Dlaczego i jak należy tworzyć silne hasła?

Ze względu na zmianę polityki bezpieczeństwa Akademii Leona Koźmińskiego wszystkie osoby posiadające konta umożliwiające dostęp do sieci ALK muszą posiadać przynajmniej ośmioznakowe, trudne do złamania hasła. W niniejszym artykule odpowiem na pytanie dlaczego tak musi być i jak stworzyć bezpieczne hasło.

1. **Po co jest potrzebne trudne, przynajmniej ośmioznakowe hasło?**

XXI wiek nie bez powodu nazywany jest wiekiem informacji. Informacja jest obecnie niemal tak cenna jak złoto czy pieniądze. Można wręcz powiedzieć, że w obecnych czasach posiadanie informacji pozwala się wzbogacić. Wszystko jest w porządku, dopóki wzbogacenie to nie odbywa się cudzym kosztem, niestety czasem jest odwrotnie i to właśnie przed tym broni każdego użytkownika silne hasło.

Być może brzmi to jak fantastyka, ale należy pamiętać, że każde pojedyncze konto zarejestrowane w Akademii Leona Koźmińskiego zawiera w sobie ogromną ilość informacji, które zgodnie z prawem muszą być chronione. Adresy e-mail czy pełne dane osobowe, to tylko część informacji jakich poszukują cyber-przestępcy. Zbyt proste hasło, to wręcz zaproszenie do zaatakowania naszej sieci chociażby po to by uzyskać wspomniany adres e-mail i dodać go do ogromnych baz danych SPAM-erów. Również pełny adres zamieszkania czy numer telefonu mogą posłużyć do nękania nas niechcianymi reklamami. A to tylko jedna z wielu rzeczy, które można zrobić z takimi danymi.

Bezpieczeństwo danych naszych użytkowników jest więc pierwszym powodem w wyniku którego w ALK zdecydowaliśmy się na zaostrzenie polityki bezpieczeństwa. Nie można jednak zapomnieć o drugim powodzie. Zbyt proste hasła nie tylko umożliwiają włamanie się do sieci i zdobycie poufnych danych, ale również umożliwiają hakerom działanie na szkodę całej sieci ALK. Nikt z Państwa chyba nie chce by serwery pocztowe zamiast e-maili studentów i wykładowców rozsyłały SPAM, a sieciowe dyski pełne były wirusów i robaków?

Niestety w XXI wieku pomysłowość hakerów na łamanie haseł (o tym za chwilę więcej) jest ogromna. Ogromne są również szkody, które mogą oni wywołać jeśli dostaną się do chronionego systemu. Obecną sytuację można przyrównać do wojny, w której jedna ze strona cały czas udoskonala środki zagłady. Obrońcy nie mogą pozostać bierni na takie działania i muszą wzmocnić swoje środki obrony. Dlatego też niezbędne jest wzmocnienie siły haseł broniących sieć Akademii Leona Koźmińskiego.

ul. Jagiellońska 57/59, 03-301 Warszawa
tel. 22 519 21 00, fax 22 519 23 01
akademia@kozminski.edu.pl, www.kozminski.edu.pl

2. Jakie powinno być hasło, a jakie być nie może?

Generalnie możemy wyróżnić dwa kryteria, których spełnienie gwarantuje bezpieczeństwo hasła. Kryteria te, to:

- **Długość** – powszechnie uznaje się, że 8 znaków to minimum jeśli chcemy mieć do czynienia z naprawdę bezpiecznym hasłem;
- **Różnorodność** – dobre hasło powinno składać się z cyfr, małych i dużych liter oraz symboli.

Z drugiej strony możemy wyróżnić kilka sposobów na formułowanie haseł, które definitywnie sprawią, że hasło nie będzie bezpieczne. Oto i one:

- **Proste do bólu** – niestety dobre hasło nie może być proste. Hasła typu: *12345*, *qwerty*, *stokrotka*, *konik* czy takie same jak nasze *imię*, *nazwisko*, *login* lub też każdy inny pojedynczy wyraz są BEZUŻYTECZNE i nie stanowią żadnej przeszkody dla osób próbujących włamać się do systemu.
- **Trudny wyraz wystarczy** – często wydaje się nam, że jeśli jako hasło użyjemy prostego słowa, to rzeczywiście każdy je zgadnie, natomiast jeśli użyjemy trudnego to będziemy bezpieczni, bo w końcu po co kombinować skoro większość ludzi na pewno ma łatwe. A poza tym czy haker mógłby znać na przykład model czyjegoś ulubionego samolotu? Logika ta nie jest pozbawiona sensu. Rzeczywiście nie każdy haker wie czym jest na przykład palindrom. Problem tkwi jednak w tym, że on tego wiedzieć nie musi. Zamiast tego posiada specjalny słownik który sam sprawdza hasła. W słowniku tym są wszystkie wyrazy występujące w polskim, angielskim, hiszpańskim, duńskim i każdym innym języku. Na pewno jest tam i palindrom.
- **Urodziny, imieniny, rocznice, pesele** – zdecydowanie nie. Ustawianie jako hasło daty urodzin, daty rocznicy ślubu czy PESELU również nie ma najmniejszego sensu. Nawet jeśli będzie to data urodzin koleżanki córki siostry ciotecznej. Haker, który będzie chciał się włamać będzie znał te wszystkie dane i na pewno je sprawdzi.

Przykładowe dobre hasła stworzone na podstawie wszystkich opisywanych wyżej kryteriów, to na przykład: *!@moA42^* czy *4mb^Oa*1*. Jak jednak łatwo zauważyć hasła te są dość trudne zarówno do wymyślenia, jak i do zapamiętania. Dlatego też w przypadku, gdy musimy używać wielu haseł warto skorzystać z kilku wskazówek ułatwiających generowanie i zapamiętywanie haseł. W następnej części artykułu opiszę dwie takie możliwości.

ul. Jagiellońska 57/59, 03-301 Warszawa
tel. 22 519 21 00, fax 22 519 23 01
akademia@kozminski.edu.pl, www.kozminski.edu.pl

3. Wskazówki ułatwiające wygenerowanie haseł

Pierwsza z możliwości wymaga odrobinę czasu i cierpliwości. Oto i ona:

a) Najpierw należy wymyślić jakieś zdanie, które łatwo nam zapamiętać. Na przykład: *Moi synowie Łukasz i Adrian, to kochane chłopaki*;
b) Następnie należy „odciąć" od każdego wyrazu końcówki pozostawiając jedynie pierwsze litery, w tym wypadku: *MsŁiAtkc*. Ze względu na fakt, że systemy często nie akceptują polskich znaków przerabiamy *Ł* na *L* => *MsLiAtkc*. W ten prosty sposób powstała baza do hasła składająca się z dużych i małych liter;
c) Teraz należy wpleść w to hasło jakieś znaki specjalne. Trzeba to zrobić w taki sposób, by łatwo zapamiętać, gdzie wstawiliśmy znaki. Dobrym pomysłem może być ich wstawienie obok spójnika występującego w pierwotnym zdaniu czy na początku i na końcu hasła. Powiedzmy, że znaki specjalne, które zdecydujemy się dodać do naszego przykładowego hasła, to *@* i ***, a wstawimy je na początku i na końcu wyrazu. Mamy więc => *@MsLiAtkc**;
d) Na koniec potrzeba jeszcze jakiejś cyfry. Przy tak skomplikowanym zalążku można sobie troszkę ułatwić i zastąpić cyfrą taką literę, którą łatwo da się skojarzyć z jakąś cyfrą – na przykład i zamienić na *1*. Powstanie więc *@MsL1Atkc**.

Stworzone hasło można za darmo przetestować za pomocą narzędzia do sprawdzania bezpieczeństwa haseł firmy Microsoft, które znajduje się pod adresem internetowym:

https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

Przykładowe, stworzone powyżej hasło otrzymało ocenę *Medium*, a więc spokojnie mogłoby być używane do zabezpieczenia sieci szkolnej. Gdyby chcieli Państwo stworzyć hasło jeszcze trudniejsze, na przykład do bankowości internetowej, to powyższe hasło należy jeszcze bardziej rozbudować (dodać więcej symboli i cyfr, a nawet zacząć od dłuższego zdania) – tak stworzone hasło otrzymałoby ocenę najlepsze.

Druga metoda jest prostsza, a opiera się na wykorzystaniu istniejących w sieci stron internetowych, które umożliwiają generowanie haseł. W tym artykule skupię się na jednej z nich, a konkretnie na stronie

http://www.safepasswd.com/

Sposób działania strony jest bardzo prosty. Po otwarciu jej w przeglądarce internetowej interesują Państwa trzy miejsca: *Type*, *Length* oraz *New Password*. Strony używa się w następujący sposób:

a) Najpierw w ramce *Type* należy wybrać z listy jakiego rodzaju hasło Państwa interesuje. Wśród wielu możliwości najlepsze to *Easy to Remeber* (generuje hasła, które według systemu najłatwiej zapamiętać) lub *All Characters* (generuje najtrudniejsze hasła). Ponadto nie należy odznaczać pola *Use UpperCase and LowerCase*.

c) Następnie w ramce *Length* należy wybrać długość hasła. Jeśli wcześniej zdecydowali się Państwo na opcję *Easy to Remember*, to powinni teraz wybrać przynajmniej 10, natomiast jeśli na *All Characters*, to przynajmniej 8 znaków.

d) Na koniec pozostało klikanie w pole *New Password* tak długo, aż dane hasło zadowoli Państwa i zdecydują się go Państwo używać. Przykładowe hasło wygenerowane za pomocą *SafePasswd.com*, to: *coUrses1$9*.

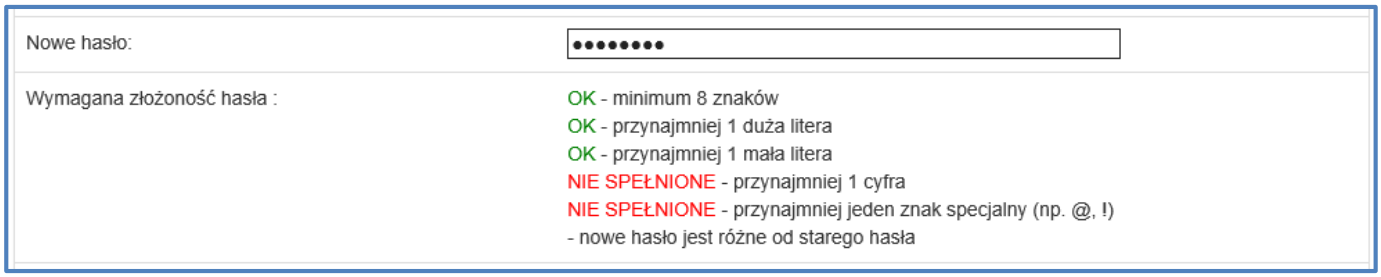
Tak wygenerowane hasła wystarczą by Państwa konto w sieci ALK było bezpieczne. W przypadku kont bankowych warto jednak znacznie wydłużyć ilość znaków i wygenerować hasło w przedziale przynajmniej 15-20 znaków.

4. Jak zmienić hasło w Akademii Leona Koźmińskiego?

Najprościej robi się to za pomocą specjalnie przeznaczonego do tego formularza, który znajduje się pod adresem:

http://haslo.kozminski.edu.pl/

Po wejściu na stronę Państwa oczom ukażą się dwa formularze. Pierwszy z nich pozwala zmienić hasło w sytuacji, gdy znamy stare hasło. Podczas wpisywania kolejnych znaków w formularzu do zmiany hasła podświetleniu ulegną kolejne wymagania, które nowe hasło powinno spełniać.



Drugi formularz pozwala na zmianę hasła w sytuacji, gdy stare hasło zostało zapomniane. Aby móc z niego skorzystać należy w jednym z pól podać numer klienta, który znajduje się na odwrocie legitymacji studenckiej.

Więcej informacji o tym jak zmienić hasło do usług informatycznych w Akademii Leona Koźmińskiego znajdą Państwo na stronie Działu Obsługi Klienta i Wdrażania Innowacyjnych Rozwiązań

http://it.kozminski.edu.pl

Autor: *Maciej Madziński*
Edycja: *Krzysztof Demczuk*
Dział Obsługi Klienta i Wdrażania Innowacyjnych Rozwiązań ALK
Na podstawie doświadczeń własnych i oraz bloga:
http://jacek50.blox.pl/2009/01/Tworzymy-hasla-trudne-hasla.html