Pamiętaj o bezpiecznym haśle do swojego konta

Czwartek, 23 luty 2017, 14:39, autor: Fakturowo.pl

Zapewne każdy z nas zna historię o Alibabie i czterdziestu rozbójnikach. Jak wiemy by dostać się do skarbu, należało wypowiedzieć słowa: "Sezamie otwórz się!". Zatem na podstawie tego bajkowego przykładu widzimy, że już starożytni Persowie używali pewnego rodzaju haseł, które strzegły dostępu do ich kosztowności. Mimo tak dużego postępu technicznego jaki miał miejsce na przełomie ostatnich, hasła nadal są najpowszechniejszą metodą uwierzytelniania. Współczesne mechanizmy wykorzystujące hasła, strzegą dostępu nie tylko do systemów informatycznych. Jednak w tej dziedzinie stały się podstawowym elementem bezpieczeństwa. Do tak dużej popularności tej metody uwierzytelniania przyczynił się z pewnością fakt, że w systemach informatycznych metoda ta nie wymaga dodatkowych kosztów (na jakie z pewnością bylibyśmy narażeni decydując się na innego rodzaju zabezpieczenia na przykład czytniki kart elektronicznych). Zapewne dużym plusem takiego rozwiązania jest również to, że chyba wszyscy użytkownicy wiedzą jak z niego korzystać.

We współczesnych systemach informatycznych w celu uwierzytelnienia się, musimy podać hasło, a także nazwę użytkownika. Dzięki takiemu rozwiązaniu komputer nie tylko "wie", że dana osoba jest uprawniona do korzystania z jego zasobów, ale także ma możliwość sprawdzenia z kim ma do czynienia. Mimo wielu zalet jakie niesie ze sobą używanie haseł, metoda ta nie jest bezpieczna. Chyba najpowszechniejszą techniką wykorzystywaną przez hakerów, w celu dostania się do zabezpieczonych systemów, jest właśnie odgadywanie haseł, bądź ich łamanie za pomocą specjalistycznych narzędzi. Sytuacja taka ma miejsce ponieważ znaczna większość użytkowników, nie rozumie istoty tego mechanizmu i nie umie stworzyć haseł na tyle skomplikowanych, by ich odgadnięcie przez osoby niepowołane było niemożliwe.

Najczęściej stosowane hasła są po prostu zbyt proste. Takie hasła dają możliwość ataku siłowego (ang. brute force). W tej metodzie haker stara się odgadnąć hasło, podając jego wszystkie możliwe kombinacje. Przyczyn tworzenia zbyt słabych haseł jest wiele. Bardzo często wybieramy hasła, które łatwo jest nam zapamiętać. W gruncie rzeczy nie jest to złe rozumowanie, jednakże takie hasła są łatwe do odgadnięcia przez inne osoby. Powinniśmy pamiętać, że dobre hasła to hasła łatwe do zapamiętania przez właściciela, a zarazem trudne do odgadnięcia przez intruza. Zatem jako hasła nie powinniśmy wybierać:

- nazwisk, pseudonimów, imion ukochanych osób (na przykład Gosia), imion przyjaciół, ulubionych aktorów (na przykład Sylwester) czy zwierząt (na przykład PiesKuba), przezwisk, widzimy więc, że w ogóle nie powinniśmy stosować żadnych nazwisk czy imion,
- nazwy naszego komputera czy używanego systemu operacyjnego,
- numeru naszego samochodu, telefonu, prawa jazdy, dowodu osobistego czy paszportu lub też nazwy ulicy, na której mieszkamy – nie powinniśmy używać żadnych informacji, które łatwo jest zdobyć,
- nazw miejscowości, kraju, kontynentów, rzek, jezior czy gór – zatem ogólnie nazw geograficznych,
- dat urodzin naszych lub naszych bliskich, znajomych,
- słów ze słownika,
- ciągów składających się z tych samych znaków (na przykład: dddddddd, 77777777 czy $$$$$$$$) lub ciągów będących kolejnymi znakami na klawiaturze (na przykład 12345678, zxcvbnm),
- wulgaryzmów, przekleństw także w obcych językach (na przykład fuck you).

Chcąc stworzyć bezpieczne hasło, musimy wiedzieć, że takie hasło nie istnieje, gdyż wszystkie hasła można złamać metodą siłową (ang. brute force attack), czyli metodą sprawdzającą wszystkie istniejące możliwości. Powinniśmy jednak wiedzieć jak wiele mamy możliwości tworzenia haseł. Jeśli za "k" przyjmiemy liczbę dostępnych na klawiaturze znaków, a "j" oznaczać będzie długość hasła (czyli liczbę jego znaków), wówczas, ze wzoru Lhaseł = kj jesteśmy w stanie wyliczyć liczbę możliwych do utworzenia haseł, gdyż z matematycznego punktu widzenia są to wariacje z powtórzeniami. Na tej podstawie, jeśli nasze hasło będzie się składało z dwóch znaków i jeśli za "k" przyjmiemy 26, gdyż przeważnie tyle mamy liter na klawiaturze, wówczas istnieje tylko 676 możliwości jego kombinacji. W przypadku hasła 8 literowego liczba ta wynosi już ponad 208 milionów. W tych przypadkach założyłem, że do ich stworzenia użyte

zostały tylko duże lub tylko małe litery. Współczesne systemy uwierzytelniania rozróżniają przeważnie oba rodzaje liter, a także dają możliwość używania cyfr lub innych dowolnych znaków. Wówczas tworząc hasło złożone z ośmiu liter i mając do dyspozycji na przykład 100 różnych znaków, liczba możliwych kombinacji wynosi 10000000000000000. Liczba ta mówi chyba sama za siebie. Niektóre systemy dopuszczają możliwość stosowania haseł o długości nawet do 32 znaków! Widzimy więc, że wybierając hasło mamy bardzo dużo możliwości.

Oczywiście długość hasła nie świadczy o bezpieczeństwie systemu, jednak powinniśmy pamiętać, że im dłuższego hasła użyjemy, tym trudniej będzie je złamać. Chcąc zatem stworzyć hasło, które będzie stosunkowo trudno złamać, powinniśmy przestrzegać pewnych podstawowych zasad. Dobre hasło, to takie, które nie znajduje się w żadnym słowniku i nie pochodzi z żadnego języka (także z języka programowania), nie powinno być również modyfikacją takiego słowa.