

Jakie hasła są naprawdę mocne?

Dyskusja nad wdrożeniem skutecznych i naprawdę bezpiecznych metod autoryzacji użytkowników trwa od kilku lat, nic jednak nie wskazuje na to, aby udało się w najbliższym czasie funkcjonować bez haseł, a więc również bez znajomości podstawowych zasad ich opracowywania oraz stosowania. Niestety bardzo wiele osób, mimo niezwykle intensywnych kampanii informacyjnych i ostrzeżeń wciąż używa mało bezpiecznych haseł, żyjąc w przekonaniu, że aby hasło było naprawdę mocne, musi być ono trudne do zapamiętania dla nich samych, co oczywiście nie jest prawdą.

Cyberbezpieczeństwo (błąd w słowie kluczowym: cyberbezpieczeństwo) - podstawowe zasady

Z telewizji oraz internetu wciąż dobiegają informacje o lekceważeniu przez użytkowników komputerów kwestii dotyczących bezpieczeństwa w sieci, głównie przez osoby indywidualne. Sytuacja wygląda zupełnie inaczej w firmach, gdzie to administratorzy dbają o bezpieczeństwo użytkowników komputerów i przestrzeganie podstawowych zasad, takich jak: wymuszenie ponownego logowania do systemu po kilkuminutowej bezczynności, zmianie hasła po upływie określonego czasu czy odpowiedniej konstrukcji tych haseł. Podejście takie jest uciążliwe zarówno dla użytkowników komputerów, jak i samych administratorów, jednak nic nie wskazuje na to, że sytuacja ta ulegnie zmianie w związku z czym znajomość zasad tworzenia dobrych i mocnych haseł jest koniecznością.

Reguły tworzenia bezpiecznych haseł

Należy wiedzieć, że za cyberbezpieczeństwo (błąd w słowie kluczowym: cyberbezpieczeństwo) odpowiadają głównie hasła, które powinny być tworzone według kilku uniwersalnych reguł. Po pierwsze muszą być one łatwe do zapamiętania dla ich użytkownika oraz niezwykle trudne do przypadkowego odgadnięcia. Jak to zrobić? Powszechnie znaną metodą jest skorzystanie z ulubionego przez siebie cytatu i zapisanie go w sposób zupełnie nieoczywisty (wykorzystuje się do tego np. pierwsze litery z cytatu, zmienia się ich wielkość, używa się znaków specjalnych oraz zamienia się litery z cyframi, co doskonale da się zrobić na przykładzie zero i literki o). Hasło musi być tak skonstruowane, że nawet jeżeli jakaś osoba je zobaczy, nie będzie ona w stanie go zapamiętać.

Kolejną uniwersalną zasadą jest to, że im hasło ma więcej znaków, tym jest trudniejsze. Absolutne minimum to jednak 8 znaków. Ważną sprawą jest jego uaktualnianie, które według specjalistów nie powinno się odbywać rzadziej niż raz na 30 dni.

Rzeczą, o której również nie można zapomnieć, jest konieczność posiadania odrębnych haseł do różnych, posiadanych przez siebie kont i aplikacji, dzięki czemu prawdopodobieństwo straty wszystkiego w jednym momencie jest niewielkie. Osobne hasła znacznie zwiększają poziom cyberbezpieczeństwa.

Zakazane praktyki

Podstawową rzeczą, jakiej nie powinno się robić, jest wykorzystywanie całych, istniejących w rzeczywistości słów. Hasło powinno być przede wszystkim niezrozumiałą dla innych kombinacją znaków, która nie jest możliwa do odgadnięcia na podstawie czyjejś wiedzy o nas. Unikać należy również powtórzeń i sekwencji tych samych znaków oraz zapisywania haseł na komputerze czy w swoim własnym notesie, co niestety wciąż jest popularną praktyką.

Alternatywne metody autoryzacji użytkownika

Na rynku istnieją już inne metody autoryzacji użytkowników, choć niestety nie są, i nic nie wskazuje na

to, żeby w najbliższej przyszłości były powszechnie dostępne – są to np. metody wykorzystujące linie papilarne (smartfony marki Apple), metody wykorzystujące skanowanie siatkówki czy rozpoznanie twarzy, a nawet metoda opierająca się na wykorzystaniu emotikonek, która wydaje się najbardziej możliwa do szerokiego zastosowania (znacznie utrudnia ona życie cyberprzestępcom – o wiele trudniej złamać hasła, które nie składają się ze znaków dostępnych na klawiaturze). Na razie jednak to wciąż odpowiednio skonstruowane, tradycyjne hasła odpowiadają za nasze cyberbezpieczeństwo (błąd w słowie kluczowym: cyberbezpieczeństwo), dlatego należy wiedzieć jak je tworzyć i się nimi odpowiednio posługiwać.

artykuł przygotowany przez

CTS Customized Training Solutions

www.cts.com.pl