Bharp – Bartosz Balik

tel.: +48-22-245-22-90
biuro@bharp.biz
www.bharp.biz

Wordpress.
Zagrożenia, zapobieganie, oferta.

Przygotował:
Bartosz Balik
BARTOSZ@BHARP.BIZ
tel.: +48-508-871-474

Szanowni Państwo!

Firma Bharp realizuje kompleksową obsługę informatyczną dla małych i średnich przedsiębiorstw. Tworzymy zespół ludzi, będących specjalistami w swoich dziedzinach. Działamy rzetelnie, dokładnie i profesjonalnie, przy zastosowaniu szerokiej wiedzy, najnowocześniejszych narzędzi oraz wszelkich dostępnych mediów.

Nasza firma specjalizuje się we wdrażaniu usług sieciowych, systemów internetowych oraz w prowadzeniu serwisu komputerowego. Świadczymy usługi w zakresie:

- wdrażania i administrowania serwerami opartymi o systemy Linux/Unix oraz MS Windows, jak również sprzętowymi firewallami,
- projektowania i administrowania sieciami komputerowymi,
- opieki nad infrastrukturą informatyczną,
- spersonalizowanego hostingu,
- doradztwa w zakresie sprzętu informatycznego oraz sieciowego,
- tworzenia oraz prowadzenia stron i portali internetowych (w szczególności w oparciu o platformę wordpress),
- organizacji i prowadzenia szkoleń grupowych oraz indywidualnych (programowanie i obsługa aplikacji internetowych oraz administracja systemami i serwerami).

Firma Bharp jest elastyczna i dostosowuje się do wymagań klienta. Dodatkowo, wspólnie z naszymi partnerami, zajmujemy się:

- sprzedażą części komputerowych i materiałów eksploatacyjnych, z możliwością dostarczenia ich bezpośrednio do klienta,
- odzyskiwaniem danych z nośników,
- projektowaniem środków reklamy i informacji,
- grafiką komputerową, składem DTP,
- innymi usługami IT,
- remontami sprzętu peryferyjnego (drukarki, kserokopiarki itp.).

Wszystkie ceny są cenami netto. Wyceny usług i wdrożeń nie zawierają ewentualnych kosztów sprzętu i licencji na oprogramowanie.

Spis treści

Zagrożenia.

Strony internetowe stworzone na bazie dostępnych silników (m.in. wordpress) mają ogromne możliwości rozwoju oraz dają dużą niezależność klienta od wykonawcy. Dalsze zmiany, rozwój, rozbudowa mogą być wykonywane przez zupełnie innego wykonawcę niż pierwotny twórca witryny. A mnogość wtyczek pozwala na niemalże nieograniczoną rozbudowę funkcjonalności.

W związku z tym, że kod jest znany, łatwo też wykryć jego podatności. To dobrze, bo takie podatności twórcy silnika, wtyczek czy szablonów mogą stosunkowo szybko usunąć tworząc kolejne wersje i aktualizacje. Niestety podobną wiedzę ma ta „zła grupa", która może wykorzystać luki w systemie do włamania i przejęcia strony. Wiele osób uważa, że kto byłby zainteresowany moją malutką, nic nie znaczącą stronką. Nic bardziej mylnego. Taka strona może posłużyć jako farma linków do pozycjonowania, może służyć do wysyłania spamu, czy też do publikowania zainfekowanych wirusem plików. Każdy może stać się ofiarą hackerów.

Sprzątanie po włamaniu jest bardzo kosztowne i nie jest to tylko oczyszczenie kodu strony. Działania hakerów mogą się wiązać z dodaniem witryny do czarnej listy (programy antywirusowe zaczną blokować serwer), mogą się wiązać ze znacznym spadkiem pozycji strony w wyszukiwarkach, czy wręcz w ostateczności zablokowaniem w wyszukiwarkach. To jest też oczywiście strata wizerunkowa, szczególnie w przypadku, gdy na stronie pojawią się nieautoryzowane treści.

Kodeks dobrych praktyk.

Poniższe działania nie zabezpieczą w 100% strony, natomiast w znacznym stopniu zmniejszą ryzyko przejęcia strony przez hakerów:

1. Zawsze używaj trudnych haseł, które nie są lekką modyfikacją loginu. Bezpieczne hasło powinno być minimum 8 znakowe, powinno zawierać zarówno małe jak i duże litery, cyfry i znaki specjalne. Wiele włamań na wordpressa polega na brutalnym wielokrotnym próbowaniu zalogowania się do panelu.
2. Dbaj o aktualny kod strony i wtyczek. Atakujący lubią weryfikować wersję wordpressa i wtyczek i dla starszych wersji wykorzystywać ich znane podatności.
3. Wykup certyfikat SSL i wymuś logowanie do panelu przez szyfrowane połączenie. Pozwoli się to zabezpieczyć przed dość popularnym włamaniem polegającym na podsłuchaniu hasła.
4. Wprowadź dodatkowe zabezpieczenia (blokada adresu IP po kilku nieudanych próbach logowania, zmiana domyślnego adresu panelu, co pozwoli na zablokowanie automatów wyszukujących panele wordpress i inne), zweryfikuj uprawnienia do plików i katalogów. Może do tego posłużyć wtyczka iThemes Security.
5. Loguj które pliki strony były modyfikowane – pozwoli to w przypadku włamania szybko i sprawnie wykryć zainfekowany kod i oczyścić stronę. Hakerzy coraz skuteczniej ukrywają swój kod na stronie. Potrafią modyfikować daty plików, wygląda to tak, że zainfekowany kod znajduje się w plikach, których czas modyfikacji wskazuje na datę instalacji strony.
6. Wykonuj regularny backup strony (pliki i baza danych) – pozwoli na szybkie przywrócenie w przypadku włamania i podmienienia strony.
7. Monitoruj reputację strony – w ten sposób możesz szybciej wykryć włamanie.
8. Regularnie skanuj stronę pod kątem złośliwego kodu. Zdarza się, że po włamaniu przez pewien czas hakerzy nie wykorzystają jej do dalszych celów, więc można wykryć i uchronić się przed włamaniem zanim przyniesie szkody.
9. Dodaj stronę do google search console – ułatwi to oczyszczanie po włamaniu.
10. Zawsze używaj tzw. child themes. Pozwoli to na aktualizację szablonu bez uszczerbku na jego wyglądzie po modyfikacjach.

Powyższe czynności nie wyczerpują spektrum możliwości zabezpieczenia strony, są jedynie listą podstawowych czynności. Właściwy dobór narzędzi zawsze zależy od popularności witryny i budżetu oraz kalkulacji ryzyka i strat.

Oferta.

Z przyjemnością zajmiemy się tą mozolną i bardziej wymagającą częścią administracji stroną wordpress.

Administracja podstawowa.

Koszt: 200zł miesięcznie.

Cena dotyczy jednej instancji wordpressa. Jeśli strona jest zbudowana w oparciu o kilka instancji cena jest odpowiednio wyższa.

W ramach usługi wykonamy:

- Wstępny audyt zabezpieczeń oraz wdrożenie podstawowych funkcji bezpieczeństwa. Jeśli będą wymagane dodatkowe wdrożenia, przedstawimy ewentualną wycenę.
- Minimum raz w tygodniu weryfikację aktualizacji dla wordpressa, wtyczek oraz szablonów oraz ich instalację. W przypadku, gdy wtyczka lub szablon nie może być aktualizowana, poinformujemy o tym.
- Raz w tygodniu backup plików i bazy danych. Backupy są przechowywany w innym miejscu niż strona, dzięki temu minimalizujemy ryzyko infekcji, przejęcia backupów. Przechowujemy 3 ostatnie backupy.
- Stały monitoring dostępności strony. Jeśli zauważymy niepokojące objawy, to wysyłamy informację z propozycją dalszych działań i ewentualnych kosztów.
- Raz w miesiącu skanowanie w poszukiwaniu złośliwego kodu oraz weryfikacja reputacji witryny. Uwaga, w szczególnych przypadkach może się zdarzyć, że nie wykryjemy śladów włamania mimo uruchomienia odpowiednich narzędzi. Nie gwarantujemy, że brak wykryć oznacza w 100% czystą stronę.
- Przywracanie na wypadek włamania z dostępnych backupów.

Zastrzegamy sobie możliwość rezygnacji z dalszego wykonywania usługi po wykonaniu wstępnego audytu. Dotyczy to w szczególności wyjątkowo rozbudowanych stron wordpressa (np. zawierających również sklep internetowy) lub nie aktualizowanych od dłuższego czasu stron. W takim wypadku po wykonaniu audytu przedstawimy propozycję kosztową i ewentualnie listę wymaganych działań bezpłatnie.

Usługi dodatkowe.

Jest to zestaw usług, które możemy wykonać na dodatkowe zlecenie, bądź rozszerzając abonament podstawowy.

- Stały monitoring zmienianych plików i podjęcie odpowiednich działań: zgodnie z osobną wyceną.
- Stały monitoring logowania się do panelu i podjęcie odpowiednich działań: zgodnie z osobną wyceną.
- Zmiana częstotliwości backupów i ilości przechowywanych kopii: zgodnie z osobną wyceną.
- Modyfikacja kodu strony, wyglądu, dodawanie treści: 70zł za każdą rozpoczętą godzinę a przy większych zleceniach zgodnie z osobną wyceną.
- Zmiana częstotliwości innych działań z abonamentu podstawowego: zgodnie z osobną wyceną.

- Instalacja dodatkowych wtyczek, rozbudowa funkcjonalności: 70zł za każdą rozpoczętą godzinę a przy większych zleceniach zgodnie z osobną wyceną.
- Oczyszczanie kodu strony po włamaniu (jeśli ostatni backup również zawiera zainfekowany kod lub przywrócenie nie wyeliminowało problemu): według osobnej wyceny. Uwaga, koszt będzie znacznie niższy jeśli będą dostępne logi modyfikacji plików.
- Analiza powłamaniowa. Szczególnie przydatna, jeśli przywrócenie z backupu nie powoduje pożądanych efektów: według osobnej wyceny. Uwaga, do analizy możemy potrzebować dostępu do logów komputerów osób zarządzających treścią strony oraz serwera na którym przechowywana jest strona.
- Wsparcie przy minimalizacji strat wynikłych z włamania (wyszukiwarki, reputacja itp.): według osobnej wyceny.