

Odkryj techniki zabezpieczania i ochrony serwisów WWW!

- Jak zabezpieczyć swój serwis internetowy przed atakami
- Jak wykryć infekcje strony internetowej
- Jak tworzyć kopie zapasowe i przywracać serwis do działania

Wśród ogromnej liczby serwisów dostępnych w internecie miliony działają w oparciu o niezwykle popularne systemy **CMS**, jakimi bez wątpienia są **WordPress** i **Joomla!**. Ich twórcy i administratorzy dbają zwykle o wygląd stron oraz bieżącą aktualizację treści, często jednak brak im świadomości zagrożeń, a także wystarczającej wiedzy i doświadczenia, aby wdrożyć odpowiednią politykę bezpieczeństwa i procedury reakcji na awarię lub atak hakerski.

Jeśli jesteś twórcą witryn WWW lub osobą administrującą serwisami działającymi w oparciu o **WordPress** oraz **Joomla!** i leży Ci na sercu bezpieczeństwo Twoich stron, sięgnij po książkę „*Joomla i WordPress. Zabezpieczanie i ratowanie stron WWW*”. Dowiesz się dzięki niej, co należy zrobić, aby Twoje serwisy były właściwie chronione, zapoznasz się z rodzajami zagrożeń i metodami zabezpieczania się przed nimi, nauczysz się korzystać z narzędzi, które ułatwiają wykonywanie związanych z tym czynności, przekonasz się, jak ważne jest regularne tworzenie kopii zapasowych, oraz poznasz sposób szybkiego przywracania serwisów do działania. Nauczysz się także ograniczać zbędny ruch na stronie i przenosić ją pomiędzy serwerami oraz otrzymasz garść przydatnych informacji prawnych.

- Typowe zagrożenia dla serwisów WWW opartych na popularnych CMS-ach
- Sposoby zabezpieczania serwisów przed awariami i atakami
- Oczyszczanie serwisów po atakach i przywracanie ich do działania
- Tworzenie kopii zapasowych i odtwarzanie z nich danych
- Przenoszenie kompletnych stron pomiędzy serwerami
- Ograniczanie zbędnego ruchu na serwerach
- Narzędzia pomocne w codziennym zabezpieczaniu serwisów

Upredź hakerów, nie daj szansy włamywaczom, zabezpiecz się przed złodziejami!

Spis treści

Słowo wstępne (9)

Rozdział 1. Strony internetowe w obliczu zagrożeń (13)

- Dziś każdy może zarówno tworzyć, jak i psuć (13)
- Rodzaje podatności (14)
- Czy to był haker? (16)
- Dlaczego włamali się akurat do mnie? (18)
 - Co hakerzy robią z zainfekowanymi stronami? (21)
- Skutki włamań (24)
 - Kara od Google'a (25)

- Czas to pieniądz (25)
 - Falszywy podatek lub lubimy tylko różowych (27)
 - Skąd ten spam? (27)
- Jak oni to robią? (28)
 - Skąd oni są? (31)
- Kto jest winny? (31)
- Kwestie prawne - obowiązki administratora strony (32)
- Cyberbezpieczeństwo - uwzględnij to w wycenie (34)
- Moment szczerości (35)

Rozdział 2. Kopia zapasowa (37)

- Raz, dwa, trzy, kopię robisz Ty (37)
- Czy każda kopia jest kopią zapasową? (38)
 - Czy każda kopia zapasowa zadziała? (39)
- Rola, sposoby tworzenia i rodzaje kopii zapasowych stron internetowych (39)
 - Cel kopii zapasowej (39)
 - Rodzaje kopii zapasowych (40)
 - Sposoby wykonywania kopii zapasowych (40)
- Kopia od firmy hostingowej (40)
- Ręczna kopia zapasowa (42)
- WordPress - wtyczki do tworzenia kopii zapasowej (45)
 - Akeeba Backup dla WordPressa (45)
 - BackWPup (51)
- Joomla! - rozszerzenia do tworzenia kopii zapasowej (55)
- Leniwa kopia bazy (62)
- Podsumowanie (62)
- Statyczna kopia zapasowa strony (62)
 - Wersja strony offline (63)
 - Bezpieczeństwo kopii zapasowych (67)
 - Jak często robić kopie zapasowe? (68)
 - Jak zarobić na posiadaniu kopii zapasowej? (70)
 - Czy 5 minut wystarczy, aby zrobić kopię zapasową? (71)
- Podsumowanie (72)

Rozdział 3. Pierwsza linia obrony (73)

- Wiele sposobów, jeden cel (73)
- Hosting (74)
 - Podstawowe kryteria (74)
 - Hosting współdzielony (74)
 - Niemalże jak u siebie (75)
 - Ochroniarz w pakiecie (75)
 - Darmowe hostingi (77)
 - Zanim klikniesz "Zamawiam i płacę" (77)
- Uprawnienia katalogów oraz plików (78)
- Ciemność widzę, ciemność... (78)
 - Ukryj witrynę przed premierą (79)
 - Ukryj sygnaturę serwera (80)
 - Ukryj informacje o błędach (81)

- Blokowanie robotów i innych szkodników (83)
 - Niedostępne zaplecze (85)
 - Proszę mi tu nie skakać (88)
- Ochrona przed obcym PHP (88)
- Dlaczego nie warto być admin(em)? (89)
 - Wykluczyć zagrożenie (89)
 - Porządne hasło to... (90)
 - Każdy ma swoje konto (91)
 - Dodatkowa zasuwka (91)
- Synku, czy już posprzątałeś? (92)
 - Stare klocki to groźne klocki (92)
 - Zbędne wypełnienie (93)
 - Pokaż, co masz w pudełku (93)
- Czysty komputer to mniej podglądaczy (95)
 - Źródła infekcji (96)
 - ABC higieny laptopa (96)
 - Pomyśl dwa razy, zanim klikniesz (97)
- Htaccess 6G Firewall (97)
- PHP Firewall (99)
- Skanery podatności na atak (101)
- Certyfikat SSL (101)
 - Darmowy SSL (102)
- Wiedza, czyli co czytać (103)

Rozdział 4. Jak zabezpieczyć WordPressa (105)

- Numer jeden nie ma łatwo (105)
 - Główni winowajcy (106)
 - Utwardzanie WordPressa (106)
- Zalecane ustawienia serwera (107)
- Zaufane źródła plików (108)
 - Motyw lub wtyczka z niespodzianką (108)
- Nie prześpij aktualizacji (110)
- Jak ukryć WordPressa? (111)
- Ochrona zaplecza (114)
 - Ochrona formularza logowania (115)
 - Podwójna autoryzacja (116)
 - Ukrycie nazwy użytkownika (117)
 - Hasło użytkownika (119)
 - Dodatkowy kod jednorazowy (120)
 - Ograniczenie możliwości edycji (121)
 - Ukrycie błędów logowania (121)
- Zarządzanie użytkownikami (121)
- Mniej (wtyczek, motywów) znaczy bezpieczniej (122)
 - Czy tyle osób może się mylić? (123)
 - Weryfikacja wtyczek i motywów (124)
 - Zbieractwo nie popłaca (125)
 - Podsumowanie (126)
- Ochrona bazy danych (126)
 - Zmiana przedrostka (prefiksu) (127)

- Poprawiamy uprawnienia dostępu do bazy danych (129)
 - Ochrona za pomocą HTACCESS (130)
- Ochrona plików WordPressa (131)
 - Blokuj niechciane rozszerzenia (132)
- Szyfrowane połączenia (134)
 - Włącz SSL jednym kliknięciem (135)
 - HTTP/2 a SSL (136)
- Firewalle - kombajny ochrony (136)
 - Jak działają? (137)
 - Ogólne zalety i wady firewalli (137)
 - Którą zaporę wybrać? (138)
- Podsumowanie (140)

Rozdział 5. Jak zabezpieczyć system Joomla! (143)

- Drugi nie znaczy gorszy (143)
 - Popularność ma swoją cenę (144)
 - Utwardzanie systemu Joomla! (144)
- Zalecane ustawienia serwera (145)
- Zaufane źródła plików (146)
 - Szablon lub rozszerzenie z niespodzianką (147)
- Nie prześpij aktualizacji (148)
- Usuwanie informacji, że to system Joomla! (152)
- Ochrona zaplecza (154)
 - Ochrona formularza logowania (155)
 - Podwójna autoryzacja (156)
 - Gdzie się podział ekran logowania? (157)
 - Unikatowa nazwa użytkownika (157)
 - Hasło użytkownika (157)
 - Dodatkowy kod jednorazowy (160)
- Zarządzanie użytkownikami (162)
 - Minimalny poziom dostępu (162)
 - Nieużywane oraz zbędne konta (163)
 - Nie korzystasz, to wyłącz (163)
 - Admin może być tylko jeden (164)
- Mniej rozszerzeń znaczy bezpieczniej (164)
 - Czy tyle osób może się mylić? (164)
 - Weryfikacja rozszerzeń (165)
 - Zbieractwo nie popłaca (166)
- Ochrona bazy danych (168)
 - Przedrostek jos_ nie jest bezpieczny (169)
 - Poprawiamy uprawnienia dostępu do bazy danych (170)
 - Ochrona za pomocą HTACCESS (171)
 - Ochrona za pomocą dodatku (171)
- Ochrona plików systemu Joomla! (172)
 - Blokuj niechciane rozszerzenia plików (173)
- Szyfrowane połączenia (175)
 - Włącz SSL jednym kliknięciem (176)
 - HTTP/2 a SSL (177)
- Zainstaluj swój firewall (178)

- Jak działa? (178)
- Ogólne zalety i wady firewalli (178)
- Którą zaporę wybrać? (179)
- Polski akcent (184)
- Pomocnik online (185)
- Podsumowanie (185)

Rozdział 6. Oczyszczanie strony po włamaniu (187)

- Wykrycie śladów włamania (187)
 - Co wskazuje na udany atak? (188)
 - Zagrożenia w olbrzymiej skali (191)
- Czy zawsze można odzyskać stronę WWW i jak długo to trwa? (192)
- Biała strona (193)
 - Jak wyłączyć ręcznie wtyczkę lub rozszerzenie? (193)
- Jak odzyskać hasło administratora? (194)
 - Sposób dla użytkowników WordPressa (195)
 - Sposób dla użytkowników systemu Joomla! (196)
- Procedura czyszczenia krok po kroku (197)
 - Krok zerowy - przygotowania na sali operacyjnej (198)
 - Krok pierwszy - wykonanie kopii zapasowej (199)
 - Krok drugi - zewnętrzne sprawdzenie (200)
 - Krok trzeci - poinformuj zainteresowanych (201)
 - Krok czwarty - wyłącz zainfekowaną stronę (201)
 - Krok piąty - zmień hasła i przejrzyj dziennik (202)
 - Krok szósty - automatyczne skanowanie plików (202)
 - Krok siódmy - nadpisanie, skanowanie i ręczna analiza plików (206)
 - Krok ósmy - aktualizacja i zabezpieczenie (214)
 - Krok dziewiąty - sprawdź, zgłoś do sprawdzenia, uruchom witrynę i napisz raport (215)
- Odtwarzanie strony z kopii (216)
 - Nigdy nie wiesz na pewno, kiedy było włamanie (217)
- Włamanie a prawo (217)
 - Karalność za cyberwłamanie (218)
 - Gdzie zgłosić incydent? (220)
 - CERT Polska (222)

Dodatek A. Lista sprawdzająca (225)

Dodatek B. Odpłatna opieka nad witryną klienta (229)

Dodatek C. Jak przenieść stronę między serwerami (233)

Zakończenie, czyli zanim odłożysz książkę na półkę (239)

Skorowidz (241)