Prestashop – jak wyczyścić sklep ze złośliwego oprogramowania

1. **Wyłącz tymczasowo sklep**

A) Jak najszybciej wyłącz tymczasowo swój sklep internetowy. Im szybciej, tym lepiej – roboty wyszukiwarek internetowych często odwiedzają Twoją stronę w poszukiwaniu zmian i aktualności – jeśli znajdą na niej złośliwy kod, mogą oznaczyć ją jako zainfekowaną, co z kolei poskutkuje częściowym wyndeiksowaniem strony oraz znaczącym spadkiem wizyt organicznych.

b) **Co zrobić, jeśli wyszukiwarka już oznaczyła Twój sklep internetowy jako zainfekowany?**



Przede wszystkim upewnij się, że strona została w pełni wyleczona ze złośliwego kodu. Jeśli nie dodałeś wcześniej swojej strony do google.com/webmaster – zrób to teraz. Następnie w sekcji „Problemy dotyczące bezpieczeństwa w Search Console” zgłoś swoją stronę do ponownej weryfikacji. Jeśli Google będzie pewny, że luki w bezpieczeństwie zostały usunięte, komunikat zniknie.

c) **Jak sprawdzić, czy strona trafiła na czarną listę?**

Za pomocą darmowego scannera online <https://sitecheck.sucuri.net/> dowiemy się, czy strona widnieje w dalszym ciągu jako blacklistowana oraz czy w dalszym ciągu znajduje się na niej złosliwe oprogramowanie. Pomocnym narzędziem, do sprawdzania blacklisty, jest również Virus Total.

1. **Przeskanuj wszystkie pliki Twojego sklepu**

**A) Przeskanuj wszystkie pliki na serwerze za pomocą ClamAV**

Większość serwerów posiada w Cpanelu zainstalowany skaner antywirusowy – ClamAV. Warto z niego skorzystać, by sprawdzić, które pliki zostały zainfekowane. Dobrym pomysłem będzie również poproszenie swojego hostingodawcy o pełne przeskanowanie wszystkich Twoich stron na serwerze FTP (jeśli na jednym serwerze posiadasz więcej stron, jest bardzo prawdopodobne, że również zostały zainfekowane).

**b) Co zrobić, gdy nie masz dostępu do Shell’a na serwerze?**

a) By całkowicie usunąć wszystkie zainfekowane pliki, warto ściągnąć całą zawartość FTP oraz bazę danych MySQL na swój komputer lokalny z wydzielonym logicznie miejscem na dysku twardym, odpowiednio do tego przygotowanym.

Jeśli posiadasz dostęp do Shell, zacznij od komendy:

*find . -type f -name '\*.php' | xargs egrep -i "(shell\_exec|system|stream\_socket\_client|gzinflate|system|passthru|eval|base64\_decode) \*\(" > scanresult\_suspciouse.txt*

A następnie przeanalizuj stworzony plik\*.

\*(Uwaga! Nie wszystkie otrzymane rekordy będą zawierać złośliwy kod – jeśli nie masz pewności, czy plik jest podejrzany, porównaj go z oryginalnym plikiem Twojej wersji Presty ściągnietym bezpośrednio z prestashop.com

**b) Sprawdź ostatnio zmodyfikowane pliki**

Za pomocą poniższej komendy sprawdź ostatnio zmienione pliki php (w poniższym przykładzie zastosowano wyszukiwanie wszystkich plików .php, które zostały zmodyfikowane w ciągu ostatnich **14** dni). Niezwykle ważne jest, by ustalić datę ataku (warto prześledzić logi z serwera).

find . mtime-**14** 2>/dev/null | egrep -i "\.(php)$" > scan-results.txt

Następnie sprawdź utworzony plik w poszukiwaniu zainfekowanych plików php.

1. **Przywróć pliki z czystej instalacji Prestashop**

Kolejną czynnością będzie przywrócenie najważniejszych plików z czystej instalacji Prestashop (sciągnietej z prestashop).

* ./index.php
* ./controllers/admin/AdminLoginController.php
* Pliki block-cart

**UWAGA! Jeśli posiadasz zainstalowane moduły płatności online USUŃ JE z serwera i zainstaluj ponownie (ściągnij najnowszą wersję ze strony dostawcy Twoich płatności).**

1. **Wygeneruj ponownie plik .htaaccess**

Złośliwy kod może znajdować sie

równiez w pliku .htaaccess w folderze public\_html. Najlepszym rozwiązaniem będzie skasowanie go, i ponowne wygenerowanie z backendu Prestashop.

1. **Zmień wszystkie hasła**

Zmien wszystkie hasła dostępowe do:

**- baz mysql,**

**- cpanelu,**

**- kont ftp,**

**- dane do backoffic’u.**

Pamiętaj, że powinieneś mieć zawsze aktualną wersję modułów Prestashop oraz wersję samego oprogramowania.

KONIECZNYM jest również wykonywania backupów (przynajmniej raz dziennie – baz danych jak i FTP).