

Bezpieczeństwo e-commerce

praca dyplomowa inżynierska

Bezpieczeństwo w dziedzinie handlu elektronicznego jest bardzo ważnym zagadnieniem, które często jest bagatelizowane i większość małych i średnich firm o nim zapomina lub nie traktuje go z należytą powagą. Osoby, które uważają, iż skoro ich firma nie jest duża i nie ma popularnej strony, to już samo to stanowi wystarczającą ochronę – nic bardziej mylnego. To, czy firma posiada dwóch pracowników i jeden serwer internetowy czy jest to duży serwer w dużej firmie tak samo mogą stać się obiektem ataku. Anonimowość nie jest absolutnie żadnym zabezpieczeniem. Dla hakera jest najważniejsze to, iż włamie się do kolejnego systemu, a co za tym idzie – zdobędzie kolejne trofeum.

Uruchamiając serwis, w którym będziemy przechowywać dane o klientach jest jeszcze lepszym i ważniejszym powodem aby zabezpieczyć serwer. Niewątpliwie bardzo ważne jest zabezpieczenie systemu wspomagające pracę agencji reklamowych, gdyż oprócz danych klientów na kradzież lub zniszczenie narażone są również prace, które zostały wykonane dla kontrahentów. Często są to rzeczy oryginalne i nietuzinkowe, a ich utrata mogłaby wiązać się z poważnymi konsekwencjami.

Oczywiście najbezpieczniejszy komputer to taki, który nie ma użytkowników i nie jest podłączony do Sieci. Ponieważ taki komputer nie znajduje praktycznego wykorzystania w większości zastosowań, trzeba na coś pozwolić: komputer w przypadku serwisu on-line potrzebuje administratora i musi być podłączony do sieci.

Dobrym rozwiązaniem jest udostępnienie możliwości przesyłanie plików poprzez serwer FTP^[1]. Jest niewiele możliwości na zawieszenie serwera mając do niego dostęp tylko poprzez FTP.

Nie ma wglądu do innych danych niż tylko te udostępnione. Usługa FTP może być tak skonfigurowana, aby możliwe było wyłącznie zapisanie, ale pliki nie będą mogły zostać odczytane, co znacznie ogranicza możliwość manipulacji danymi.

Takie metody oczywiście pomagają ustrzec się przed włamaniem do systemu, jednak nie są one absolutnie pewne. Jest przy tego rodzaju rozwiązaniach kilka problemów, które niestety nie mogą być rozwiązane tak długo, jak komputer jest podłączony do sieci. Zalecane jest zatem skorzystanie z rozwiązania typu „firewall”. Przy korzystaniu z tego typu rozwiązań istnieje jednak niebezpieczeństwo, iż będą one na tyle kosztowne, iż inwestycja może być ekonomicznie nieopłacalna. Koszty wdrożenia i utrzymywania takiego rozwiązania zaczynają się od zera i nie mają górnej granicy. Wszystko zależy od tego, jakie decyzje zostaną podjęte przy wdrożeniu zabezpieczeń. Czy wybór padnie na doradztwo eksperta z dziedziny bezpieczeństwa czy będą to profesjonalne zabezpieczenia, które wdroży i nadzór nad nim będzie sprawował specjalizujący się w tym usługodawca czy też firma chce kupić gotowy produkt lub usługę lub czy chce sama zbudować swoje rozwiązanie typu firewall. Aby wybrać najlepsze rozwiązanie należy poradzić się eksperta lub posiadać szczegółową wiedzę odnośnie bezpieczeństwa i protokołów.

Najczęściej jednak w przypadku małych i średnich firm korzysta się z gotowych, niedrogich rozwiązań w postaci aplikacji, którą konfiguruje się na serwerze, routerze z funkcjonalnością firewall lub osobnego urządzenia firewall.

Istnieją dwa różne rodzaje firewall: serwer pośredniczący (ang. proxy) i filtr pakietowy. Najczęściej stosuje się oba rozwiązania jednocześnie, gdyż tak jest po prostu bezpieczniej.

Serwer proxy jest komputerem, który chroni granicę pomiędzy zewnętrznym Internetem, a wewnętrzną siecią lokalną. Serwer pośredniczący sam nawiązuje wszystkie połączenia z siecią

zewnętrzną i wyłącznie poprzez niego dochodzi do kontaktu z zewnątrz.

W tym momencie bezpieczeństwo jest związane z tym serwerem, gdyż tylko on narażony jest na atak hakera. Oczywiście pokonanie serwera proxy oznacza wolny dostęp do sieci lokalnej.

Z powyższego powodu stosuje się filtry pakietowe. Filtrację zapewnia komputer, który analizuje ruch wszystkich pakietów danych, ażeby upewnić się, że są one dozwolone w sieci lokalnej.

Bardzo dobrym zabezpieczeniem jest tzw. „honeypot”. Jest to pułapka składająca się z „komputera, danych i wyodrębnionego obszaru sieci lokalnej które udają prawdziwą sieć, lecz są odizolowane i odpowiednio zabezpieczone. Wszystko to z zewnątrz wygląda jakby zawierało informacje lub zasób który mógłby być potencjalnym celem cyberprzestępcy.

^[1] FTP – File Transfer Protocol – protokół umożliwiający przesyłanie danych (teksty, dane audio-video, obrazy) z tzw. serwera FTP do własnego komputera poprzez Internet bądź w kierunku odwrotnym.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę [pisanie prac](#) - profesjonalna pomoc w pisaniu prac w granicach prawa.