

Bezpieczny Hosting WWW: Jak hosting może chronić (albo narażać) Twoją stronę?

Aleksandra Grygiel



O mnie...

Od ponad czterech lat pracuję w branży hostingowej, gdzie na co dzień łączę doświadczenie w obsłudze klienta z praktyczną administracją serwerami. Specjalizuję się w bezpieczeństwie usług hostingowych, konfiguracji serwerów WWW oraz technicznym wsparciu stron internetowych.

Studiuje Cyberbezpieczeństwo na Politechnice Częstochowskiej i aktywnie rozwijam swoje kompetencje zarówno w zakresie wiedzy technicznej, jak i edukacyjnej. Z pasją dzielę się swoją wiedzą, szczególnie w obszarze praktycznego wdrażania zasad bezpieczeństwa w infrastrukturze hostingowej.





Dlaczego bezpieczeństwo hostingu jest ważne?

Twoja strona WWW to nie tylko kod i treść!

Konsekwencje zaniedbań w bezpieczeństwie hostingu:

- Utrata danych i funkcjonalności strony.
- Infekcje złośliwym oprogramowaniem.
- Wyciek poufnych informacji (dane klientów, dane logowania).
- Problemy z SEO i reputacją.
- Koszty naprawy i przywrócenia strony.

Jak hosting MOŻE chronić Twoją stronę WWW? – Kluczowe mechanizmy bezpieczeństwa

1

Zapora sieciowa (Firewall)

Monitorowanie i blokowanie nieautoryzowanego ruchu.

2

Ochrona przed atakami DDoS

Minimalizowanie przestoju spowodowanych przeciążeniem serwerów.

3

Regularne aktualizacje oprogramowania

Łatanie luk bezpieczeństwa w systemie operacyjnym i aplikacjach serwerowych.

4

Izolacja kont

Zapobieganie rozprzestrzenianiu się problemów z innymi stronami na tym samym serwerze.

5

Kopie zapasowe

Możliwość szybkiego przywrócenia strony w przypadku awarii lub ataku.

Jak hosting MOŻE chronić Twoją stronę WWW? – Kluczowe mechanizmy bezpieczeństwa

6

**Skanowanie
w
poszukiwaniu
wirusów**

Regularne
sprawdzanie plików
w poszukiwaniu
infekcji.

7

**Certyfikaty
SSL/TLS**

Szyfrowanie
połączenia
między
przeglądarką
użytkownika a
serwerem.

8

**Bezpieczne
protokoły
dostępu**

Zabezpieczenie
przesyłania plików i
zdalnego dostępu.

9

**Monitoring
bezpiecze
ństwa**

Ciągłe
monitorowanie
serwerów pod
kątem
podejrzanej
aktywności.

10

**Informowanie
o
zagrożeniach**

informowanie klientów o
potencjalnych
zagrożeniach czy
pracach serwisowych

Jak hosting MOŻE narażać Twoją stronę WWW? – Potencjalne zagrożenia

1

**Przestarzałe
oprogramowa-
nie
serwerowe**

Znane luki
bezpieczeństwa
łatwe do
wykorzystania.

2

**Brak
odpowiedniej
konfiguracji**

Otwarcie na ataki z
zewnątrz.

3

**Słabe
zabezpieczenia
fizyczne
serwerowni**

Możliwość
nieautoryzowanego
dostępu do sprzętu.

4

**Brak
regularnych
kopii
zapasowych**

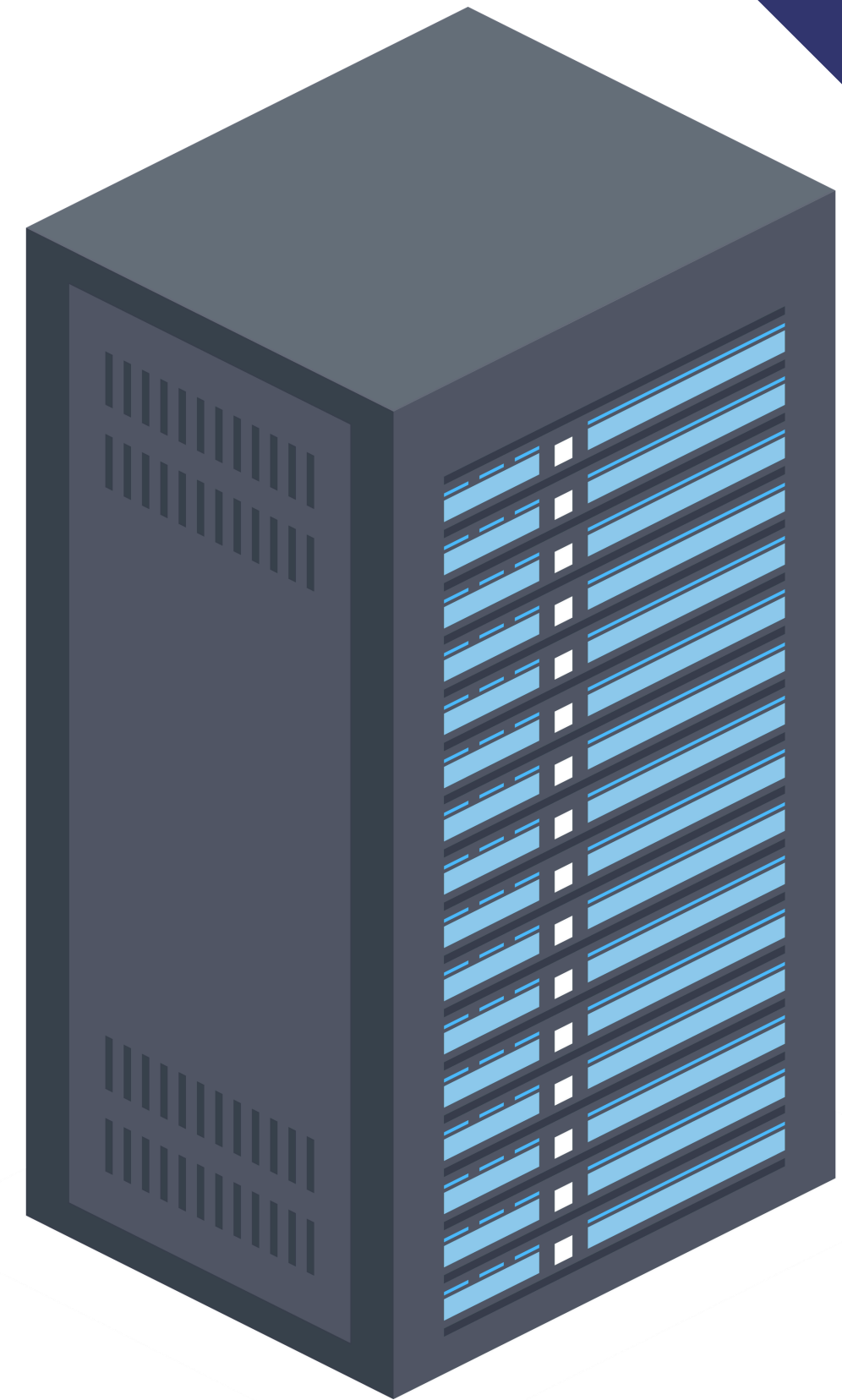
5

**Ignorowanie
alertów
bezpieczeństwa**

Wybór bezpiecznego hostingu – Na co zwrócić uwagę?

Mądry wybór to bezpieczna przyszłość Twojej strony!

- Reputacja i doświadczenie dostawcy: Sprawdź opinie i historię firmy.
- Zakres oferowanych funkcji bezpieczeństwa: Upewnij się, że oferują kluczowe mechanizmy.
- Polityka aktualizacji i zarządzania łatkami bezpieczeństwa.
- Jasne zasady dotyczące kopii zapasowych i ich przywracania.
- Dostępność wsparcia technicznego w zakresie bezpieczeństwa.
- Lokalizacja serwerów i zabezpieczenia fizyczne serwerowni.



Dobre praktyki po stronie użytkownika

Bezpieczeństwo to wspólna odpowiedzialność

Ty też masz swój wkład w bezpieczeństwo!

- Silne hasła i uwierzytelnianie dwuskładnikowe (2FA) dla wszystkich kont (hosting, panel administracyjny strony).
- Regularne aktualizacje CMS (np. WordPress, Joomla, Drupal), wtyczek i motywów.
- Usuwanie nieużywanych wtyczek i motywów.
- Ograniczenie dostępu do panelu administracyjnego.
- Regularne skanowanie strony pod kątem złośliwego oprogramowania (nawet jeśli hosting to robi).
- Świadomość zagrożeń phishingowych i socjotechnicznych.

Implementacja własnych zabezpieczeń



Poczta email to nierozłączna część hostingu
oraz działalności w internecie

Bezpieczeństwo Poczty E-mail – Dodatkowy Wektor Ataku

Typowe zagrożenia dla bezpieczeństwa poczty elektronicznej

- Phishing
- Podsywanie się pod zaufane źródła w celu wyłudzenia danych logowania lub informacji finansowych.
- Malware w załącznikach i linkach
- Złośliwe oprogramowanie rozprzestrzeniane przez wiadomości e-mail – najczęściej jako załączniki lub linki.
- Ataki na serwery pocztowe
- Próby przejęcia kontroli nad serwerem pocztowym, np. w celu rozsyłania spamu lub kradzieży danych.



Zalecenia dotyczące ochrony

- Stosowanie silnych haseł i uwierzytelniania dwuskładnikowego (2FA)
- Szyfrowanie wiadomości
- Wdrożenie filtrów antyspamowych i antywirusowych
- Automatyczna ochrona przed znanymi zagrożeniami.
- Konfiguracja polityk SPF, DKIM i DMARC



Masz pytania?

Adres e-mail

hosting@smarthost.pl

Strona internetowa

smarthost.pl

Dziękuję za uwagę!