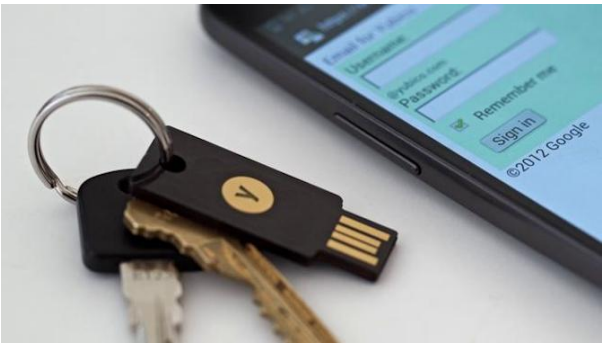

CZY TWARDOŚĆ MA ZNACZENIE?

Posted on 6 listopada 2013 by Maciej Cybulski

Categories: aktualności, bezpieczeństwo, dla początkujących, porady, Slider

31.V.2013 wykryty został błąd w *class-phpass.php* pozwalający zdalnemu użytkownikowi, po odpowiednim spreparowaniu ciasteczka, doprowadzić do załamania działania strony, poprzez nagły wzrost użycia pamięci i procesora, czyli klasyczny przykład ataku odmowy usług - DoS. Naprawa błędu skutkowała wydaniem WordPressa w wersji 3.5.2

Inne ważne błędy zauważono w WordPressie wersji 3.6, gdzie uwierzytelnieni użytkownicy mogli w specyficznych warunkach podwyższyć sobie poziom uprawnień i wykonać dowolny kod na stronie. Reakcja społeczności WordPress była praktycznie błyskawiczna. Kilka dni później (11 września) pojawiła się aktualizacja 3.6.1 likwidująca tę podatność oraz kilka innych zauważonych w międzyczasie.
Inne ważne podatności i skuteczne ich wykorzystanie przez intruzów to np. zauważony 15 kwietnia 2013 **exploit, który umożliwiał przejęcie kontroli nad instalacją WordPressa** jeśli w systemie był standardowy użytkownik "Admin". Zostało to odkryte przez społeczność WordPress po tym, gdy 11 kwietnia zauważono zmasowane ataki BruteForce, w wyniku których włamywacze budowali olbrzymią sieć typu Botnet.
Czy zatem WordPress jest bezpieczny? Czy świadomość tego, że platforma WordPress nie jest rozwiązaniem idealnym i 100% bezpiecznym powinna odstraszać nas od stawiania stron na niej? **Rozwój WordPressa w międzyczasie mocno przyspieszył**. Od 11 września kiedy pojawiła się

wersja 3.6.1 pojawiły się już dwie aktualizacje 3.7 (24 października) i 3.7.1 (29 października).

Zastanówmy się zatem jak wygląda zapewnienie bezpieczeństwa i najczęstsze błędy z nim związane.

Intruz na naszą stronę może dostać się na kilka sposobów. **W 90% przypadków słabym ogniwem jest człowiek a dokładniej niefrasobliwość i grzech zaniechania.**
Podatności na włamanie mogą tkwić w:

1. **środowisku w którym pracuje WordPress** - na hostingu - użytkownik ma mały wpływ na te podatności, jednak firmy hostingowe nie mogą sobie pozwolić na błędy w tej materii, zatem prawdopodobieństwo wystąpienia podatności w tym zakresie jest minimalne.
2. **samym jądrze WordPress'a** - podatności likwidowane najczęściej w kilka dni po ich wykryciu
3. **wtyczkach -** likwidacja podatności jest uzależniona od autora wtyczki
4. **motywach -** podobnie jak we wtyczkach, likwidacja jest uzależniona od szybkości reakcji autora. Jednak stosowanie się do wytycznych WordPressa (codex) podczas tworzenia motywu zapewnia w większości przypadków podstawowe bezpieczeństwo. **Warto zatem instalować komercyjne motywy ze sprawdzonego źródła**, gdzie możemy być pewni jakości i bezpieczeństwa kodu. Najczęściej firmy piszące motywy reagują równie szybko na wykryte podatności jak Team WordPress'a.
5. **bezpieczeństwo zdalnego użytkownika** - najczęstszy problem, brak antywirusa na komputerze użytkownika, brak bezpiecznego połączenia z panelem logowania, transfer za pomocą FTP, stosowanie prostych haseł.

Oczywiście najczęściej na stronach występuje wypadkowa wszystkich tych czynników.
W naszych rozważaniach możemy praktycznie pominąć punkt 1) skupimy się na tym co od nas, właścicieli strony www, zależy.

Jak własnoręcznie zapobiec włamaniu?

Popatrzymy na statystyki. Tylko *60% wszystkich witryn WordPressa jest zaktualizowana do najnowszej wersji*, co znaczy, że reszta, czyli *40% instalacji WordPress* korzysta z wcześniejszych *potencjalnie niebezpiecznych jego wersji*. Mamy tu ewidentną podatność z punktu 2, jednak zawinioną przez właściciela/użytkownika.

- W internecie obecnie pracuje ponad **670 milionów stron** z czego ponad 10% korzysta z WordPressa
- W każdej minucie atakowane jest kilkaset tysięcy adresów IP. Biorąc pod uwagę fakt, że bardzo dużo instalacji WordPress'a przeprowadzanych jest na hostingach współdzielonych (czyli na jednym IP może być kilkaset instalacji WordPressa) potencjalnie daje nam to już zupełnie inną skalę ataku.
- Atakowane są różne IP, czyli potencjalnie również ten który kieruje do Twojego serwera.

Jak sobie radzić z tym faktem?

Najlepszą formą ochrony jest prewencja, czyli właściwe zabezpieczenie strony, tworzenie kopii zapasowych, monitorowanie zmian i ataków.

Właściwe zabezpieczenie strony to temat bardzo szeroki, jednak w własnym zakresie można bardzo znacząco podnieść jej bezpieczeństwo stosując "utwardzenia" na trzech obszarach działania:

1. **Kontrola**
2. **Ograniczanie**
3. **Plan działania**

KONTROLA

By kontrolować co dzieje się na i z naszą stroną trzeba na początek ograniczyć ilość potencjalnych "punktów wejścia" do systemu.

- *dostęp do systemu plików* - **kopiowanie plików** na i z serwera - do tego celu używamy protokołów SFTP lub FTPS zamiast FTP. Protokoły SFTP i FTPS umożliwiają, w przeciwieństwie do protokołu FTP, nawiązanie szyfrowanego połączenia z naszym zdalnym serwerem. Zatem nasz login i hasło nie jest możliwy do podsłuchania. Dodatkowo protokół SFTP pozwala zamiast hasła użyć klucza PKI co znacznie podwyższa standard bezpieczeństwa. Nie każdy hosting umożliwia stosowanie protokołów z szyfrowaniem transmisji zatem nie zawsze możemy to rozwiązanie zastosować.
- *dostęp do systemu plików* - bezpieczeństwo zdalnego użytkownika - bardzo częstym i nadal spotykanym błędem jest... **brak aktualnego dobrego programu antywirusowego na komputerze z którego łączymy się z naszym hostingiem.**
- *dostęp do zaplecza /wp-login/* - jeśli możliwe, stosujemy wymuszenie połączenia przez www z

wykorzystaniem protokołu SSL. Wymaga zakupu certyfikatu SSL dla naszej strony. Możemy też uzupełnić panel logowania o systemy sprzętowej autoryzacji dostępu 2FA, działający na zasadzie haseł jednorazowych.
- *dostęp do systemu plików* - **uprawnienia.** Tutaj stosujemy zasadę - użytkownik powinien mieć najniższe możliwe uprawnienia niezbędne do poprawnej pracy.
  I tak:

- */ katalog główny* WordPress - dostęp - tylko Ty - poza nielicznymi wyjątkami
- */wp-admin/* - dostęp - tylko Ty
- */wp-includes/* - dostęp - tylko Ty
- */wp-content/* - dostęp - Ty oraz serwer
- */wp-content/themes/* - dostęp - Ty. Tutaj powinniśmy też pomyśleć o wyłączeniu możliwości edycji plików z poziomu WordPressa
- */wp-content/plugins/* - dostęp - Ty

Ciekawym i rzadko stosowanym zabezpieczeniem jest **przeniesienie pliku *wp-config.php* do katalogu nadrzędnego lub/i zablokowanie go użyciem konfiguracji .htaccess**

- *dostęp do systemu plików* - blokada bezpośredniego dostępu do plików PHP - tak by mimo znajomości nazwy i adresu pliku nie było możliwości wywołania go z dowolnymi parametrami bezpośrednio z przeglądarki
- *dostęp do Bazy Danych*
  - separacja bazy danych - stosujemy dla WordPressa dedykowaną bazę danych, w której stosujemy różne ciągi znaków dla nazwy bazy, użytkownika i hasła.
  - zmiana prefixu tabel z domyślnego wp_ na inny
  - modyfikacja stałej w pliku wp-config.php
- *dostęp do panelu administracyjnego*
  - po domyślnej instalacji WordPressa zaloguj się i utwórz konto o poziomie dostępu Administrator, następnie zaloguj się na nim i usuń konto o loginie "admin". Konto "admin" jest najczęstszym celem ataków BruteForce.
  - dodaj do */wp-admin/* autoryzację BasicAuth z użyciem .htaccess i .htpasswd
  - nie zapomnij udostępnić *admin-ajax.php*
  - używaj wtyczek blokujących nieudane logowania
  - w systemie powinieneś mieć min. 2 konta. Do publikowania treści stosuj *wyłącznie konta z uprawnieniami innymi niż "Administrator"*. **Konto o poziomie uprawnień "Administrator" stosuj wyłącznie do prac administracyjnych**. W ten sposób

unikniesz przypadkowego ujawnienia Twojego loginu do konta administratora.

OGRANICZANIE

Jak ktoś się już przebije przez zabezpieczenia to co dalej? Konfiguracja systemu powinna minimalizować ilość groźnych operacji po uzyskaniu nieuprawnionego dostępu.
Co zatem zrobić? :

- miej zawsze **aktualną** wersję WordPressa
- miej zawsze aktualne wersje wtyczek, *nie używane usuwaj*,
- miej zawsze aktualną wersję motywu, *nie używane usuwaj*,
- wyłącz możliwość edycji plików z poziomu panelu WordPressa
- użytkownik MySQL powinien mieć dostęp tylko do bazy z tabelami WordPress'a

PLAN DZIAŁANIA

na każdą sytuację powinnismy mieć scenariusz, by w możliwie krótkim czasie móc skutecznie zareagować i tak:

- bądź zawsze gotowy na podjęcie akcji w przypadku wystapienia zagrożenia
- bądź gotów na odtworzenie instalacji
- dokonuj regularnych kopii bezpieczeństwa zarówno baz danych jak i plików WordPressa i innych
- im częściej publikujesz tym częściej rób kopie, mniej będziesz musiał odtwarzać po ataku
- wyłącz wyświetlanie błędów PHP
- zbieraj informacje o tym co dzieje się z Twoją stroną, rejestruj błędy, próby nieautoryzowanego dostępu itd...
- obserwuj raporty dziennika zdarzeń systemowych

PREWENCJA

zapewnia największą skuteczność a **MONITORING** "święty spokój"

There are no comments yet.