

Paweł Frankowski

WordPress i Joomla!

ZABEZPIECZANIE I RATOWANIE STRON WWW

UPRZEDŹ HAKERÓW, NIE DAJ SZANSY WŁAMYWACZOM,
ZMINIMALIZUJ RYZYKO!



Helion

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Opieka redakcyjna: Ewelina Burska

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
<http://helion.pl/user/opinie/jowozr>
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-2899-0

Copyright © Helion 2017

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

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
Fałszywy 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
Utwarczanie 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 płaca	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
Firewall — 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 zabezpieczanie	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

Rozdział 2.

Kopia zapasowa

Nigdy nie wiesz, co masz, póki tego nie stracisz.

— Katja Millay, *Morze spokoju*

Raz, dwa, trzy, kopię robisz Ty

Kopia bezpieczeństwa (*backup copy*, a potocznie *backup*) to nic innego, jak kopia danych tworzona na wypadek utraty lub uszkodzenia oryginalnych danych. Backup może dotyczyć zarówno prywatnych danych znajdujących się na domowym komputerze, jak i zawartości serwera.

Ktoś kiedyś powiedział, że administratorzy stron i sklepów internetowych dzielą się na tych, którzy robią kopie zapasowe, oraz na tych, którzy będą je robić. Dużo wcześniej, niż powstała sieć internetowa, Benjamin Franklin trafnie stwierdził, że uncja prewencji jest warta funta leczenia. Jest w tym sporo prawdy i — jak ze wszystkim w życiu — zaczynamy to doceniać wtedy, gdy zazwyczaj jest już za późno. Utrata dodanych, często unikatowych treści, w tym zdjęć, to — mówiąc delikatnie — nieprzyjemna sytuacja. Niestety, ale może przydarzyć się każdemu.

Nie zawsze jest to wina sprzętu, hakera, pechowego redaktora czy administratora strony. Czasami, jak podpowiada życie, głównym winowajcą okazuje się firma hostingowa. Przykładów nie trzeba szukać daleko: pod koniec lutego 2016 roku blisko 2 tysiące klientów hostingowych i około 10 tysięcy domen obsługiwanych przez polską firmę 2be.pl całkowicie utraciło dostęp do swoich usług. Klienci nie mieli dostępu zarówno do skrzynek pocztowych, serwerów, baz danych, danych swoich klientów, jak i do panelu do zarządzania domenami. Przez kilka tygodni nie mogli też przekierować domen w inne miejsce. Z różnych przecieków wiadomo, że dane zostały skasowane, a dyski z serwerowni nadpisane. Oznacza to, że dane prawdopodobnie zniknęły bezpowrotnie. Klienci grupy Adweb zostali zatem z niczym. Na szczęście część z nich miała kopie zapasowe trzymane z dala od „wyczyszczonej” infrastruktury. Dla wielu firm oraz osób prywatnych to była bardzo kosztowna lekcja pokory.



31 marca obchodzimy Światowy Dzień Backupu (*World Backup Day*).

Rozdział ten powstał głównie z myślą o użytkownikach niezaawansowanych. Jeśli zatem masz już wyrobiony nawyk regularnego tworzenia kopii zapasowych swoich danych i trzymasz je na osobnym zewnętrznym dysku, w chmurze lub innym bezpiecznym miejscu, jest to już połowa sukcesu. Jeśli do tego choć raz sprawdzałeś, czy na podstawie tych kopii danych możesz odtworzyć cały serwis, należą Ci się brawa.

Czy każda kopia jest kopią zapasową?

Aktualnie praktycznie wszystkie CMS-y, w tym systemy WordPress, Joomla! oraz Drupal, są zbudowane z dwóch kluczowych elementów: plików oraz bazy danych. Część użytkowników, która posiada prawdopodobnie pewne nawyki wyrobione podczas budowania prostych stron HTML, nadal uważa, że wystarczy skopiować pliki strony, aby ją przenieść lub uratować. Niestety, ale są w dużym błędzie. Najważniejszym elementem składowym jest bowiem baza danych. To tam jest przechowywana cała treść strony, w tym:

- ◆ dane kont użytkowników (także baza klientów),
- ◆ lista zainstalowanych rozszerzeń, wtyczek oraz szablonów,
- ◆ konfiguracja wszystkich rozszerzeń, wtyczek, motywów oraz szablonów,
- ◆ struktura i pozycje menu,
- ◆ treść stron, wpisów, artykułów, modułów,
- ◆ zamówienia ze sklepu,
- ◆ wpisy na forum,
- ◆ komentarze, recenzje oraz oceny produktów,
- ◆ hasła, nazwy kont oraz API usług społecznościowych.

Dobra kopia zapasowa powinna zapewnić całkowite odtworzenie zawartości serwisu w razie uszkodzenia bądź skasowania plików lub bazy danych. Czasami jednak niepełna, lub nawet nieaktualna, kopia jest lepsza od żadnej.



Zapamiętaj, że jeśli masz bazę danych, to strukturę plików możesz odtworzyć, bazując na paczkach instalacyjnych. Odtworzenie bazy danych na podstawie struktury plików jest praktycznie niemożliwe.

Generalne zalecenie jest takie, że należy posiadać taki system wykonywania kopii zapasowych oraz procedurę odtwarzania danych, aby minimalizować straty.

Czy każda kopia zapasowa zadziała?

Jedynie kopia, która była przetestowana, daje taką gwarancję. Warto zatem regularnie czytać raporty z utworzenia kopii zapasowych podawane przez wtyczkę lub rozszerzenie. Ma to na celu upewnienie się, że kopia zapasowa obejmuje wszystkie potrzebne dane i nie wystąpił jakiś nieoczekiwany problem, na przykład brak miejsca czy błąd podczas archiwizowania określonego folderu.

Najpewniejszą metodą jest jednak próba samodzielnego odtworzenia serwisu, choćby w testowej subdomenie. Na szczęście większość obecnych wtyczek oraz komponentów do wykonywania ich kopii zapasowych dba o weryfikację poprawności zapisu danych i na bieżąco informuje, czy nie występują jakieś błędy, na przykład brak miejsca na zapis na serwerze.

Krzysztof Palikowski, autor książek o CMS-ie Drupal oraz współautor bloga elimu, podpowiada jeszcze jeden sposób: jeśli już masz działający serwis, sprawdź, czy firma hostingowa potrafi wywiązać się ze zobowiązania. Poproś administratora o otwarcie plików i bazy danych serwisu do wskazanego przez Ciebie folderu, a następnie sprawdź, czy na podstawie tych zbiorów jesteś w stanie odtworzyć swoją witrynę.

Rola, sposoby tworzenia i rodzaje kopii zapasowych stron internetowych

Kopią bezpieczeństwa, kopią zapasową lub backupem nazywamy kopię danych, z której możemy skorzystać, gdy potrzebujemy odtworzyć zainfekowane, uszkodzone lub skasowane dane. Przydaje się również wtedy, kiedy uszkodzimy stronę, nieumiejętnie ją edytując lub źle aktualizując wtyczkę. Pełna kopia zapasowa to coś na wzór zahibernowanej, w pełni działającej strony, która jest gotowa do „odmrożenia” w dowolnym momencie.

Dla wielu osób tworzenie kopii zapasowych wydaje się uciążliwe, czego skutkiem jest ich brak lub brak systematyczności w ich tworzeniu. Z własnej praktyki pamiętam, że jeśli ktoś w ogóle posiadał kopię, to często pochodziła ona sprzed roku, a i to można nazwać „sukcesem”. Czasami właściciel strony internetowej panicznie szukał pomocy nawet u pierwotnego wykonawcy, jakby to ten miał sprawować stałą, najlepiej bezpłatną, pieczę nad jego plikami oraz bazą danych. Wiele osób uważa, że jeśli nie robimy kopii zapasowych, oznacza to, że nam na tych danych po prostu nie zależy.

Cel kopii zapasowej

Kopia zapasowa jest duplikatem wszystkich istotnych danych, które zawiera strona lub sklep internetowy. W przypadku wystąpienia awarii systemu lub uszkodzenia taki zestaw umożliwi przywrócenie CMS-a wraz z danymi aktualnymi w momencie robienia backupu. Kopia zapasowa jest również nieodzowna podczas przenoszenia strony z serwera A na serwer B.

Rodzaje kopii zapasowych

Kopie zapasowe można podzielić według kilku kryteriów. Jeśli chodzi o sposób wykonania, mogą to być kopie robione ręcznie albo automatycznie. W przypadku zakresu kopii mamy do czynienia z następującym podziałem:

- ◆ **Pełna kopia zapasowa** — zawiera wszystkie foldery, pliki oraz bazę danych. Można też się spotkać z opcją polegającą na wykonaniu pełnego zrzutu, łącznie z ustawieniami poczty, FTP oraz domen i subdomen.
- ◆ **Kopia bazy danych** — zawiera jedynie zrzut wybranej bazy danych. Jeśli ta baza danych jest wykorzystywana dla kilku odrębnych stron (używających innych prefiksów tabel), wtedy będzie zawierała komplet danych. Przy okazji warto o dodatkową uwagę. Nie zalecam korzystania z jednej bazy dla kilku stron z uwagi na ryzyko jej przejęcia i zmodyfikowania przed podmiot zewnętrzny (hakera). Wtedy strata będzie X razy większa.
- ◆ **Kopia plików** — zawiera wszystkie foldery oraz pliki (w tym zdjęcia, załączniki). Niestety, nie zawiera bazy danych, zatem nie można tylko na jej podstawie przywrócić działania CMS-a opartego na PHP oraz MySQL, na przykład takich systemów jak WordPress czy Joomla!.
- ◆ **Różnicowa kopia zapasowa** — wybór tego typu kopii zapasowej powoduje, że są kopiowane te pliki, które zostały zmodyfikowane lub utworzone od momentu wykonania ostatniej normalnej lub przyrostowej kopii zapasowej. Ten rodzaj kopii nie zajmuje dużo miejsca i wykonywany jest stosunkowo krótko.
- ◆ **Przyrostowa kopia zapasowa** — umożliwia wykonanie kopii zapasowej tylko tych danych (z reguły plików), które zostały utworzone lub zmodyfikowane od momentu wykonania ostatniej normalnej lub przyrostowej kopii zapasowej. Kopia przyrostowa nie kumuluje plików nowych i zmodyfikowanych, dlatego każdorazowo odnosi się do ostatniej wykonanej kopii zapasowej i pomija poprzednie.

Sposoby wykonywania kopii zapasowych

Kopie zapasowe możemy robić na wiele sposobów. Niestety, ani WordPress, ani w Joomla! nie dysponują wbudowanym na stałe narzędziem do wykonywania kopii zapasowych. Być może zmieni się to w następnych wersjach, podobnie jak wprowadzono „automatyczną” aktualizację CMS-a. Na szczęście dla obu tych systemów dostępnych jest wiele zarówno darmowych, jak i płatnych wtyczek oraz komponentów umożliwiających automatyczne lub ręczne wykonywanie kopii zapasowych w dowolnym momencie.

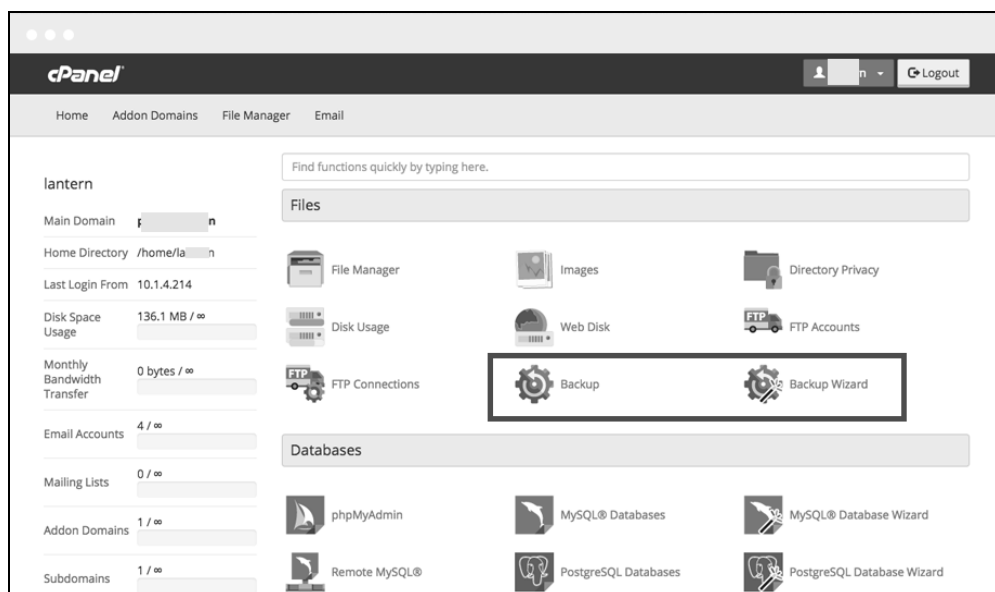
Kopia od firmy hostingowej

Zanim jednak przejdziemy do narzędzi dodatkowych, sprawdźmy, co mamy w ofercie firmy hostingowej, w której mamy wykupione konto albo którą zamierzamy wybrać.

Wykonywanie kopii zapasowych przez tego typu firmy jest standardową praktyką, ale jak podpowiadają realia, każdy stosuje inne zasady. Są operatorzy, którzy do swoich usług oferują backup tylko na 3 dni wstecz. Łatwo w takiej sytuacji o tragedię. W przykładowym scenariuszu do włamania lub uszkodzenia bazy danych sklepu doszło w piątek, a dowiadujesz się o tym dopiero w poniedziałek wieczorem lub we wtorek rano. Jeśli liczyłeś tylko na tę formę zabezpieczenia, no cóż, zamówienia z tych dni przepadły.

Firmy hostingowe robią kopie zapasowe z różną częstotliwością i przechowują je przez określoną liczbę dni. Na szczęście z uwagi na dużą konkurencyjność tej branży niektóre firmy stawiają na jakość i wysoką ochronę danych swoich klientów. I tu warto wspomnieć między innymi o zenbox.pl — jako jedna z nielicznych firm w naszym kraju tworzy ona kopie zapasowe co 6 godzin (czyli 4 razy dziennie), zwiększając tym samym bezpieczeństwo danych. Duża część firm oferuje jednak skromniejsze usługi, na przykład codzienny backup konta, cotygodniowy backup konta na zdalnym serwerze. Optymalny okres przechowywanie kopii z baz danych to 14, lub nawet 30 dni. Zanim zatem wybierzemy lub zmienimy usługodawcę, koniecznie powinniśmy zorientować się:

- ♦ jak często robi on kopie bezpieczeństwa;
- ♦ co obejmują kopie zapasowe — tylko bazę, czy również pliki;
- ♦ gdzie i jak długo są przechowywane kopie bezpieczeństwa;
- ♦ czy można wykonać ręczną kopię zapasową (rysunek 2.1).



Rysunek 2.1. Opcje do wykonywania kopii zapasowych w panelu hostingowym cPanel

Warto jednak bez względu na to, jak dobrze zaprezentowana jest oferta firmy, sprawdzić jej jakość, jeśli dostępny jest okres testowy na pakiet hostingowy. Ponadto zawsze powinniśmy się kierować zasadą ograniczonego zaufania, czyli nie powinniśmy opierać się tylko i wyłącznie na kopii bezpieczeństwa z tego źródła. Mimo wszystko

jednak kryterium kopii zapasowych powinno być jednym z kluczowych, które zdecydują o wyborze tej, a nie innej firmy hostingowej.

Ręczna kopia zapasowa

Umiejętność tworzenia ręcznej kopii zapasowej jest szczególnie przydatną umiejętnością, jeśli zaplecze CMS-a odmawia posłuszeństwa i nie masz możliwości skorzystania z dedykowanych wtyczek lub komponentów (opisanych w dalszej części tego rozdziału). Może się też zdarzyć sytuacja, kiedy klient nie może przekazać Ci danych do panelu hostingowego, ponieważ na przykład nie posiada aktualnie do nich dostępu albo na tyle Ci nie ufa. Wtedy zastosujesz pierwszą z opisanych poniżej metod. Zakładam, że w tym przypadku po prostu liczy się szybka reakcja z Twojej strony i nie masz czasu, aby czekać, aż ktoś prześle Ci właściwe dane. Też tak miałem kilkukrotnie, więc uwierz mi, że warto poznać oba sposoby.

Aby utworzyć kompletną kopię witryny, trzeba uzyskać dostęp do zasobów serwera i je skopiować. Na ogół wystarczy posiadać bądź (alternatywnie) otrzymać od klienta następujące dane:

1. dane niezbędne do skonfigurowania klienta FTP (nazwa serwera, numer portu, typ szyfrowania, nazwa użytkownika oraz hasło),
2. lub dane do panelu hostingowego (na przykład adres strony, nazwa użytkownika/domeny oraz hasło).

Pamiętajmy, aby ustalić również dokładną nazwę domeny, bowiem wiele firm oraz osób prywatnych posiada jednocześnie kilka(naście) różnych serwisów występujących pod domenami: *.pl*, *.com.pl*, *.info.pl*, *.eu*, *.com*. Czasami zatem łatwo o pomyłkę. A przecież naszym celem jest wykonanie zadania dotyczącego konkretnego serwisu.

W zależności od tego, jakimi danymi dysponujesz (patrz punkty 1. i 2.), musisz dopasować procedurę postępowania. Chyba najwygodniejsza jest sytuacja opisana jako druga. Wynika to z tego, że:

- ♦ prawie każdy panel hostingowy (na przykład DirectAdmin, cPanel) posiada opcje do wykonywania pełnej kopii zapasowej (rysunki 2.1 oraz 2.2);
- ♦ ta metoda jest szybka i raczej bezawaryjna.

Oznacza to, że nie musisz tracić czasu na ręczne kopiowanie kilkuset plików oraz eksportowanie bazy danych. Jedynie, co powinieneś zrobić, to po wykonaniu kopii zgrać ją na docelowy, zewnętrzny nośnik.

A co w sytuacji, gdy jedynymi danymi, jakie posiadasz, są dane do SFTP (FTP)? Także ten wariant pozwoli Ci wykonać w pełni wartościową kopię. Oto, czego potrzebujesz:

- ♦ klienta FTP (na przykład FileZilla),
- ♦ jednoplikowego skryptu o nazwie Adminer (<http://www.adminer.org>).

Skorowidz

6G Firewall, 97

A

Acunetix Web Vulnerability Scanner, 101

Adminer, 194, 196

adres

IP, 79, 220

URL

szyfrowanie, 17

AI-Bolit, 203

Akeeba Backup, 233, 236

Akeeba Kickstart, 234

Akeeba Solo, 237

Akeeba Tools, 237

AppSpider, 101

atak, 126

Local Files Inclusion, 171

słownikowy, 119, 158

typ

brute force, 30, 85, 113, 114, 116, 154, 156

CSFRF, 164

DDoS, 188

DoS, 188

SQL injection, *Patrz:* SQL injection

XSS, *Patrz:* XSS

B

backup online, *Patrz:* kopia zapasowa w chmurze

bezpieczeństwo, 34, 75, 92, 106, 114, 138, 143,

145, 150, 164

kopia, *Patrz:* kopia bezpieczeństwa

kopii zapasowej, 67

zasady, 96, 97

C

certyfiakat

Let's Encrypt, 102

SSL, 101, 102, 135, 175, 176

darmowy, 102

SSL/TLS, 102

checklist, *Patrz:* lista kontrolna

CMS, 13, 31

aktualizacja, 28

baza danych, 38, 40, 63, 71, 213

ochrona, 126, 127, 168, 169, 171

przedrostek, 169

uprawnienia dostępu, 129, 170

kopia zapasowa, *Patrz:* kopia zapasowa CMS

pliki, 38, 40, 63, 71, 131, 207

ochrona, 172, 173, 175

wytrzymałość na obciążenia, 15

zagrożenia, 15, 28

cracker, 218

Cross-Site Scripting, *Patrz:* XSS

Cybercrime as a Service, *Patrz:*

cyberprzestępstwo na żądanie

cyberprzestępczość, 218

skala, *Patrz:* włamanie skala

cyberprzestępstwo, 35, 83

na żądanie, 20

D

dane

kradzież, 19

wyciek, *Patrz:* wyciek danych

DDoS, 77

Denial-of-Service, *Patrz:* DoS

domena, 75

DoS, 15

Drupal, 105

dziennik

logowania, 101, 121, 202

E

exploit, 17, 18, 20, 152
 0-day, 125, 166
 tworzenie, 28
 zestaw automatyzujący ataki, *Patrz:* exploit kit
 exploit kit, 28

F

firewall, 73, 97, 99, 100, 136, 137, 178, 225
 wady, 137, 179
 zalety, 137, 179
 formularz
 logowania, 154
 ochrona, 114, 115, 155

G

Google, 25
 Grey Wizard, 101

H

haker, 16, 17, 18, 97, 217
 pochodzenie, 31
 pozytywny, 16
 usługa, 20
 haktywizm, 20
 hasło, 89, 90, 114, 154, 157, 226
 administratora
 odzyskiwanie, 194, 195, 196
 dwuskładnikowe uwierzytelnienie, 91, 116, 120,
 156, 160, 161
 łamanie, 119, 158
 resetowanie, 194
 tworzenie, 90, 119, 158, 225
 hosting, 77, 225
 cena, 74
 kryteria, 74
 współdzielony, 74, 75, 88, 99, 147

J

Joomla!, 13, 31, 105, 143
 aktualizacja, 148, 149, 150, 151
 szablonu, 151
 dodatki, 147
 instalacja, 146, 169
 komponent, 164, 165, 166
 Abivia Non-Activated User Killer, 163
 AdminExile, 155
 Akeeba Admin Tools Pro, 180

Akeeba Backup, 233, 236
 Akeeba CMS Update, 151
 Akeeba Tools, 170
 Akeeba Tools Pro, 155
 Antivirus Website Protection, 180
 DMC Firewall, 180
 jSecure, 155
 kSecure, 155
 RSFirewall!, 154, 155, 180, 181, 207
 Securitycheck, 154
 Securitycheck Pro, 155, 180, 183
 SP Page Builder Pro, 168
 wyłączanie, 193
 kopia zapasowa, *Patrz:* kopia zapasowa
 tworzenie Joomla!
 reinstalacja, 151
 ustawienia, 159
 utwardzanie, 144, 145
 wersja, 144, 154, 163
 zagrożenia, 15, 28
 zaplecze, 149, *Patrz:* zaplecze
 znaki szczególne, 152

K

kod
 wstrzyknięcie, 88, 126
 zaciemnianie, 17
 kopia bezpieczeństwa, 37
 kopia zapasowa, 39, 192, 199
 automatyczna, 227
 baza danych, 71
 bazy danych, 40, 71, 151
 bezpieczeństwo, 67
 CMS, 38
 częstotliwość, 41, 68, 69
 godzina wykonania, 70
 MySQL Backup FTP, 69
 od firmy hostingowej, 40
 offline, 66
 pełna, 40
 pliki, 71
 plików, 40, 151
 przyrostowa, 40
 ręczna, 42
 rodzaj, 40
 różnicowa, 40
 statyczna, 62, 64
 testowanie, 39
 tworzenie, 40, 42, 43, 111
 Joomla!, 55, 56, 57, 61, 62, 71
 WordPress, 45, 50, 51, 52, 71
 w chmurze, 68
 Kosiński Jacek, 17

L

lista kontrolna, 225
luka, 16, 28, 29, 136, 150

M

Magento
 zagrożenia, 15
Magnet, 31
Mitnick Kevin, 16

N

Netsparker, 101
NinjaFirewall, 100

O

OpenCart, 85
 zagrożenia, 15
oprogramowanie
 ransomware, 22
 zabezpieczające, 30

P

Palikowski Krzysztof, 39
Path Traversal, 15
phishing, 24
PHP, 225
 ustawienia, 107
 wersja, 107, 145
phpMussel, 100
phpMyAdmin, 117, 118, 128, 129, 170, 194, 195,
 196, 217
platforma
 e-learningowa, 19
plik
 .gitignore, 92
 .htaccess, 78, 79, 83, 85, 94, 97, 116, 130, 131,
 132, 133, 153, 155, 156, 171, 172, 226
 ochrona przed nieuprawnionym dostępem,
 79
 .htpasswd, 116, 155, 156
 configuration.php, 78, 169, 172
 function.php, 121
 htaccess.txt, 145, 226
 php.ini, 81, 107, 145
 robots.txt, 93
 web.config.txt, 93
 wp-config.php, 78, 82, 131
 xmlrpc.php, 132

polityka bezpieczeństwa, 201
prawa dostępu, 78
PrestaShop
 zagrożenia, 15
program
 antywirusowy, *Patrz:* skaner antywirusowy
protokół
 HTTP/2, 136, 177
 SSL, 101, 103, 134, 135
 TLS, 134, 175
przeglądarka
 offline, 63

R

RCE, 15
Remote Code Execution, *Patrz:* RCE
Remote File Inclusion, *Patrz:* RFI
RFI, 15
robot, 226
 blokowanie, 84
robot sieciowy, 97
root, 16

S

script kiddy, 17, 18, 97
SEO Spam, 23
serwer
 Apache, 75, 99
 dedykowany, 75
 HTTP
 zapytanie, 76
 IdeaWebServer, 94
 LiteSpeed, 99
 Nginx, 99
 prawa dostępu, 78
 raportowanie błędów, 81, 82
 Joomla!, 82
 WordPress, 82
 Smarthost.pl, 76
 sygnatura, 80
 ustawienia, 107
 wirtualny, 74
 prywatny, *Patrz:* VPS
serwis
 randkowy, 19
 społecznościowy, 19
Shadow Daemon, 100
skaner
 podatności na atak, 101
 skaner antywirusowy, 202, 203
sklep

internetowy, 19, 34
 spam, 19, 22, 27, 33, 77
 SQL injection, 15, 76, 77, 126, 128, 149, 164, 168, 171, 191
 podatność, 126
 zapobieganie, 126
 Starr Jeff, 97
 strona, 19
 administrator
 obowiązki, 32, 33
 dostęp
 dla wybranych adresów IP, 79
 hosting, 40, 74, *Patrz też:* hosting
 mapa, 135, 177
 oczyszczanie, 66
 podmiana, 23
 pozycjonowanie, 19
 ukryte, 22
 projektowanie, 34
 przekierowywanie, 23
 przeniesienie na inny serwer, 233, 236, 237
 przywracanie, 192, 216
 wersja offline, 63, 64, 66
 superadministrator, *Patrz:* root
 system
 kontroli wersji, 92
 luka, *Patrz:* luka
 zarządzania
 treścią, *Patrz:* CMS

U

użytkownik
 nazwa, 89, 114, 154, 157
 ukrywanie, 117, 118
 profil, 19
 przechwytywanie danych, 22, 23
 uprawnienia, 21, 121, 131, 162, 226

V

VPN, 90
 VPS, 75

W

w3af, 101
 webmaster
 narzędzia, 27
 włamania
 aspekty prawne, 218
 włamanie, 28, 30, 35, 83, 109, 126, 145, 187
 cel, 19

oznaki, 188
 skala, 191, 217, 219
 skutki, 24, 25, 27
 usuwanie zagrożenia, 197, 198, 200, 201, 206, 207, 214, 216
 zgłaszanie incydentów, 221, 223
 WordPress, 13, 31, 105
 aktualizacja, 110, 111
 dodatek
 Akeeba Backup, 55, 56, 57, 61
 LazyDbBackup, 62
 instalacja, 108, 127
 motyw, 108, 122, 124
 prefiks bazy danych, 127, 128
 tworzenie kopii zapasowej, *Patrz:* kopia
 zapasowa tworzenie WordPress
 ukrywanie, 111
 utwardzanie, 106
 wtyczka, 108, 122, 124, 125
 Akeeba Backup, 45, 50, 51, 233, 236
 All In One WP Security and Firewall, 138, 139
 Anti-Malware Security, 206
 BackWPup, 51, 52
 BBQ Free/Pro, 138, 139
 Better Search Replace, 135
 Better WP Security, 138
 BulletProof Security, 138
 Change DB Prefix, 128
 Custom Login URL, 115
 Force Strong Passwords, 119
 Hide My WP, 112
 iThemes Security, 115, 128, 138, 139
 Loginizer, 115
 Look-See Security Scanner, 207
 NinjaFirewall, 138
 Really Simple SSL, 135
 Rename wp-login.php, 115
 Shield, 138
 Sucuri Security, 138, 207
 Wordfence Security, 138
 WordPress Simple Firewall, 138
 WP Edition, 138
 WP Limit Login Attempts, 115, 116
 WP-DBManager, 128
 WPS Hide Login, 115
 wyłączanie, 193
 zagrożenia, 15, 21, 28, 29, 30
 zaplecze, *Patrz:* zaplecze
 ochrona, 114
 wyciek danych, 77

X

xDedic, 20
XML Quadratic Blowup, 15
XSS, 15, 76, 149, 164

Z

zaplecze, 85
 ochrona, 114, 121, 154
zaporą
 sieciowa
 ModSecurity, 75
ZB Block, 100
znacznik
 meta, 112, 113, 153

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA

 **Helion SA**

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

Działanie milionów serwisów dostępnych w internecie jest oparte na niezwykle popularnych systemach 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 oraz właściwe procedury reakcji na awarię lub atak hakerski.

Jeśli jesteś twórcą witryn WWW lub osobą administrującą serwisami opartymi na systemach WordPress oraz Joomla! i leży Ci na sercu bezpieczeństwo Twoich stron, sięgnij po tę książkę. Dzięki niej dowiesz się, 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

Helion

49605 numer katalogowy
księgarnia internetowa

<http://helion.pl>

zamówienia telefoniczne



0 801 339900



0 601 339900

Sprawdź najnowsze promocje:
 • <http://helion.pl/promocje>
 Książki najchętniej czytane:
 • <http://helion.pl/bestsellery>
 Zamów informacje o nowościach:
 • <http://helion.pl/novowosci>

Helion SA
 ul. Kościuszki 1c, 44-100 Gliwice
 tel.: 32 230 98 63
 e-mail: helion@helion.pl
<http://helion.pl>

sięgnij po **WIĘCEJ**



KOD KORZYŚCI

ISBN 978-83-283-2899-0



9 788328 328990

Informatyka w najlepszym wydaniu

cena: 49,00 zł