BEZPIECZNY WORDPRESS. WPROWADZENIE

Posted on 10 kwietnia 2013 by Maciej Cybulski

Categories: aktualności, bezpieczeństwo

informują, że do 10. kwietnia 2013 (czyli do dzisiaj) postawiono ponad 63 mln witryn na WordPress'ie i liczba ta wciąż rośnie.

Popularność tej platformy spowodowała, że stała się ona też celem dla cyberprzestępców, którzy stosują automaty do kompromitacji wielu stron jednocześnie. Dlaczego automaty i jednoczesny atak?

Z pewnością jednym z czynników jest oczekiwana skuteczność i minimalizacja czasu. Nie każda witryna postawiona na WordPress'ie ulegnie atakowi. Zatem by wyselekcjonować te najbardziej podatne, stosowane są zmasowane synchroniczne ataki.

Czy to oznacza że WordPress jest niebezpieczny lub podatny na włamania?

Absolutnie nie!

Z WordPress'em jest jak z SEO, wzrost pozycji powoduje wzrost popularności zarówno u "tych dobrych" jak i u "tych złych". Zatem i jedni i drudzy coraz częściej zaglądają na popularną stronę. Oczywiście "tych dobrych" jest po prostu więcej :) , co nie zmienia faktu, że często wystarczy jeden

skuteczny włamywacz, by nasza strona przestała już pracować tylko dla nas...

Popularność WordPress'a powoduje, że jest wielu autorów i systemów, które pomagają zapobiegać przedostaniu się złośliwego kodu na strony postawione na WordPress'ie.

Natomiast statystyki też pokazują, że niewiele osób zdaje sobie sprawę z zagrożenia i wie jak sobie z nim radzić (czy to samodzielnie czy zwracając się o pomoc).
Statystyki stopbadware.org informują o prawie 1,5 mln zarejestrowanych przez serwis zainfekowanych stron, z których jedynie nie całe 10% po usunięciu złośliwego kodu zostało usuniętych z "czarnych list".

Zatem jak zapobiegać? Czym jest ten bezpieczny WordPress?

Poniższe kilka ogólnych wskazówek, to podstawowe zasady, którymi należy się kierować dbając o bezpieczeństwo WordPress'a, a których przestrzeganie spowoduje iż nasza strona stanie się bardziej bezpieczna.

- **Pobieraj kod zawsze z zaufanych źródeł** ,czyli najczęściej będzie to Wordpress.org lub strony autorów szablonów czy wtyczek. W przypadku wtyczek i szablonów warto też poczytać opinie użytkowników, bo często one odzwierciedlają stan bezpieczeństwa danego komponentu.
- **Aktualizuj WordPress'a, wtyczki, szablony i skrypty** niezwłocznie po ukazaniu się aktualizacji. Nie zwlekaj. Dotyczy to zarówno samego WordPress'a jak i komponentów strony. Aktualizacja oprogramowania jest jednym z najważniejszych czynników obronnych przeciw kompromitacji strony. Nowe wersje nie tylko dodają nowe funkcjonalności ale też bardzo często zawierają poprawki bezpieczeństwa.
- **Bądź ostrożny i dokładnie sprawdzaj co instalujesz**. Wiele wspaniałych dodatków do WordPress'a jest napisanych i przechowywanych przez autorów, którzy nie są bezpośrednio związani z programistami WordPress.Org i to na nich spoczywa odpowiedzialność za utrzymanie dodatków , ich bezpieczeństwa i aktualności. Jeśli o to nie dbają, to zwiększają podatność na włamanie. Tutaj również opinia klientów/użytkowników jest dobrą wskazówką.
- **Pozbądź się "admina" :)** Utrzymanie domyślnej nazwy użytkownika jako "admin" powoduje, że automat, który próbuje włamać się na naszą stronę, musi jedynie złamać hasło, a to już na samym początku znacznie obniża jakość naszych zabezpieczeń.

- **Korzystaj z wtyczek anty-malware** i innych związanych z bezpieczeństwem, których różnorodność znajdziesz na WordPress.Org. Jest też kilku dostawców systemów do monitoringu i skanowania bezpieczeństwa strony z których usług też warto skorzystać.

To na początek. Niebawem przyjrzymy się dokładniej poszczególnym rozwiązaniom.

There are no comments yet.