Jak postępować, gdy ktoś włamie s[..]

2024-05-05 06:29:46

Wydruk artykułu FAQ

Kategoria:	Hosting ITL::Bezpieczeństwo	**Ostatnia aktualizacja:**	2015-10-22 22:36:44
Status:	publiczny (dla wszystkich)		
Język:	pl		

Objawy (publiczny)

Na mojej stronie internetowej pojawił się jakiś złośliwy kod, którego tam nie umieszczałem! Co robić?

Problem (publiczny)

Często zdarza się, że instalujemy na stronie jakieś darmowe oprogramowanie (np. WordPress, osCommerce, Joomla!, Mambo, PHPNuke itp.). Podobnie jak przypadku każdego innego oprogramowania, powinniśmy dbać o to, aby było aktualne. W przeciwnym wypadku, może okazać się, że w naszej dawno nieaktualizowanej wersji ktoś znalazł lukę, przez którą hakerzy mogą włamać się na stronę i nam zaszkodzić.
Szczególnie ważne to jest w przypadku popularnych aplikacji - w nich luki w bezpieczeństwie wykorzystywane są w sposób zautomatyzowany, masowy.

Rozwiązanie (publiczny)

Kolejność postępowania w przypadku włamania na stronę powinna być następująca:

- Zablokowanie publicznego dostępu do strony przez WWW np. w pliku .htaccess:

```
deny from all allow
    allow from moj.ad.res.ip
```

- Odzyskanie plików strony z backupu. W przypadku braku backupu, można zwrócić się z tym do operatora hostingu (odzyskanie odpłatne).
Alternatywnie - można wykonać pracochłonne, ręczne usuwanie pozostałego złośliwego kodu ze stron. Złośliwy kod może być umieszczony w każdym pliku. Najczęściej w plikach html, php, js, jednak należy dokładnie sprawdzić cały serwis.
- Aktualizacja aplikacji.
- Zmiana hasła do bazy danych aplikacji.
- Zmiana haseł kluczowych użytkowników aplikacji (np. kont administratorów).
- Dodatkowo proponujemy użyć "Zabezpieczenie strony" w panelu [1]admin.itl.pl
.
- Odblokowanie publicznego dostępu do strony.

[1] http://admin.itl.pl