Czy Ty także sądzisz, że Twoje hasło jest trudne do złamania?

Kategoria: Styl życia
Opublikowano: piątek, 10, styczeń 2025 13:39
Alina Piekarz

Kradzież danych, pieniędzy, a nawet tożsamości – takie skutki może przynieść zbyt lekkomyślne podejście do ustawiania haseł internetowych. Jak nie dać się przestępcom, którzy wykorzystują coraz bardziej zaawansowane metody wirtualnych włamań podpowiadają specjaliści z Zespołu CERT Polska, którzy przygotowali najbardziej aktualny pakiet wytycznych dotyczących nadawania haseł w sieci.

Hakerzy już to wiedzą...

Informacje o kradzieży danych w Internecie nikogo już dzisiaj nie dziwią. Mimo coraz większej świadomości społeczeństwa dotyczącej zasad bezpiecznego korzystania z sieci okazuje się, że wciąż zdarzają tacy, którzy uważają, że ciąg liczb „12345678" czy data urodzenia stanowią dobrą barierę przed internetowym przestępcą. Tylko w ubiegłym roku jednorazowo – 4 lipca – za sprawą hakera kryjącego się pod nickiem „ObamaCare" wyciekło do sieci około 10 miliardów haseł do różnych stron. Codziennie przydarzają się dziesiątki podobnych incydentów, choć nie na tak spektakularną skalę. Specjaliści z zespołu CERT Polska, działającego w instytucie NASK, opublikowali właśnie rekomendacje, które porządkują i aktualizują dotychczasowe zasady zakładania haseł internetowych.

Zaktualizowana lista wytycznych dotyczących bezpiecznego korzystania z sieci może zaskakiwać, ponieważ podważa pewne dotychczas stosowane metody. Jedną z nich jest częsta zmiana haseł, która szczególnie chętnie jest stosowana w firmach i instytucjach publicznych. Wykorzystywane systemy informatyczne wymuszają na pracownikach regularną korektę stosowanych zabezpieczeń. Zdaniem specjalistów z zakresu cyberbezpieczeństwa takie podejście jest błędne, ponieważ w rzeczywistości nowe hasła są coraz prostsze, co za tym idzie – coraz łatwiejsze do złamania. Jednocześnie zalecają niezwłoczną zmianę hasła wyłącznie w przypadku podejrzenia, że ktoś je poznał.

Bezpieczne hasło wcale nie musi być trudne do zapamiętania!

Z danych zebranych przez CERT wynika, że najmniej podatne na ujawnienie są hasła, które składają się z co najmniej szesnastu znaków. Każda mniejsza ich liczba proporcjonalnie zwiększa szansę na złamanie. Jednak sama długość to nie wszystko. Aby długie hasło było skutecznym zabezpieczeniem, musi być także odpowiednio skomplikowane. Wykorzystanie ciągu znaków: „admin.1admin.1admin.1admin.1" nie jest więc dostatecznym zabezpieczeniem konta, podobnie jak hasła określane jako pozornie trudne typu: „Galwaniczny123$" czy „zaq1@WSXcde3$RFV". Eksperyment przeprowadzony przez specjalistów CERT wykazał, że złamanie takowych zajmuje poniżej pięciu minut.

Jak więc powinno wyglądać silne i trudne do ujawnienia hasło? Przede wszystkim powinno być łatwe do zapamiętania przez użytkownika. Choć skomplikowane układy kilkunastu czy kilkudziesięciu cyfr, liter różnej wielkości i znaków specjalnych są bardzo dobrymi zabezpieczeniami, zapamiętanie ich może przysporzyć wielu kłopotów. Specjaliści CERT podsuwają więc łatwiejsze rozwiązanie w postaci formułowania haseł jednozdaniowych o abstrakcyjnym lub wyimaginowanym charakterze, na przykład: „WlazlKostekNaMostekIStuka". Innym dobrym rozwiązaniem jest stworzenie podobnego hasła z wykorzystaniem obcych słów, na przykład: „DwaBialeLatajaceSophisticatedKroliki". Według obliczeń złamanie podobnych kombinacji zajmie przestępcom setki lat.

Dodatkowe zabezpieczenia

Specjaliści CERT zaznaczają, że aby jeszcze lepiej zabezpieczyć się przed niechcianymi gośćmi na naszych kontach internetowych, powinniśmy stosować, oprócz unikalnych i trudnych do złamania haseł,

dodatkowe metody uwierzytelniania w postaci chociażby dwuetapowej weryfikacji. Polega ona na wprowadzeniu znanego tylko nam hasła lub PIN-u oraz dodatkowej autoryzacji, na przykład kodem jednorazowym, potwierdzeniem w aplikacji na naszym urządzeniu lub użyciem dedykowanego klucza USB.

Bezwzględnie należy także pamiętać o używaniu różnych haseł do różnych kont. Oczywiste jest, że ich zapamiętanie może okazać się dość kłopotliwe, dlatego do ich zapisywania można używać rożnego rodzaju manedżerów haseł. Mogą działać jako funkcje przeglądarek lub aplikacje w chmurze. Umożliwiają bezpieczne przechowywanie, generowanie mocnych haseł i automatyczne logowanie. Najpopularniejsze są menedżery wbudowane w przeglądarki. Warto jednak pamiętać o ryzyku utraty danych przy awarii urządzenia, zwłaszcza bez kopii zapasowej. Aplikacje oparte o rozwiązania chmurowe są w tym względzie bezpieczniejsze, ponieważ przechowują dane online, niezależnie od sprzętu użytkownika – wskazują specjaliści z zakresu cybrebezpieczeństwa.

Uwaga! Hasła podane w artykule jako bezpieczne i prawidłowe nie nadają się do powielania ze względu na ich ujawnienie!

Źródło: NASK/CERT