Na zabezpieczenie strony internetowej przed {yootooltip title=[***niepowołanym dostępem***] width=[350]}
Pod pojęciem "niepowołany dostęp" należy rozumieć wszelkie działania skierowane przeciwko serwerowi, oprogramowaniu lub samej stronie internetowej zmierzające do unieruchomienia, zmiany treści, uszkodzenia przez osoby, które zdobyły taki dostęp nielegalnym sposobem poprzez złamanie zabezpieczeń serwera lub działających na nim aplikacji.
{/yootooltip} ma wpływ wiele czynników, poczynając od zabezpieczenia serwera, a kończąc na osobach znających hasła dostępu do aplikacji znajdujących się na serwerze.
Niestety żaden system, ani żadne oprogramowanie nie jest doskonałe i dlatego zawsze istnieje niebezpieczeństwo, że ktoś celowo lub przypadkowo znajdzie sposób na ominięcie zabezpieczeń poszczególnych składników serwera lub oprogramowania.

Tworząc stronę internetową dokładamy wszelkich starań, żeby serwer (doradzamy wybór serwera w sprawdzonych firmach hostingowych, dbamy o bezpieczeństwo naszych serwerów hostingowych) działał pod kontrolą najnowszego, sprawdzonego oprogramowania, które gwarantuje, że wszelkie znane luki w zabezpieczeniach są wyeliminowane. Skrypty stron internetowych są systematycznie aktualizowane i testowane w poszukiwaniu luk w bezpieczeństwie.

Pomimo zabezpieczenia strony internetowej przed znanymi zagrożeniami nigdy nie ma pewności, że ktoś nie znajdzie nieznanej luki w zabezpieczeniach i dokona ataku na serwer lub stronę. Dlatego jako dodatkowe zabezpieczenie stosujemy dwustopniowy system ochrony danych strony internetowej. Pierwszym stopniem jest codzienna kopia bezpieczeństwa wszelkich danych znajdujących się na koncie hostingowym Klienta. Drugim stopniem zabezpieczenia jest ręczna kopia danych wykonywana po każdorazowym wprowadzeniu zmian na stronie internetowej.
W przypadku ataku odtworzenie danych nie stanowi problemu i można odzyskać stronę internetową w takiej postaci, jak przed atakiem.

Zdarzają się spektakularne ataki na strony internetowe znanych portali społecznościowych (kradzież milionów danych użytkowników portalu Facebook), organizacji rządowych (włamania na serwery Pentagonu lub NASA), koncernów międzynarodowych (włamanie na strony Sony Playstation i kradzież danych), ale Państwa strona może czuć się bezpiecznie, ponieważ do włamania również jest potrzebne kilka czynników.
Najpierw haker, cracker lub inny internetowy wandal musi trafić na Państwa stronę, potem musi ona zainteresować go jako obiekt ataku, w końcu musi sprawdzić na jakim serwerze jest strona, jak jest zbudowana i czy posiada jakieś luki w zabezpieczeniach. Początkującego włamywacza zniechęcą prawdopodobnie zabezpieczenia, a doświadczony będzie chciał się wykazać na jakieś stronie, która przyniesie mu choć trochę splendoru w środowisku.

Chociaż szansa na włamanie na Państwa stronę jest niewielka, to nie można jednak wykluczyć, że jakiś wandal, który niszczy tylko po to, żeby niszczyć trafi na stronę i zniszczy ją tylko dla samego dzieła zniszczenia.