BEZPIECZEŃSTWO WORDPRESS'A - SŁÓW KILKA CZ. I

Posted on 5 lutego 2013 by Maciej Cybulski

Categories: aktualności, porady

Przeglądając publikacje z okazji "Dnia Bezpiecznego Internetu" można trafić na różne podejście do tematu. Zatem ja coś dodam też od siebie... czyli jeden z moich ulubionych tematów bezpieczeństwo WordPress'a i ogólnie pojętego bezpieczeństwa IT.

Dziś pierwsza część czyli dwa zagadnienia związane stricte z WordPressem.
Kilka dni temu pojawiła się kolejne wydanie WordPress'a 3.5.1 z sporą ilością załatanych dziur w bezpieczeństwie. No i bardzo dobrze, bo od momentu wydania wersji 3.5, kilka osób zgłaszało do mnie problemy z infekcją stron, które w najlepszym wypadku objawiały się znanym czerwonym ekranem z Googla.

A przynajmniej od czasu ukazania się aktualizacji WordPress'a (a często i wcześniej) do momentu aktualizacji naszej instalacji, po Sieci krążą roboty szukające instalacji niezaktualizowanych, po to by potem na nie przeprowadzić atak z pomocą znanych już (bo niwelowanych przez aktualizację) podatności. Zatem przekonujemy się tu jak niebezpieczną może być... informacja.
Gdy występuje problem z bezpieczeństwem, to najczęściej nie jest to tylko jeden czynnik. Efekt w postaci włamania zawsze ma wiele przyczyn. Co ciekawe, osoby którym włamuje się ktoś na stronę przeważnie są zaskoczone. Dominuje podejście, że przecież ten problem ich nie dotyczy... No bo przecież nie mają nie wiadomo czego na stronie. Nie są żadną "agencją", żeby interesowały się nimi jakieś "anonimowe" grupy... Niby tak... ale...
Zastanówmy się po co ktoś włamuje się na stronę?

Celem może być strona sama w sobie - bo jest podatność - czyli cel "szkoleniowy". Ok tego typu włamania w większości blogów wykonują osoby, które dopiero zaczynają zabawę z "ciemną stroną"... i łatwo sobie z takim włamaniem poradzić stosując metody opisane w "Houston we have a problem"

Jednak najczęściej nikt nie włamuje się na naszą stronę, by ją niszczyć. Cel jest bardziej zakamuflowany. Włamanie ma na celu przejęcie kontroli nad stroną i wykorzystanie strony do dalszych włamań, a kolejne do kolejnych włamań. Uzyskuje się w ten sposób długi łańcuszek powiązanych ze sobą stron, a przy odpowiedniej jego długości "strona początkowa"- autora, staje się trudna do namierzenia.
W takiej sytuacji najczęściej o włamaniach dowiadujemy się przypadkiem, z najdziwniejszych miejsc.

Sytuację taką miałem kilka miesięcy temu. Znajomy napisał do mnie, że dostał informację z... działu bezpieczeństwa jednego z kanadyjskich banków, że na jego blogu wykryto jakąś phishingową aplikację. Po szczegółowej analizie okazało się, że faktycznie jest coś takiego na stronie, głęboko ukryte w strukturze katalogów i... pojawiło się tam kilka miesięcy wcześniej.
Zatem był to przykład włamania, typu "egg drop" - gdzie od "podrzucenia" "jaja" - złośliwego kodu, do czasu jego aktywowania mija jakiś czas, co często myli właścicieli stron, jak też utrudnia oczyszczenie strony z zbędnego kodu - rzadko jaki hosting przechowuje kopię bezpieczeństwa strony dłużej niż tydzień.

Co zatem robić i czego nie robić, aby nie zwiększać podatności na włamania?

1.Szablony i pluginy a bezpieczeństwo WordPress'a.

Jakiś czas temu miałem ciekawą rozmowę z klientem, który chcąc maksymalnie obniżyć koszty wykonania strony wskazał mi, że zamiast kupować szablon i wtyczki na stronie sklepów, czy twórców znalazł stronę, na której dostępne są te same szablony premium za free... No faktycznie dać za szablon 80$ a uzyskać go za free, to często w wykorzystaniu niskobudżetowym, prywatnym bloga, jest nie lada pokusą. Jednak szybko okazało się, że szablon może wygląda ok, działa tak samo jak oryginalny, jednak ma pewną "funkcjonalność", której nie ma oryginał. Porównałem kod oryginalnego szablonu, z tym który wskazał klient z "bezpłatnego" źródła. Różnica była w tym, że ten z bezpłatnego źródła posiadał kilka linijek zahaszowanego kodu, który pozornie wydawał się niegroźny. Oczywiście system bezpieczeństwa alarmował, ale... "klient ma zawsze rację" .
Po kilku tygodniach od instalacji, okazało się, że niestety strona jest zainfekowana - uaktywnił się zahaszowany kod, dając dostęp jego autorom do praktycznie całego kodu strony.
Rozpoznanie zagrożenia i oczyszczenie strony niestety okazało się bardziej kosztowne, niż legalny zakup szablonu.
Zatem najczęściej to co wydaje się nam oszczędnością, tylko pozornie nią jest.

WNIOSEK: nigdy nie instaluj oprogramowania, które pochodzi z podejrzanego źródła, lub jest podejrzanie tanie. Dotyczy to zarówno oprogramowania związanego z WordPressem jak i jakiegokolwiek innego oprogramowania. Najbezpieczniejszym źródłem szablonów i pluginów jest oficjalne repozytorium WordPressa lub oficjalne sklepy- choćby te z naszego panela bocznego.

2.Brak aktualizacji.

Temat ten był już opisywany przeze mnie w artykule "Houston we have a problem". Co jakiś czas na kokpicie WordPressa pojawiają się nam informacje, że mamy do zaktualizowania czy to wtyczki czy szablon , czy samego WP. Olbrzymim błędem jest bagatelizować te komunikaty.
Zaktualizowana wersja platformy WordPress, to tylko część sukcesu. Niestety brak aktualizacji bezpieczeństwa systemu na komputerze, czy bazy wirusów w programie antywirusowym powoduje nie mniejsze zagrożenie.
WNIOSEK: Wykonujemy możliwie szybko aktualizacje pluginów, szablonów, WordPressa, ale też aktualizacji krytycznych i bezpieczeństwa systemu (Windows).

Już w przyszłym tygodniu kolejna część czyli o bezpieczeństwie troszkę szerzej.

Tym czasem zapraszam do dyskusji...

There are no comments yet.