opieka wordpress

Włamania na stronę WordPress? Jak sobie z nimi radzić?

Hakerzy szukają luk w Wordpresie

Strony oparte na WordPressie cieszą się ogromną popularnością – to jeden z najczęściej wybieranych systemów zarządzania treścią (CMS) na świecie. Niestety, ich popularność przyciąga również uwagę hakerów, którzy stale szukają luk w zabezpieczeniach. Włamanie na stronę WordPress **może skutkować utratą danych, wyciekiem informacji, a także poważnymistratami finansowymi i wizerunkowymi.**

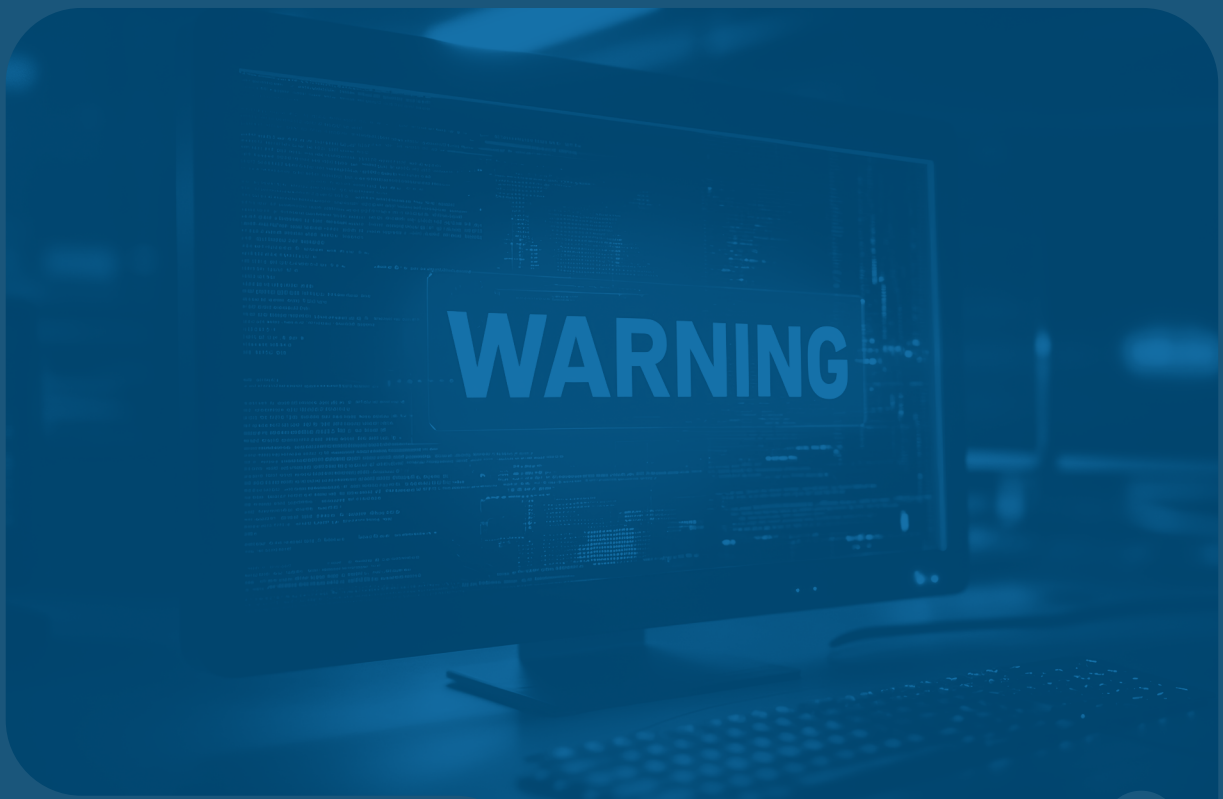
Pamiętaj!

Jeżeli doszło do włamania na Twoją stronę WordPress, najważniejsze jest, aby szybko podjąć odpowiednie kroki, a w przyszłości zapobiec podobnym incydentom.

Dowiedz się więcej!

Co zrobić **po wykryciu włamania** na stronę WordPress?

Jeśli podejrzewasz, że Twoja strona padła ofiarą ataku hakerskiego, szybka reakcja jest kluczowa. Im dłużej strona pozostaje w rękach hakerów, tym większe szkody mogą zostać wyrządzone.



Na kolejnych stronach
znajdziesz kilka **podpowiedzi!**

Odizoluj zagrożenie

1

Nasza rada

Pierwszym krokiem po włamaniu jest natychmiastowe zablokowanie dostępu do strony dla użytkowników zewnętrznych. Możesz to zrobić, np. **przekierowując ruch na stronę "w budowie" lub wyłączając witrynę.**

Pamiętaj!

Odizolowując zagrożenie zminimalizujesz ryzyko rozprzestrzenienia się szkód, np. w postaci zainfekowania komputerów użytkowników odwiedzających stronę. Dzięki temu chronisz użytkowników!

Nasza pomoc

W ramach naszych usług zajmujemy się **szybkim odizolowaniem zagrożenia**, aby chronić zarówno Ciebie, jak i Twoich klientów.

Przywróć **kopię zapasową**

2

Regularne tworzenie kopii zapasowych to fundament bezpieczeństwa strony. Jeśli Twoja strona została zaatakowana, jednym z najprostszych rozwiązań może być przywrócenie kopii zapasowej sprzed ataku.

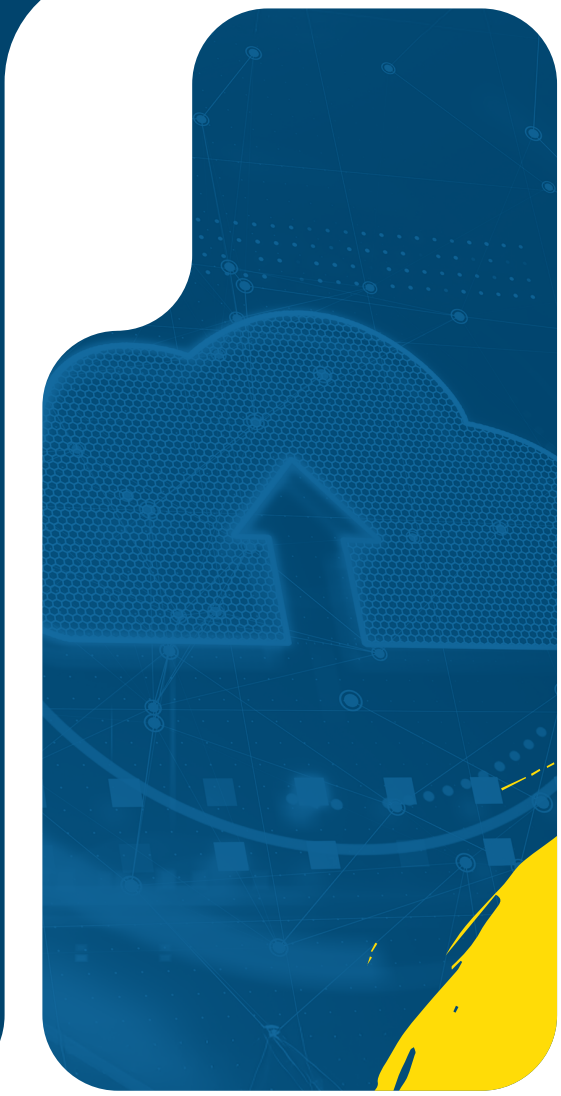
Nasza rada

Twórz kopie zapasowe regularnie:

- **Codziennie**
  Jeśli masz dynamiczną stronę (sklep, forum, portal z treścią dodawaną codziennie).
- **Co tydzień**
  Dla stron firmowych, blogów, stron wizytówek z mniejszą liczbą aktualizacji.
- **Przed każdą aktualizacją**
  WordPressa, wtyczek, motywu – na wypadek problemów z kompatybilnością.

Nasza pomoc

Oferujemy regularne i bezpieczne tworzenie backupów, co pozwala na **szybkie przywrócenie witryny** w przypadku jakichkolwiek problemów. Pomożemy stworzyć system backupów, który w przyszłości pozwoli uniknąć podobnych problemów.



Skanowanie i usuwanie **złośliwego oprogramowania**

3

Hakerzy często pozostawiają na stronie złośliwe skrypty, które mogą powodować dalsze problemy, nawet po przywróceniu kopii zapasowej. Należy dokładnie przeskanować stronę, aby upewnić się, że nie ma tam żadnych ukrytych zagrożeń.

Nasza rada

Skanuj stronę w zależności od sytuacji:

- **Codziennie**
  Jeśli masz stronę o wysokim ruchu lub prowadzisz sklep internetowy (WooCommerce).
- **Co tydzień**
  Dla standardowych stron firmowych, blogów i portfolio.
- **Po każdej aktualizacji**
  Wtyczek, motywu lub samego WordPressa.
- **Po incydencie**
  Jeśli zauważysz podejrzane zachowanie, np. spadek wydajności, dziwne przekierowania lub nieautoryzowane zmiany

Nasza pomoc

Oferujemy regularne skanowanie stron WordPress w poszukiwaniu złośliwego oprogramowania oraz usuwanie wszystkich potencjalnych zagrożeń. Nasze zaawansowane narzędzia monitorują stronę w czasie rzeczywistym, co pozwala na wykrywanie i **eliminowanie złośliwego oprogramowania na bieżąco.**

Zmiana
wszystkich haseł

4

Po włamaniu koniecznie zmień hasła do wszystkich kont związanych z WordPressem.

Nasza rada

Po włamaniu musisz zmienić hasła:

- **Panelu administracyjnego,**
- **FTP**
- **Baz danych**
- **Hostingu**

Pamiętaj!

Używać silnych haseł – długich, zawierających kombinację liter, cyfr i symboli.

Nasza pomoc

Pomożemy Ci w zarządzaniu dostępami i hasłami, tak aby były one bezpieczne i trudne do złamania. Oferujemy również wdrożenie **dwustopniowej weryfikacji (2FA)** dla dodatkowej ochrony.

Aktualizacja WordPressa, motywów i wtyczek

5

Nieaktualizowane wtyczki i motywy to jedna z najczęstszych przyczyn włamań na strony WordPress. Z tego powodu konieczne jest regularne aktualizowanie wszystkich komponentów witryny.

Pamiętaj!

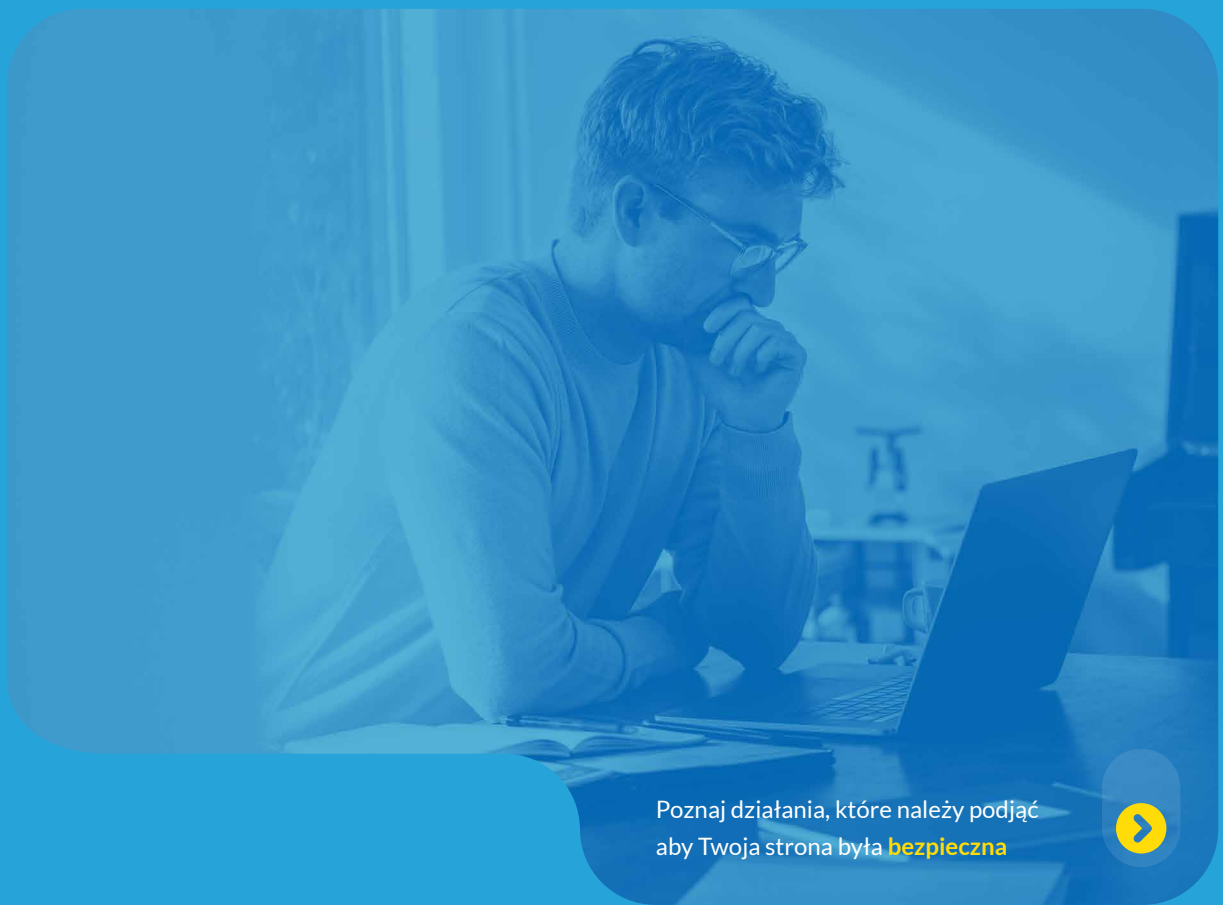
Aktualizacje zawierają poprawki bezpieczeństwa, które zabezpieczają stronę przed nowymi zagrożeniami.

Nasza pomoc

Oferujemy bieżące monitorowanie i aktualizowanie WordPressa, wtyczek oraz motywów, dzięki czemu Twoja strona **będzie zawsze chroniona przed najnowszymi zagrożeniami.**

Jak zapobiec kolejnym **włamaniom?**

Odzyskanie kontroli nad stroną po ataku to jedno, ale zapobieganie przyszłym incydentom jest równie ważne.



Poznaj działania, które należy podjąć aby Twoja strona była **bezpieczna**

Instalacja zabezpieczeń

Zarządzanie bezpieczeństwem strony to ciągły proces, który należy mieć pod pełną kontrolą.

Przykładowe formy ataków, przed którymi powinnieneś chronić swoją witrynę:

- **Brute force**
- **SQL injection**
- **Cross - site scripting (XSS)**

Monitoruj witrynę **24/7,** aby szybko reagować na wszelkie próby włamania. Można do tego wykorzystać zewnętrze narzędzia i wtyczki tj. Wordfence Security czy Sucuri Security.

Nasza pomoc

Oferujemy **instalację i konfigurację zaawansowanych wtyczek bezpieczeństwa**, które chronią Twoją witrynę przed różnymi formami ataków.

Regularne aktualizacje

Nieaktualne wersje oprogramowania to potencjalne luki w zabezpieczeniach.

Pamiętaj o aktualizacji:

- **Wordpressa**
- **Wtyczek**
- **Motywów**

Przed aktualizacją powinno się wykonać backup.

Dostępne są automatyczne aktualizacje, ale musisz pamiętać, że mimo iż są wygodne, to mogą powodować błędy – warto testować na stronie stagingowej.

Nasza pomoc

Dbamy o regularne aktualizowanie, dzięki czemu Twoja strona jest **zawsze chroniona** przez najnowsze poprawki bezpieczeństwa.

Backupy

Nic nie daje większego spokoju niż regularne, automatyczne kopie zapasowe.

Aby skutecznie zabezpieczyć stronę, należy wykonać kopię:

- **Bazy danych**
  Zawiera wpisy, komentarze, ustawienia, użytkowników.
- **Plików WordPressa**
  Motywy, wtyczki, przesłane multimedia.
- **Pliku “wp-config.php”**
  Zawiera dane logowania do bazy danych.
- **Plików “.htaccess” i “robots.txt”**
  Mogą zawierać ważne reguły dotyczące działania strony.

Nasza pomoc

Oferujemy pakiety **backupów dostosowane do potrzeb** małych, średnich i dużych witryn, w tym sklepów internetowych.

Audyt

Monitorowanie i audyt bezpieczeństwa

Kilka pytań, które pomogą w audycie:

- **Czy WordPress jest zaktualizowany do najnowszej wersji?**
- **Czy wtyczki i motywy są aktualne?**
- **Czy nie ma nieużywanych, nieaktualizowanych wtyczek (mogą stanowić zagrożenie)?**
- **Czy wszyscy użytkownicy mają tylko niezbędne uprawnienia?**
- **Czy są nieużywane konta (np. byłych redaktorów, deweloperów)?**
- **Czy włączone jest uwierzytelnianie dwuskładnikowe (2FA)?**
- **Czy istnieje ochrona przed atakami brute-force?**
- **Czy ograniczono liczbę prób logowania?**

Nasza pomoc

Oferujemy **regularne audyty bezpieczeństwa,** które pomagają zidentyfikować potencjalne słabe punkty Twojej strony.

Podsumowanie

Włamanie na stronę WordPress może mieć poważne konsekwencje, ale z odpowiednią strategią i pomocą ekspertów, można szybko **odzyskać kontrolę i zapobiec kolejnym atakom.**

Opieka WordPress oferuje kompleksową pomoc w sytuacjach kryzysowych, a także proaktywne zabezpieczenia, które chronią Twoją stronę przed przyszłymi zagrożeniami.

Kwalifikacje są bardzo ważne

Bez względu na to, czy zarządzasz małą stroną, dużym serwisem czy sklepem internetowym, nasza oferta jest elastyczna i dopasowana do Twoich potrzeb. Zaufaj profesjonalistom i **zadbaj o bezpieczeństwo swojej strony oraz dane użytkowników.**

Monitorujemy bezpieczeństwo

Pomożemy Ci utrzymać Twoją witrynę na najwyższym poziomie **bezpieczeństwa.**

Optymalizujemy stronę

Twoja strona będzie, wydajna, dobrze widoczna w **wynikach wyszukiwania.**

Aktualizujemy wtyczki

Dzięki temu poprawiamy bezpieczeństwo i eliminujemy ryzyko problemów z **kompatybilnością.**

Wykonujemy backupy

Tworzymy kopie zapasowe, aby **wszystkie Twoje dane** były bezpieczne.

Odwiedź opiekawordpress.pl

Opieka WordPress – bezpieczeństwo, na które możesz liczyć!

opieka wordpress

Dziękuję za poświęcony czas

Zachęcam do kontaktu.
W razie dodatkowych pytań, pozostaję do dyspozycji.

Łukasz
Zieliński

+48 730 820 704

kontakt@opiekawordpress.pl