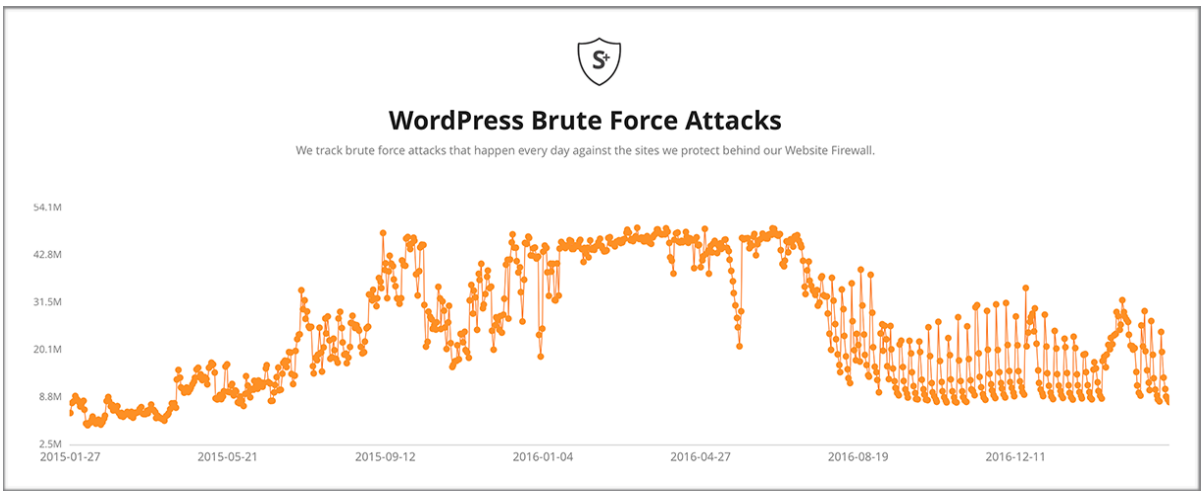
wpsec.pl

WordPress – wydajność i bezpieczeństwo

POTRZEBUJĘ NATYCHMIASTOWEJ POMOCY

Dlaczego atakować?

Już 27,8%[1] stron w Internecie wykorzystujących CMS opartych jest o system WordPress. Dzięki temu, że wszystkie z nich korzystają z tego samego silnika, podatności są powszechnie znane i proste w użyciu. Oznacza to, że niespełna jedna trzecia stron w Internecie jest potencjalnie podatna na atak ze strony hakerów i robotów internetowych zorientowanych na przejęcie **Twojej strony** i umieszczenia na niej złośliwego oprogramowania, lub odnośników prowadzących do Twojej konkurencji.



Codziennie **od dziesięciu do trzydziestu milionów stron** WordPress jest atakowanych metodą brute force[2]. Nikt nie robi tego ręcznie – w Internecie działają automaty, które samodzielnie odnajdują i atakują witryny podobne do Twojej. Dlatego tak ważnym jest, aby prawidłowo zabezpieczyć swoją stronę internetową.

Czy poradzę sobie sam z zabezpieczeniami?

Z większością na pewno tak. Najważniejsze z nich wymagają jednak logowania na serwer SFTP i wprowadzania zmian w kodzie Twojej strony internetowej. Jeśli nie jesteś biegły w programowaniu – poproś o pomoc specjalistę.

POTRZEBUJĘ NATYCHMIASTOWEJ POMOCY

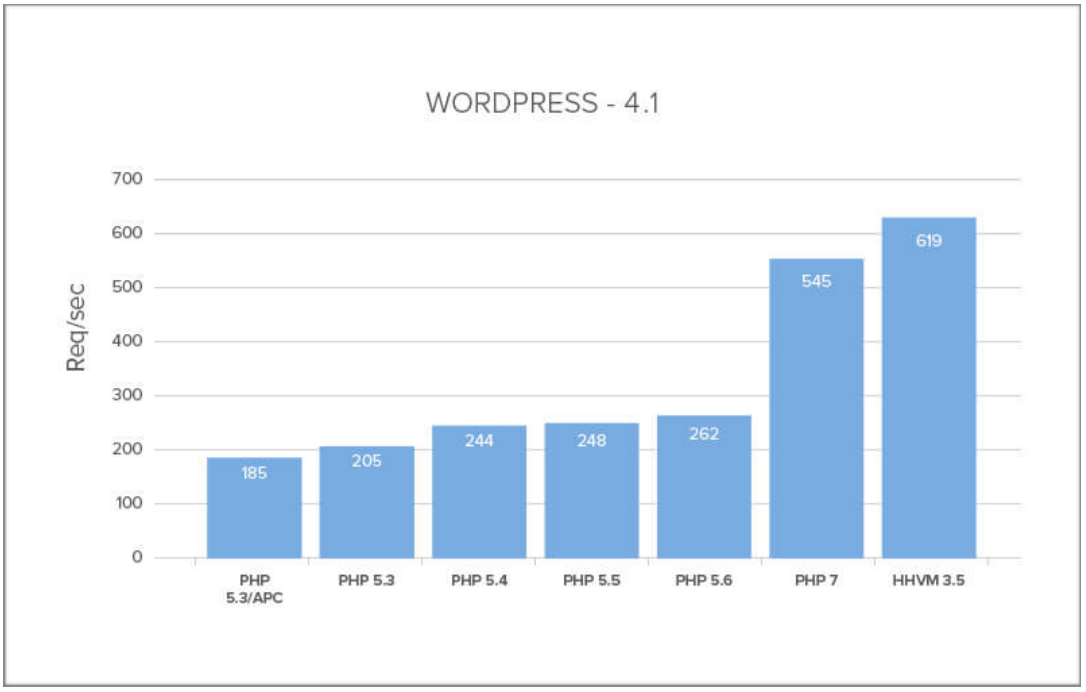
[1] Dane na dzień 1 marca 2017; https://w3techs.com

[2] Dane na dzień 5 kwietnia 2017; https://sucuri.net/security-reports/brute-force/

Zacznij od odpowiedniego hostingu

Serwer, na którym umieścisz swoją witrynę to podstawa. Zadbaj o to, aby zapewniał on separację różnych domen, dzięki czemu w przypadku zaatakowania jednej z Twoich stron złośliwe oprogramowanie nie będzie miało możliwości przeniesienia się na inne witryny. Jest to ważny element nawet, jeśli planujesz uruchomić tylko jedną witrynę – wraz z rozwojem Twojego biznesu marketing może wymagać uruchomienia drobnych stron produktowych lub tzw. *landing page*. Aspekt separacji uznaj za środek zapobiegawczy, o który nie będziesz musiał martwić się w przyszłości.

Kolejnym i nie mniej ważnym elementem jest wersja PHP obsługiwana przez Twój hosting. Najnowszą wersją jest 7.1.3[3] i takiej powinieneś używać. Jest ona o wiele wydajniejsza od PHP w wersji 5.x, czy wcześniejszych.[4]



[3] Wydany 16 marca 2017

[4] Wykres z: https://www.digitalocean.com/company/blog/getting-ready-for-php-7/

Zacznij od odpowiedniego hostingu

Czy Twój hostingodawca wykonuje kopie zapasowe? To bardzo ważne, a im częściej kopia zapasowa jest zapisywana, tym lepiej – raz dziennie to absolutne minimum. Jednak pomimo tego, że kopie zapasowe wykonywane są bezpośrednio na serwerze, to warto też wykonywać je ręcznie i pobierać na swój komputer, na przykład raz na tydzień. Dzięki temu masz pewność, że dane zgromadzone w Twojej witrynie są bezpieczne nawet jeśli firma zarządzająca serwerem zawiedzie.

Jeśli wykonywanie samodzielnych kopii poprzez FTPS lub SFTP oraz program do obsługi baz danych przekracza Twoje kompetencje, to dobrym pomysłem może okazać się użycie jednej z wtyczek ułatwiających wykonywanie kopii. Najpopularniejsze to *UpdraftPlus WordPress Backup Plugin* czy *BackWPup – WordPress Backup Plugin*.

Łącząc się ze swoim serwerem używaj SFTP, lub FTPS – FTP nie jest zalecanym protokołem ze względów bezpieczeństwa, ponieważ nie wspiera szyfrowania transferu.

Polityka haseł

Zakładanie konta w firmie hostingowej to pierwszy moment podczas tworzenia nowej strony, kiedy musisz zastanowić się jakie hasło wybierzesz. W tym momencie warto ustanowić *politykę haseł*, a więc coś, co jest swego rodzaju metodologią tworzenia haseł. Pamiętaj, że każde z nich powinno być długie na przynajmniej osiem znaków, składać się z wielkich i małych liter, cyfr, oraz znaków specjalnych, takich jak $, @ czy #. Dodatkowo wszystkie Twoje hasła powinny być unikalne, żadne z nich nie może brzmieć tak samo dla dwóch różnych usług. Ważne jest również, aby nie miały one sensu logicznego – nie mogą składać się ze słów występujących w słownikach, czy ciągów cyfr układających się w daty urodzenia czy numery telefonu. Powinny być złożone z losowo wybranych, nie mających ze sobą związku znaków.

Polityka haseł to również sposób przechowywania ich, oraz częstotliwość zmian. Idealnie byłoby, gdybyś wszystkie hasła po prostu zapamiętał, ale to nie zawsze jest możliwe. Jeśli musisz je zapisać to przechowuj je w miejscach, do których tylko Ty masz dostęp i zmieniaj przynajmniej raz na miesiąc.

Zastanów się również, czy hasło skojarzone z Twoją pocztą e–mail wpisuje się w tę politykę, a jeśli nie – zmień je.

Konfigurowanie bazy danych

Podczas konfigurowania bazy danych zadbaj, aby dostęp do niej był możliwy jedynie z *localhost* oraz ewentualnie Twojego adresu IP – *wildcard* jest niedopuszczalny. Ponadto postaraj się, aby nazwa użytkownika i nazwa tabeli były różne – technicznie nie jest to zabezpieczenie, jednak niektóre z robotów automatycznie atakujących nie będą „spodziewały się" takiego rozwiązania. W niektórych przypadkach ten prosty zabieg może uchronić Cię przed wyciekiem danych. Hasło dostępowe musi być zgodne z ustaloną wcześniej polityką.

Instalacja WordPressa

Firmy hostingowe udostępniają skrypty instalujące różne CMSy, w tym WordPressa, jednak ze względów bezpieczeństwa nie powinieneś z nich korzystać. Pobierając WP za każdym razem ściągaj najnowszą stabilną wersję ze strony https://wordpress.org/download/release-archive/, a po pobraniu weryfikuj sumy kontrolne z sumami udostępnianymi na tej samej stronie. Dzięki temu unikniesz ryzyka ataku *man in the middle*, który w konsekwencji mógłby spowodować zainfekowanie Twojej strony złośliwym oprogramowaniem już na etapie instalacji.

Podczas instalacji wymyśl własny prefiks tabeli – na przykład *mojpref_* zamiast *wp_*. Podobnie jak w przypadku tworzenia bazy danych – nie jest to zabezpieczenie samo w sobie, ale pomoże się ochronić przed wyciekiem danych w niektórych przypadkach.

Nazwa użytkownika w systemie WordPress powinna być trudna do zgadnięcia. Słowo *administrator*, *admin*, czy nazwa firmy nie są dobrym pomysłem – lepiej wykorzystać swój pseudonim z czasów szkolnych, lub po prostu imię. Hasło powinno być zgodne z polityką.

wp-config.php

Po instalacji zajmij się zmianą kluczy służących do solenia haseł w pliku *wp-config.php*. Nowe klucze wygenerujesz skryptem na stronie https://api.wordpress.org/secret-key/1.1/salt/ – skopiuj je i zamień na te zapisane w Twojej instancji WP.

W tym samym pliku znajdziesz definicje danych logowania do bazy danych. Warto je przenieść do innego, stworzonego przez Ciebie pliku PHP i dodać w oryginalne miejsce przy użyciu *require_once();*

Kolejnym krokiem jest znalezienie linijki *define('WP_DEBUG', false);* i dopisanie zaraz za nią *ini_set('display_errors', 0);* . Jest to ważne, ponieważ włączone informacje o błędach ułatwiają znalezienie luk bezpieczeństwa.

Dopisz również *define('DISALLOW_FILE_EDIT', true);* – edytor plików bywa wygodny w użyciu, ale może być ułatwieniem dla hakera, który zdobył dostęp do panelu administracyjnego.

.htaccess

Zablokuj możliwość odkrycia loginów użytkowników zarejestrowanych w Twojej kopii WP:

```
RewriteCond %{QUERY_STRING} author=\d
RewriteRule ^ /? [L,R=301]
```

Warto również zadbać o zablokowanie plików *.php* w ramach katalogów *wp-includes* oraz *wp-content*, z wyjątkiem *wp-tinymce.php* oraz *ms-files.php*.

Ukrywanie wersji

Przy użyciu pliku *.htaccess* zablokuj dla wszystkich dostęp do plików *readme.html*, *wp-config.php*, a w *wp-config.php* lub *functions.php* motywu dopisz:

```
remove_action('wp_head', ,wp_generator');
function wpsec_msg( $generator, $type ) {
      return '';
}
add_filter( 'the_generator', 'wpsec_msg', 10, 2 );
function wpsec_rsv( $src ) {
      global $wp_version;

      $version_str = '?ver='.$wp_version;
      $offset = strlen( $src ) - strlen( $version_str );

      if ( $offset >= 0 && strpos($src, $version_str, $offset) !==
FALSE )
            return substr( $src, 0, $offset );

      return $src;
}
add_filter( 'script_loader_src', 'wpsec_rsv' );
add_filter( 'style_loader_src', 'wpsec_rsv' );
```

Zabezpieczenie logowania

Powszechną praktyką jest zmiana lokalizacji pliku *wp-login.php*. Nie jest to dobre rozwiązanie – istnieją liczne sposoby na odnalezienie tak ukrytego panelu logowania. O wiele rozsądniejszym jest dodanie kolejnej warstwy autoryzacji przy użyciu *.htpasswd*, co warto zrobić – tak, aby dostęp do *wp-login.php* i *wp-admin* wymagał autoryzacji bezpośrednio na serwerze HTTP. Należy jednak pamiętać o odblokowaniu *admin-ajax.php* oraz *admin-post.php* znajdujących się w tym katalogu.

Warto również zablokować dostęp do pliku *xmlrpc.php*, o ile nie jest Ci on potrzebny do – na przykład – zarządzania stroną z poziomu zewnętrznego narzędzia.

Instalacja motywów oraz wtyczek

Motywy oraz wtyczki to wspaniałe narzędzia, które pozwolą spersonalizować i niemal dowolnie dostosować witrynę do Twoich potrzeb, jednak ważnym aspektem jest źródło ich pochodzenia. Instaluj zasoby wyłącznie z zaufanych źródeł, takich jak katalog WordPressa dostępny z poziomu panelu administracyjnego, czy sklepy polecane przez społeczność WordPressa.

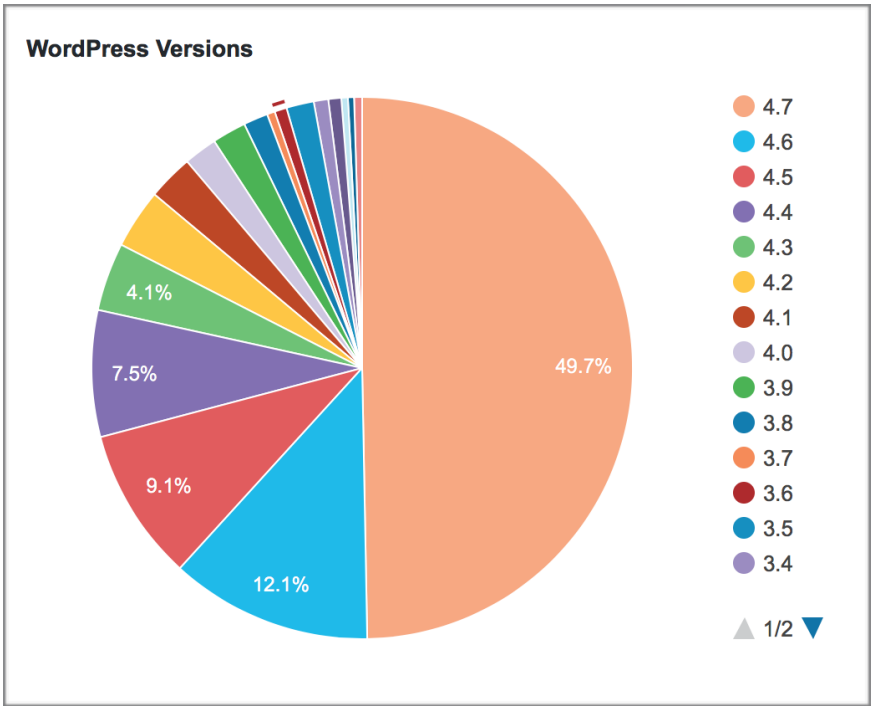
Instalując pirackie oprogramowanie z nielegalnych źródeł narażasz się na zainstalowanie wraz z nim szkodliwych skryptów – ze względów bezpieczeństwa jest to niedopuszczalne.

Aktualizacje WordPressa, motywów oraz wtyczek

Aktualizowanie WP jest jedną z najważniejszych czynności podczas jego używania. Błędy wykrywane przez społeczność są korygowane i udostępniane w kolejnych wydaniach, dlatego aktualizacji nie należy odkładać na później.

Przed przystąpieniem do aktualizacji warto zrobić kopię zapasową strony. Ważnym aspektem przeprowadzanych aktualizacji jest nie tylko kliknięcie przycisku uruchamiającego pobranie i instalację nowej wersji, ale przede wszystkim zadbanie o kompatybilność. Upewnij się, że motyw oraz wtyczki z których korzystasz wspierają już najnowszą wersję WP, a jeśli to możliwe zaktualizuj je do najnowszych wersji. Warto też śledzić fora czy strony poświęcone WordPressowi żeby mieć pewność, że najnowsze wersje używanego oprogramowania działają sprawnie. Jeśli społeczność zauważy, że któraś część programu działa nieprawidłowo zaraz zrobi się o tym głośno.

Kiepskim pomysłem jest włączenie automatycznych aktualizacji. Jest to możliwe jednak któregoś razu może się okazać, że Twoja strona po prostu nie działa i nie będziesz wiedział dlaczego.

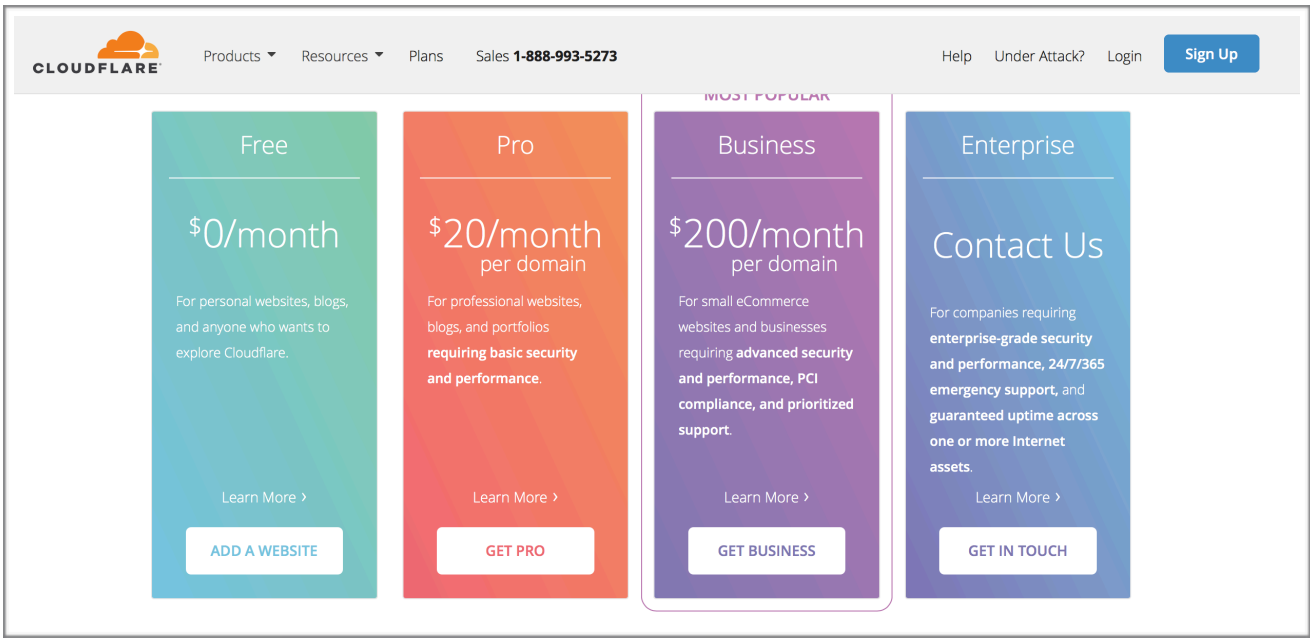


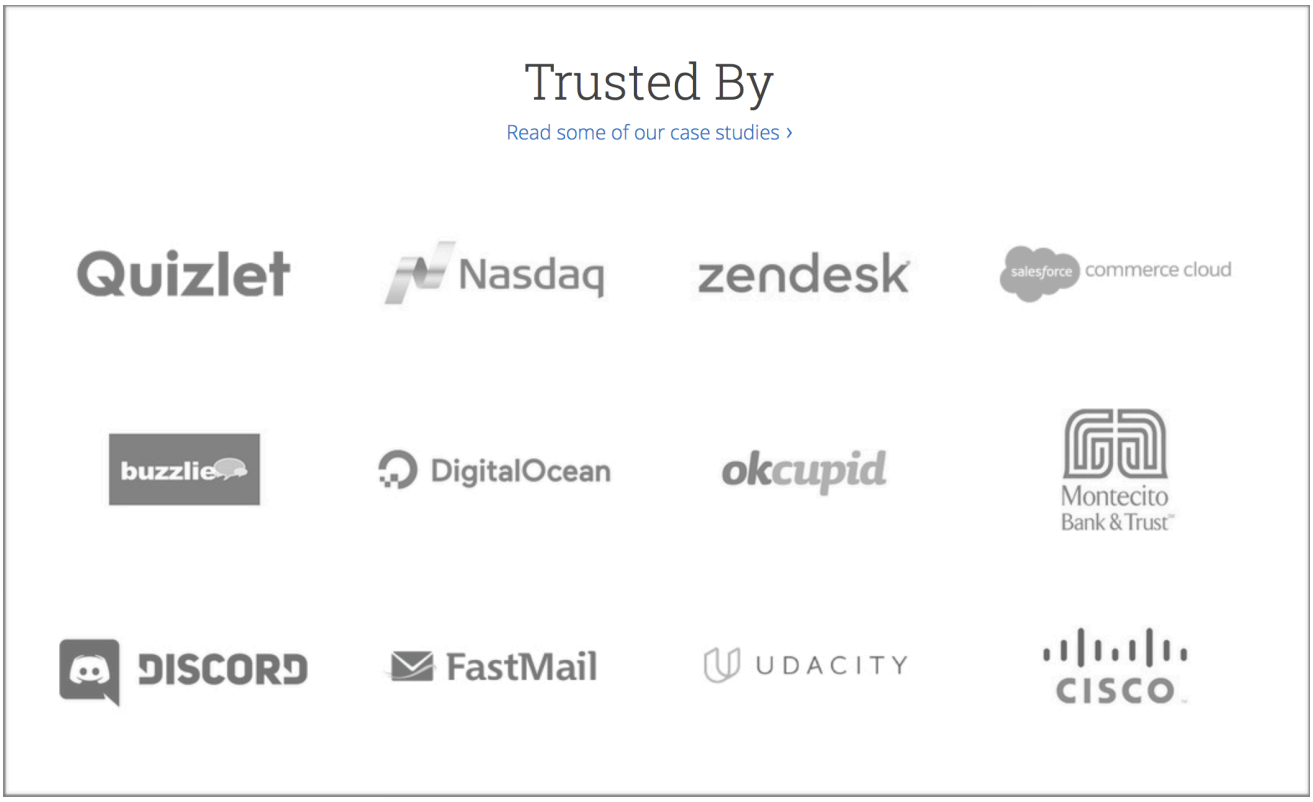
Ponad połowa stron opartych o WordPress w Internecie jest nieaktualna[5].

[5] Dane na dzień 6 kwietnia 2016; https://wordpress.org/about/stats/

Cloudflare

Skonfigurowanie Cloudflare jest bardzo proste, a może przynieść wymierne korzyści. W darmowym planie do dyspozycji mamy certyfikat SSL, który zabezpieczy połączenie pomiędzy użytkownikiem końcowym, a serwerami Cloudflare, a ponadto jesteśmy chronieni przed atakami (D)DoS. Dodatkowo niewątpliwym atutem jest CDN, który przyspieszy ładowanie naszej strony dzięki cacheowaniu obrazów i skryptów na szybkich serwerach rozsianych po całym świecie.





POTRZEBUJĘ NATYCHMIASTOWEJ POMOCY

Czy teraz moja strona jest bezpieczna?

Nie. Zabezpieczanie to proces ciągły, ponieważ kod Twojej strony jest ciągle analizowany przez przestępców, którzy codziennie odnajdują nowe podatności. Wracaj do lektury tego e–booka co tydzień i ponownie przechodź przez wszystkie etapy. Dopiero zapewnienie ciągłej higieny pozwoli Ci mieć poczucie, że Twoja witryna jest zabezpieczona w sposób prawidłowy.

Kliknij w przycisk poniżej, aby dodać przypomnienie do kalendarza.

PRZYPOMNIJ ZA TYDZIEŃ