BEZPIECZEŃSTWO WORDPRESS'A - SŁÓW KILKA CZ. II

Posted on 12 lutego 2013 by Maciej Cybulski

Categories: aktualności, porady

Tag: bezpieczeństwo WordPressa

Kontynuując artykuł z poprzedniego tygodnia dzisiaj bezpieczeństwo WordPress'a w relacji ze środowiskiem z którego się z nim łączymy...

Poprzednio mówiliśmy o zagrożeniach dla Wordpress'a jakim są niepewne źródłach wtyczek i szablonów, oraz brak aktualizacji.

Dzisiaj trochę o bezpieczeństwie programów i przeglądarki.

1. Program FTP

Wielu bardziej zaawansowanych włamywaczy wykorzystuje popularność i brak wystarczającego poziomu bezpieczeństwa niektórych programów w połączeniu z trywialnością haseł.
Wykorzystują oni fakt, że wielu użytkowników w celu ułatwienia sobie pracy włącza w programie możliwość zapamiętania hasła, a często i hasła bywają trywialnie proste.
Przy braku właściwego zabezpieczenia systemu, przejęcie hasła jest tylko kwestią czasu.

WNIOSEK: Stosujemy skomplikowane hasła i nie zapisujemy ich w programach FTP. Najlepiej stosować też, tam gdzie to możliwe, zamiast protokołu FTP, jego szyfrowane wersje SFTP lub SSH. Niektóre z programów umożliwiają też stosowanie 2FA czyli dwuczynnikowego zabezpieczenia, przy pomocy kluczy sprzętowych.
Takie rozwiązanie zdecydowanie podwyższa bezpieczeństwo połączeń.

2.Połączenie SSL

W najprostszych instalacjach WordPressa logowanie do zaplecza wykonywane jest w protokole HTTP gdzie wszelkie informacje przesyłane są otwartym tekstem.
Zatem login i hasło łatwo jest przechwycić. Tam gdzie to możliwe, (a zależy to głównie od konfiguracji serwera) należy włączać możliwość logowania
do zaplecza jedynie w szyfrowanym protokole HTTPS. Wymaga to najczęściej dodatkowej konfiguracji serwera,
jednak wiele hostingów umożliwia wykorzystanie niecertyfikowanego połączenia do naszych celów.
I mimo iż przeglądarka może nam zgłaszać, że certyfikat nie jest zaufany, to przy zrozumieniu mechanizmu można do naszych celów przyjąć, że jest to bezpieczne,
chyba, że chcemy dla naszej domeny wykupić certyfikat SSL wystawiony przez zaufane centrum certyfikacji, wtedy przeglądarka nie będzie zgłaszała nam wątpliwości.
Jednak przy świadomym działaniu nie jest to konieczne, ale więcej o certyfikatach SSL i ich zastosowaniu już niebawem.

There are no comments yet.