cyberforces.com

WordPress: najbardziej zhakowany CMS na świecie - Cyberforces

Paweł Wałuszko

8-11 minutes

Bez wątpienia WordPress jest najpopularniejszym systemem zarządzania treścią (CMS) w ostatnich latach. Według najnowszych statystyk W3Techs, w pierwszym kwartale 2019 roku WordPress posiadał około 60% udziału w całym rynku platform CMS.

Dla porównania skali przewagi WordPressa nad konkurencją warto jest zauważyć, że inne platformy – takie jak Joomla i Drupal – łącznie stanowią mniej niż 7% instalacji CMS na świecie. Natomiast Shopify, Squarespace czy Wix oscylują w granicach 2-3%. [1]

Trudno się nie dziwić. WordPress posiada wiele zalet, przez które de-facto stał się domyślnym wyborem CMS, gdy o tej kategorii wspominamy. Jest prosty w obsłudze, posiada wiele gotowych szablonów, a rozbudowanie funkcjonalności jest tak proste, jak włączenie wtyczki. Warto jest też dodać, że sam w sobie WordPress jest dość stabilnym i bezpiecznym systemem, gdy jest poprawnie zainstalowany.

Niestety, popularność WordPressa również niesie ze sobą pewne konsekwencje. Miliony użytkowników to też niezliczona ilość programistów i osób ingerujących w kod źródłowy. Z jednej strony każdy projekt oparty na licencji open-source posiada te same wady i zalety dotyczące bezpieczeństwa: każdy programista może przeprowadzić własny audyt kodu, sprawdzić jak on funkcjonuje i naprawić potencjalne błędy.

Z drugiej strony WordPress jest systemem na którym obecnie funkcjonuje duża ilość korporacyjnych stron internetowych – czyli stron, które przetwarzają dane osobowe. Jak można się domyślić, niektórzy programiści niekoniecznie są zmotywowani do zgłaszania lub poprawiania potencjalnych problemów dotyczących zabezpieczenia platformy. Rynek handlu danymi osobowymi nieustannie rośnie, a znalezioną lukę można niezacnie wykorzystać.

Statystyki dotyczące bezpieczeństwa

Niestety, tutaj nasza ulubiona platforma dość nieprzychylnie wypada. Według badań Sucuri przeprowadzonych w 2017 roku na ponad 34.000 instancjach CMS, WordPress stanowił 83% skompromitowanych instalacji CMS na świecie.[2] Niepokojący też jest fakt, że jest to ciągła, wyraźnie rosnąca tendencja. Dla

przykładu, w raporcie z 2019 r. ta liczba już osiągnęła 90%.[3]

Problemy

Czytając wyżej wymienione statystyki można byłoby dojść do wniosku, że WordPress jest nieadekwatnie zabezpieczoną platformą, lub jest niepoprawnie zaprojektowany.

Nic nie jest jednak bardziej odległe od prawdy. WordPress jest projektem o otwartym kodzie źródłowym, sprawdzanym i udoskonalanym w każdej wersji przez setki programistów i ekspertów ds. bezpieczeństwa. Ale sam fakt, że aktualizacje są regularnie publikowane nie znaczy, że są wdrażane przez administratorów – i tutaj nawiązujemy do pierwszego problemu.

Po pierwsze, należy zauważyć, że w badaniu opublikowanym w 2019 r. prawie 40% skompromitowanych instalacji posiadało nieaktualną wersję WordPressa.

Rok po roku, jedną z głównych przyczyn kompromitacji bezpieczeństwa systemów WordPress jest jego przestarzała wersja nadal obsługująca strony internetowe.

Dla niektórych administratorów może to być prosty fakt zaniedbania. Filozofia „nie naprawiaj tego, co nie jest zepsute” z pewnością jest nam dobrze znana, a systemów w przeciętnej firmie jest wiele.

Jednakże, mogą też istnieć przyczyny technologiczne, które uniemożliwiają uruchamianie aktualizacji platformy – choćby niekompatybilność wtyczek z nową wersją CMS’a – i tutaj nawiązujemy do drugiego problemu bezpieczeństwa WP.

Wtyczki często tworzą problemy.

Uruchomienie zbyt wielu wtyczek WordPressa niesie ze sobą wiele negatywnych następstw: szybciej wykorzystujemy zasoby naszych serwerów, spowalniamy czas renderowania naszej strony i konsekwentnie tracimy miejsce w rankingu wyszukiwarek internetowych. Niestety, do wad musimy też zaliczyć liczne problemy z bezpieczeństwem systemu spowodowane właśnie przez nasze ulubione wtyczki.

Aby uświadomić sobie na czym polega problem wtyczek, wystarczy sobie opisać, czym one są. Krótko mówiąc, wtyczki to kawałki kodu stworzone przez programistów na całym świecie, które rozbudowują funkcjonalność naszego systemu. Poprzez instalację stają się integralną częścią systemu i posiadają dostęp do wielu zasobów. Choć istnieją standardy dotyczące produkowania wtyczek, każdy programista posiada własną logikę i filozofię programowania – i tu pojawiają się problemy związane z ich bezpieczeństwem.

Z jednej strony zespół WP manualnie sprawdza każdą wtyczkę przed dodaniem do oficjalnego *Katalogu wtyczek WordPressa*. Z drugiej strony, mimo wstępnego audytu, użytkownicy nadal zgłaszają naruszenia bezpieczeństwa do zespołu WP, który po weryfikacji problemu kontaktuje się z autorem w celu naprawienia problemu.[4] Taki proces może poskutkować albo aktualizacją wtyczki, albo usunięciem z oficjalnego Katalogu. Tymczasem problematyczna wtyczka pozostaje włączona na serwerach osób, które ją zainstalowały.

Jak widać, mimo tak dużego nakładu pracy, bezpieczeństwo wtyczek nie jest stuprocentowe i prawdopodobnie nigdy nie będzie. Jest to spowodowane samą

ilością wtyczek, różnych ich konfiguracji i konfliktów które mogą wywołać, gdy są połączone z innymi wtyczkami. Ponadto nie każdy administrator dba o aktualizacje, mimo licznych powiadomień o ich dostępności.

Ostatnim, ale niemniej ważnym elementem jest brak trzymania się zasad bezpieczeństwa podczas instalacji i w trakcie zarządzania systemem.

Model „set it and forget it" może lepiej pasuje do obsługi termostatu, niż do prowadzenia korporacyjnej strony internetowej. Niestety, jednym z głównych przyczyn kompromitacji bezpieczeństwa w systemie WordPress jest brak tak-zwanego „security hardening", czyli utwardzania systemów. Dotyczy to m. in. błędów takich jak ustawiania łatwych do odgadnięcia haseł, błędnej lub niekompletnej konfiguracji infrastruktury back-end, czy braku certyfikatów SSL na stronach logowania.

Jak się zabezpieczyć?

Oszałamiająca liczba skompromitowanych instalacji WordPressa nie jest wskaźnikiem braku bezpieczeństwa tej platformy, tylko prostych do skorygowania błędów. Zainwestowanie odrobiny czasu w poprawne uruchomienie projektu opartego na WordPressie z pewnością pozwoli nam uniknąć bycia cytowanym w wyżej wymienionej 90. procentowej statystyce.

1. Jeśli to możliwe, zaktualizuj wtyczki i WordPress do najnowszej wersji.

Chociaż mogą istnieć problemy ze zgodnością typu wtyczka-WordPress które najpierw należy rozwiązać, zawsze najlepiej jest utrzymywać najnowszą wersję WordPressa na naszych serwerach. To samo dotyczy najnowszych aktualizacji wtyczek. Nawet jeśli drobne aktualizacje mogą nie przynosić żadnych zmian wizualnych (takich jak wprowadzenie edytora Gutenberga w WP), zmiany w back-endzie mogą być istotne i nie powinny być ignorowane.

2. Zminimalizuj swoją zależność od wtyczek.

Choć są bardzo wygodne i praktycznie działają po jednym kliknięciu, wtyczki WordPress w dużej mierze są odpowiedzialne za problemy z bezpieczeństwem całej platformy. O ile to możliwe, używajmy bardzo ograniczonej ilości wtyczek i instalujmy te, które mają największą szansę na aktualizacje w przyszłości.

3. Pamiętajmy o dobrych praktykach bezpieczeństwa podczas instalacji i aktualizacji systemów.

Od używania silnych haseł do przenoszenia adresu URL /wp-admin do innej lokalizacji, lista dobrych praktyk jest bardzo długa.

Jeśli nie jesteś pewny, czy Twój WordPress jest zabezpieczony, istnieje wiele eksperckich samouczków (tutorials), począwszy od *Hardening WordPress* na WordPress.org. Ponadto istnieją wtyczki zwiększające bezpieczeństwo, które pomagają aktywnie blokować skrypty i ataki – choć z wtyczkami warto jest zachować ostrożność.

Na koniec warto jest wspomnieć o zewnętrznych systemach filtrujących dostęp do naszej strony przez technologie takie jak reverse proxy. Używając czarne listy oraz

metody wykrywania ataków, usługi reverse proxy są w stanie „odfiltrować” zły ruch od dobrego, tym sposobem chroniąc naszą stronę przed hackerami.

Nadal posiadasz pytania lub nie jesteś pewny jak wdrożyć wymienione praktyki? Jako firma zajmująca się bezpieczeństwem systemów, służymy konsultacją i pomocą.

1. https://w3techs.com/technologies/history_overview/content_management
2. https://sucuri.net/reports/Sucuri-Hacked-Report-2017.pdf
3. https://blog.sucuri.net/2019/03/hacked-website-trend-report-2018.html
4. https://developer.wordpress.org/plugins/wordpress-org/plugin-security/