

- Po zainstalowaniu i uruchomieniu wtyczki wybierz ''Go ahead, activate SSL''

Gotowe. Kiedy przejdziesz do swojej witryny, zobaczysz, że strona została oznaczona jako bezpieczna.

AKTUALIZACJE WORDPRESSA – Jak zabezpieczyć Wordpressa za pomocą aktualizacji?

Tę kwestię powinieneś wziąć szczególnie pod uwagę, jeżeli chcesz zabezpieczyć swoją witrynę przed atakami. To jest podstawa. Nie chodzi tu tylko o aktualizację samej platformy, która

powinna przebiegać automatycznie, ale warto również sprawdzić, czy nie stosujesz wtyczek, które nie są już aktualne – to samo tyczy się motywów graficznych. Pamiętaj, żeby instalować wtyczki oraz motywy tylko z zaufanych źródeł!

Ciekawostka I: 41% ataków na WordPress jest spowodowanych luką w platformie hostingowej, natomiast 44% włamań było spowodowanych przestarzałymi witrynami WordPress.

Ciekawostka II: Jednym z największych wycieków danych, które dotknęły WordPress, był wyciek dokumentów z Panamy w 2016 r., Który dotknął 2,6 TB danych, 11,5 miliona dokumentów i 4,8 miliona e-maili. Przyczyną była witryna, na której nie była uruchomiona najnowsza wersja wtyczki.

WYKONANIE KOPII ZAPASOWYCH TWOJEJ WITRYNY

No dobrze. Zaktualizowałeś system, wtyczki i motywy, Twoja strona ma szyfrowanie. To już duży krok do zwiększenia bezpieczeństwa Twojej strony, ale czy to wystarczy? Odpowiedź brzmi - nie. Wykonanie poprzednich działań jest absolutnie ważne, ale jeszcze warto zrobić kilka rzeczy, które maksymalnie zabezpieczą Twoją stronę.

Tworzenie kopii zapasowych Twojej strony to kolejna, nie mniej ważna od pozostałych kwestia. Warto tworzyć je regularnie, chociażby przed wykonaniem aktualizacji WordPressa. Dzięki temu nie będziesz się martwił o swoje zasoby w momencie, kiedy wystąpią nagłe, nieprzewidziane zdarzenia, takie jak:

- Ludzki błąd (Nawet pozornie niewinny ludzki błąd może spowodować awarię witryny i utratę danych. Regularne tworzenie kopii zapasowych pomoże Twojej firmie szybko odzyskać dane i przywrócić stronę do stanu, w jakim była przed awarią).
- Włamanie na stronę internetową (Jeśli Twoja witryna zostanie przejęta, dostęp do kopii zapasowych może znacznie ułatwić Ci życie! Najszybszy sposób na odzyskanie danych ze zhakowanej witryny, to przywrócenie jej do najnowszej wersji, która istniała przed włamaniem. Wcześniejsze utworzenie kopii zapasowej sprawi, że przywrócisz swoją stronę do działania w ciągu kilku godzin lub nawet minut. Bez dobrej kopii zapasowej będziesz musiał ręcznie wyczyścić zhakowaną witrynę lub zapłacić specjaliście, aby zrobił to za Ciebie).
- Nieudane aktualizacje (Proces aktualizacji platformy, wtyczek lub motywów czasami może zakończyć się uszkodzeniem lub awarią witryny)

Jak utworzyć i przywrócić kopię zapasową Twojej strony?

Możesz to zrobić w prosty sposób w cPanelu.

- Wejdź w menu główne

● Z pola ‘’pliki’’ wybierz opcję ‘’kopia zapasowa’’. Po wybraniu tej opcji otworzy Ci się strona, na której możesz wykonywać wszystkie operacje związane z kopią bezpieczeństwa. Masz możliwość tworzenia jak i wczytania wcześniej utworzonej kopii bezpieczeństwa poszczególnych elementów. W taki sposób z łatwością utworzysz i przywrócisz kopię zapasową swojego konta w cPanelu.

CHROŃ SWÓJ PANEL ADMINISTRACYJNY

Hakerzy nie używają żadnej komputerowej ''magii'' włamując się do serwerów. Najczęściej dostają się do witryn i kont, uzyskując zwyczajnie, w sprytny sposób, dostęp do danych logowania konta w Twojej witrynie. Oprócz luk w zabezpieczeniach - kradzież danych logowania to jeden z najczęstszych sposobów uzyskania dostępu do witryny przez hakerów.

W ten sposób zostało zhakowanych około 20% witryn WordPress. Wystarczy, że zaostrzysz zabezpieczenia na stronie logowania i panelu administracyjnym. W ten sposób możesz powstrzymać takie ataki na ich drodze i zabezpieczysz swoją stronę internetową.

Jak to zrobić?

● Przede wszystkim nie używaj jako loginu tych dwóch nazw (admin oraz administrator). Dlaczego? Ponieważ takie nazwy są popularne i łatwiej zostają wyłapywane przez automatycznie działające oprogramowania, które realizują próby włamania. Ustawiając login jako admin lub administrator, zwyczajnie ułatwiasz włamanie, dlatego jeśli do tej pory miałeś ustawioną którąś z tych nazw, koniecznie ją zmień na inną!

● Zadbaj o to, aby Twoje hasło było bardzo silne, unikalne i trudne do odgadnięcia. Im dłuższe i bardziej skomplikowane hasło - tym lepiej dla Ciebie.

● Dodaj uwierzytelnianie dwuskładnikowe do ekranu logowania. Jest to prosta technika, która dodaje dodatkowy czynnik weryfikacji do procesu logowania, wraz z hasłem. Jak to wygląda w praktyce? Takie rozwiązanie spowoduje konieczność podania dodatkowego (drugiego) składnika, np. wpisanie kodu PIN-u, który przyjdzie na Twój telefon, odcisk palca, rozpoznanie twarzy etc.

Tutaj z pomocą przychodzi wtyczka Rublon, za pomocą której uwierzytelnisz się dwuskładnikowo.

Te 3 wymienione powyżej metody są świetnym sposobem na zwiększenie bezpieczeństwa Twojego panelu.

ZABEZPIECZENIE PRZED SPAMEM

Spam występujący w komentarzach to uciążliwy i często występujący problem, szczególnie jeżeli prowadzisz bloga, a Twoja witryna staje się coraz bardziej popularna...

Pomimo, że sekcja komentarzy pozwala na wygodną interakcję z czytelnikami Twojej witryny, to niestety wraz z decyzją o możliwości wystawiania komentarzy i dzielenia się opinią wzrasta

ryzyko spamu. Wtedy zamiast skupić się tylko i wyłącznie na odpisywaniu swoim czytelnikom na komentarze - **musisz przenieść swoją energię na zajmowanie się spamem.**

Niestety Twoja irytacja nie jest jedynym problemem występowania spamu. Masowe komentarze mogą szybko zaśmiecić Twoją witrynę, sprawiając, że będzie znacznie wolniej się ładować, ponadto Twoja strona będzie z biegiem czasu odstraszać czytelników.

To jeszcze nie wszystko. **Łącza w komentarzach, które zawierają spam, mogą prowadzić do witryn, z których pobierane jest złośliwe oprogramowanie.**

Jak się przed tym uchronić?

Swoją stronę możesz zabezpieczyć przed spamem, instalując odpowiednie wtyczki, np. **Akismet-AntiSpam.** Możesz także utworzyć ''czarną listę słów lub skonfigurować system moderowania komentarzy.

DODATKOWE WTYCZKI BEZPIECZEŃSTWA

Gdy już masz wykonane te najważniejsze kroki w kierunku zabezpieczenia WordPressa, możesz zainstalować dodatkowe wtyczki bezpieczeństwa, ale pamiętaj o tym, że mogą one służyć jako dodatkowa ochrona i **nie zastąpią ważnych aktualizacji, instalacji certyfikatu SSL czy innych bardzo ważnych rzeczy, które zostały wymienione w tym artykule.**

Na przykład instalując wtyczkę **Wordfence Security** będziesz dostawał powiadomienie e-mail, w momencie kiedy ktoś będzie próbował dostać się do Twojego panelu administracyjnego oraz przypomnienie o aktualizacji składników WordPressa.

Jak widzisz, zwiększenie bezpieczeństwa swojej strony opartej na platformie WordPress nie jest tak skomplikowane, jak mogłoby Ci się wydawać! Wiedzę już masz, teraz zacznij sukcesywnie, krok po kroku wdrażać przedstawione rozwiązania.