Cyberbezpieczeństwo zaczyna się od hasła. A kończy na „123456”

Kategoria: Styl życia
Opublikowano: wtorek, 29, kwiecień 2025 09:10
Tomasz Smaś

123456 – to nie jest wyliczanka, to najpopularniejsze hasło używane w ubiegłym roku na świecie. W Polsce było podobnie, wynika z analizy NordPass. Hasło krótkie, proste i łatwe do zapamiętania jest wymarzonym dla hakerów. Potrzebują oni zaledwie 37 sekund, aby złamać 8-znakowe hasło złożone z cyfr, a 81 proc. naruszeń związanych z hakowaniem jest wynikiem kradzieży lub stosowania słabego hasła.

To nie teoria. W 2012 roku LinkedIn padł ofiarą jednego z największych wycieków danych w historii – ujawniono ponad 117 mln haseł. Wiele z nich brzmiało banalnie: „linkedin”, „password”, „123456”. Hakerzy bez trudu je złamali i wystawili na sprzedaż w dark webie. I tak naprawdę – od tamtej pory niewiele się zmieniło.

Złe nawyki

W teorii wszyscy wiemy, hasła trzeba chronić. W praktyce – wciąż popełniamy te same błędy. Główny to używanie zbyt łatwych haseł, typu „123456” i „password”. Zgodnie z analizą NordPass, to pierwsze było w 2024 roku użyte ponad 3 mln razy (w Polsce 13 470). Według specjalistów, złamanie aż 161 wśród 200 najczęściej używanych haseł jest możliwe w zaledwie sekundę.

Kolejnym błędem jest używanie tych samych haseł do logowania w wielu miejscach. Pomysł, żeby wszędzie mieć takie samo hasło jest fatalny – wystarczy ujawnienie hasła w jednym miejscu, aby umożliwić hakerowi przejęcie całej prywatnej i służbowej aktywności. Równie złą opcją jest zapisywanie haseł w łatwo dostępnych miejscach, takich jak notesy czy pliki tekstowe. Jeśli ktoś uzyska taki notes lub dostęp do dokumentu na komputerze, może przejąć wszystkie hasła.

Spektakularnym przykładem ataku ransomware, który powiódł się dzięki złamaniu osobistego hasła pracownika, jest przypadek Colonial Pipeline z 2021 roku. Atak spowodował wówczas kilkudniowe zawieszenie pracy rurociągów naftowych zasilających południowo-wschodnie Stany Zjednoczone i kosztował firmę okup w wysokości 4,4 mln USD.

Jak łamane są hasła?

Aby dokonać ataku ransomware na organizację, cyberprzestępcy stosują różne sposoby: brute force, phishing, wyłudzanie danych czy wykorzystywanie wycieków haseł z ataków, które miały miejsce wcześniej. Brute force polega na automatycznym testowaniu ogromnej liczby kombinacji znaków w celu odgadnięcia hasła. Hakerzy używają programów, które w krótkim czasie mogą sprawdzić miliony możliwych haseł. Hasła typu „123456” czy „password”, mogą zostać złamane poniżej sekundy. Cyberprzestępcy korzystają również z tzw. ataków słownikowych, w których testowane są najczęściej używane hasła oraz ich różne warianty.

Phishing i wyłudzanie danych to metody wykorzystujące manipulację użytkownikami, aby sami ujawnili swoje dane logowania. Hakerzy podszywają się pod zaufane instytucje, wysyłając e-maile lub wiadomości SMS z linkami do fałszywych stron logowania. Gdy ofiara wpisze swoje hasło, trafia ono bezpośrednio w ręce przestępców. Coraz częściej hakerzy wykorzystują zaawansowane techniki, takie jak deep fake czy bardziej skuteczne, bo personalizowane, ataki spear phishingowe.

- *Wykorzystanie wycieków haseł to jedna z najprostszych i najczęściej stosowanych metod* – tłumaczy Paweł Kulpa, Cybersecurity Architect z firmy Safesqr i dodaje: - *Gdy użytkownicy stosują te same hasła*

w wielu serwisach, hakerzy mogą użyć baz danych z poprzednich ataków, aby sprawdzić, czy dane logowania pasują do innych kont. Dzięki specjalnym narzędziom mogą automatycznie testować te hasła na różnych platformach, uzyskując dostęp do firmowych systemów, skrzynek e-mail czy kont bankowych.

Długość ma znaczenie

Jednym z kluczowych aspektów ochrony przed cyberatakami jest stosowanie silnych, trudnych do złamania haseł. Długość ma znaczenie - im więcej znaków, tym trudniej je złamania. Silne hasło powinno zawierać małe i wielkie litery, cyfry oraz znaki specjalne. Kombinacja różnych typów znaków zwiększa jego odporność. Poza tym należy unikać łatwych do odgadnięcia fraz – nie należy używać imion, dat urodzenia, numerów telefonów czy popularnych fraz.

Zapamiętywanie wielu skomplikowanych haseł może być trudne, dlatego warto korzystać z menedżerów haseł. Są to narzędzia do przechowywania i generowania silnych haseł, umożliwiające automatyczne logowanie do serwisów. Pozwalają one użytkownikom na bezpieczne przechowywanie haseł i ich synchronizację między urządzeniami.

Uwierzytelnianie dwuskładnikowe (2FA) to jedna z najskuteczniejszych metod zarządzania dostępem. Wymaga dwóch form identyfikacji do uzyskania dostępu do zasobów, czyli nie tylko potwierdzenia tożsamości hasłem, ale dodatkowo kodem SMS, e-mail, w aplikacji uwierzytelniającej lub za pomocą klucza bezpieczeństwa. Coraz częściej w uwierzytelnianiu dwuskładnikowym wykorzystuje się także biometrię, czyli odcisk palca, tęczówkę i siatkówkę oka, twarz czy rozpoznawanie głosu.

- *Najczęściej popełnianym błędem przez użytkowników jest używanie krótkich i przewidywalnych haseł. Cyberprzestępcy dysponują dziś potężnymi narzędziami, które w ciągu sekund mogą złamać słabe hasło metodą brute force albo z użyciem słowników. Stosowanie menedżerów haseł i uwierzytelniania dwuskładnikowego to konieczność w dzisiejszym świecie. Dodatkowo należy pamiętać o tym, że drugi składnik w postaci kodu wysyłanego na email jest bezpiecznych tylko wtedy, jeśli konto pocztowe jest solidnie zabezpieczone przed przejęciem. Im trudniejsze do odgadnięcia hasło i im więcej warstw zabezpieczeń, tym mniejsze ryzyko przejęcia konta* – podkreśla Paweł Kulpa, ekspert ds. cyberbezpieczeństwa.

Regularna zmiana haseł i monitorowanie wycieków

Aby minimalizować ryzyko przejęcia konta, warto regularnie zmieniać hasła, szczególnie do kluczowych usług, takich jak bankowość internetowa czy e-mail. Warto także monitorować, czy nasze dane nie wyciekły do sieci, korzystając z narzędzi takich jak Have I Been Pwned czy bezpiecznedane.gov.pl. W tym pierwszym przypadku wystarczy wprowadzić swój adres e-mail, aby sprawdzić, czy pojawił się w znanych wyciekach danych, w drugim należy użyć profilu zaufanego.

Cyberprzestępcy stale rozwijają swoje metody ataków, dlatego stosowanie silnych haseł, menedżerów haseł, uwierzytelnianie dwuskładnikowe oraz monitorowanie wycieków to niezwykle istotne działania, które pomagają zabezpieczyć nasze dane.

Źródło: IP