Zabezpieczenie WordPressa – Checklista

Dotyczy serwisu/serwera: .....

Osoba sprawdzająca: .....

Operacja	TAK/NIE	Data weryfikacji
Czy WordPress jest aktualny? (1)		
Czy wszystkie zainstalowane wtyczki są aktualne? (2)		
Czy wykorzystywane są popularne i zaufane wtyczki? (3)		
Czy są jakieś nieużywane wtyczki? Należy je usunąć. (11)		
Czy istnieją nowsze, lepsze wersje używanych wtyczek? (11)		
Wprowadzono „solenie" haseł? (4)		
Czy używane hasło dostępowe jest unikalne, złożone i zmieniane regularnie? (5)		
Czy wykorzystywany jest mechanizm 2FA? (16)		
Czy wprowadzono dodatkowy basic auth (.htaccess) do panelu? (7)		
Położenie panelu WP jest nietypowe i unikalne? (6)		
Zablokowano dostęp do wp-includes? (8)		
Zablokowano dostęp do pliku konfiguracyjnego WP? (9)		
Czy includujemy zewnętrzne pliki styli? Czy są to pewne miejsca i bezpieczne? (12)		
Czy wprowadzono blokadę przed przeglądaniem zawartości katalogów przez przeglądarkę? (13)		
Czy zmieniono domyślny prefiks dla tabel w bazie danych? (15)		
Czy wprowadzono mechanizm reCaptcha? (17)		
Zweryfikowano uprawnienia na plikach? (18)		
Wyłączono raportowanie błędów w przeglądarce? (19)		
Wyłączono lub skutecznie zabezpieczono xml-rpc? (20)		
Ograniczono ilość błędnych logowań poprzez wprowadzenie blokady po kilku nieudanych próbach? (21)		
Przeszkolono Redakcję, aby nie umieszczała w ramach WP plików ani danych zawierających krytyczne dane? (22)		

*Wyjaśnienie wszystkich pojęć z tabeli można przeczytać TUTAJ

UWAGI: