ZALECANE SPOSOBY TWORZENIA HASEŁ I LOGOWANIA DO URZĄDZEŃ I SYSTEMÓW TELEINFORMATYCZNYCH

I. WSTĘP

Hasła to powszechnie wykorzystywany, prosty i wszystkim znany sposób chronienia dostępu do poufnych danych i usług. Aby jednak działały skutecznie, muszą być tworzone i stosowane w sposób prawidłowy, w tym dostosowany do aktualnych wymogów technicznych i organizacyjnych. Zmieniają się urządzenia, pojawiają się nowe usługi, dotychczasowa wiedza na temat skuteczności procedur uwierzytelniania jest weryfikowana. Stąd potrzeba aktualizacji rekomendacji dla użytkowników i administratora przede wszystkim w zakresie tworzenia i stosowania haseł oraz projektowania procedur logowania. W ciągu ostatnich kilku lat zmienione zostały obowiązujące od długiego czasu zalecenia mówiące między innymi o potrzebie cyklicznej, profilaktycznej zmiany hasła lub stosowania znaków specjalnych i cyfr w celu jego wzmocnienia. W wielu organizacjach procedury te jednak nadal są stosowane, co ma negatywny wpływ na bezpieczeństwo instytucji oraz użytkowników. Poniżej prezentowane są rekomendacje CERT Polska, mające na celu uporządkowanie i aktualizację wiedzy na ten temat oraz przybliżając inne niż samo hasło metody uwierzytelniania i ochrony dostępu. Zalecenia te bazują na eksperckiej wiedzy i uwzględniają doświadczenia zgromadzone w ciągu ostatnich lat.

II. UWIERZYTELNIANIE

Bezpieczny dostęp do informacji przeznaczonych dla określonej grupy osób zawsze wymaga weryfikacji, czy osoba ubiegająca się o ten dostęp jest tym, za kogo się podaje. Proces udowadniania swojej tożsamości nazywamy uwierzytelnianiem. Najczęściej wymaga on przekazania i weryfikacji tzw. sekretu. Może nim być np. hasło, czy kod PIN. Najważniejszą cechą sekretu jest jego tajność – powinien on być znany tylko uprawnionym osobom. Jest to prosty technicznie mechanizm, który ma jednak pewne mankamenty. Szybki rozwój technologii oraz przenoszenie coraz większej części naszego życia do sfery cyfrowej spowodowały, że liczba systemów, w których musimy się regularnie uwierzytelniać, znacząco wzrosła. Sprawia to, że zapamiętanie silnych, unikalnych haseł do każdego z nich może okazać się problematyczne, bądź wręcz niemożliwe. Z pomocą przychodzą różne mechanizmy i technologie, które mogą sprawić, że będzie to prostsze.

Menadżery haseł

Jednym z narzędzi ułatwiających użytkownikom radzenie sobie z dużą liczbą kont i powiązanych z nimi haseł są programy do zarządzania hasłami, popularnie zwane menedżerami haseł. Istnieje wiele rozwiązań tego typu – od narzędzi wbudowanych w przeglądarkę, po rozwiązania działające w chmurze. Zadaniem tych programów jest umożliwienie bezpiecznego przechowywania haseł, dzięki czemu nie trzeba ich zapamiętywać. Pozwalają one również na generowanie haseł oraz często umożliwiają automatyczne wpisanie hasła, gdy zajdzie potrzeba uwierzytelnienia się. Najczęściej spotykanym przykładem menedżera haseł jest ten wbudowany w przeglądarkę internetową. Jest to rozwiązanie dość powszechnie stosowane i pozwalające na zwiększenie siły haseł niewielkim kosztem. Istnieje jednak pewne ryzyko utraty dostępu do danych przechowywanych w menedżerze haseł. Może to nastąpić np. w przypadku awarii bądź utraty sprzętu. Jeżeli nie zadbaliśmy o przygotowanie kopii zapasowej, odzyskanie dostępu do wielu kont może wymagać przejścia procedur odzyskiwania konta u dostawców usług. To ryzyko jest mniejsze w przypadku rozwiązań chmurowych, gdyż dane nie są bezpośrednio przechowywane na naszym urządzeniu.

Dostawcy tożsamości

Innym rozwiązaniem odciążającym użytkowników są technologie nazywane "dostawcami tożsamości" (ang. identity providers). Są to mechanizmy, umożliwiające stworzenie

jednego miejsca zarządzającego tożsamościami oraz udostępnianie ich innym usługom w celu uwierzytelnienia użytkowników. Przykładem takiego mechanizm jest Single Sign-On (SSO), powszechnie stosowany w środowiskach korporacyjnych. Pozwala on na oddelegowanie konta użytkownika z jednego miejsca w taki sposób, aby inne usługi mogły nas rozpoznać i uwierzytelnić. Podobnym rozwiązaniem jest wykorzystanie mechanizmu OAuth do udostępniania tożsamości zewnętrznym usługom. Jest to obecnie bardzo popularne rozwiązanie, dzięki któremu możemy np. zalogować się do platformy dostawcy muzyki, używając konta w portalu społecznościowym. W ten sposób użytkownik otrzymuje dostęp do wielu usług, wykorzystując tylko jedno hasło, które potwierdza jego tożsamość u dostawcy.

Biometria
Biometria to metoda uwierzytelnienia wykorzystująca "coś czym jesteś" jako czynnik poddawany weryfikacji. Najczęściej stosowane w tym zakresie są odcisk palca, skan twarzy bądź obraz tęczówki oka. Duża dostępność urządzeń biometrycznych w telefonach oraz komputerach osobistych, jej wygoda oraz dojrzałość, jaką technologia ta osiągnęła w sprzęcie konsumenckim po wielu latach udoskonaleń, sprawia, że jest to wygodna oraz często bezpieczna forma uwierzytelnienia. Nie wszystkie systemy i urządzenia jednak pozwalają na uwierzytelnienie z użyciem tej technologii i nie wszędzie jest to najlepsze rozwiązanie.

Uwierzytelnienie dwuskładnikowe
uwierzytelniania użytkowników dzieli się na 3 grupy ze względu na weryfikowany czynnik. Sprawdzeniu mogą podlegać:

1. Coś, co znasz – np. hasło lub kod PIN
2. Coś, co posiadasz – np. token sprzętowy, telefon, karta Smart Card
3. Coś, czym jesteś – np. odcisk palca lub skan tęczówki oka

Metody uwierzytelnienie dwuskładnikowe polega na weryfikacji dwóch z trzech powyższych elementów. Najczęściej stosowaną kombinacją jest hasło (coś co znasz) plus jeden z czynników z którejś z pozostałych grup. Drugi składnik stanowi dodatkową warstwę bezpieczeństwa. Popularnie stosowanym drugim składnikiem są m.in. kody SMS, kody generowane przez token sprzętowy, albo potwierdzenie operacji w odpowiednio skonfigurowanej wcześniej aplikacji. Zastosowanie tego rozwiązania uniemożliwia atakującemu, który pozyskał nasz login i hasło, uwierzytelnienie się w usłudze, jeżeli nie zdobędzie on również drugiego składnika.

III. REKOMENDACJE DLA TWORZENIA WŁASNYCH HASEŁ

Zalecenia zawarte w tym dokumencie bazują na aktualnych publikacjach międzynarodowych takich jak NIST Digital Identity Guidelines czy materiałach opublikowanych przez FBI w ramach akcji Protected Voices, oraz na obserwacjach i doświadczeniu CERT Polska, zbudowanych podczas własnych badań przez tę instytucję i obsługi licznych incydentów bezpieczeństwa.

Rekomendacje CERT Polska zalecane do stosowania:
Poniżej prezentowane są rekomendowane wymagania dla polityki haseł.

1. Brak wymuszonej okresowej zmiany haseł użytkowników
2. Blokada tworzenia hasła znajdującego się na liście słabych/często używanych haseł
3. Blokada hasła zawierającego przewidywalne człony (np. nazwa firmy, usługi)
4. Minimalna długość hasła – co najmniej 12 znaków
5. Limit znaków w haśle nie mniejszy niż 64 znaki
6. Brak dodatkowych kryteriów złożoności, np. znaków specjalnych, cyfr czy dużych liter

Ad.1 wyjaśnienie: dnia 6 lutego 2019 uchylone zostało Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji

przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wymagające okresowej zmiany haseł w systemach przetwarzających dane osobowe. Więcej informacji na stronie: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20041001024

Ad. 2: CERT Polska publikuje polską wersję słownika haseł będącą wynikiem analizy danych upublicznionych w wyciekach. Zawiera on zestaw około miliona najpopularniejszych haseł, posortowanych malejąco od haseł najbardziej popularnych. Może on posłużyć administratorom systemów przy wdrożeniu polityki haseł zgodnej z zaleceniami.

Ad. 3: Limit 12 znaków jest minimalną długością hasła. Zalecane jest ustawianie haseł dłuższych, budowanych w oparciu o całe zdanie. Więcej informacji o tworzeniu haseł znajduje się w sekcji Hasła silne i łatwe do zapamiętania.

Uzasadnienie powyższych rekomendacji.
Skupiono się na długości hasła zamiast jego złożoności, ponieważ badania wskazują, że jest to znacznie ważniejszy czynnik, wpływający na jego bezpieczeństwo. Zrezygnowano również z wymuszania okresowej zmiany haseł, ponieważ powstające w jej wyniku nowe hasła są najczęściej wariacją poprzednich, zazwyczaj skonstruowane w łatwy do przewidzenia sposób. Badania pokazują, że użytkownicy nie są w stanie zapamiętać całkiem nowego silnego hasła np. co miesiąc. Zamiast wymogów złożoności hasła, skupiono się na wykluczeniu haseł w oczywisty sposób prostych, najczęściej używanych, przewidywalnych, bądź ujawnionych w wyciekach. Należą do tej grupy hasła, które są np. zbudowane według prostych schematów, ale także najpopularniejsze imiona, zwroty czy nazwy własne. W zasadzie wszystkie słowniki używane do łamania haseł zawierają na początku listy hasła typu 123456, zaq1@WSX, albo słowo password. Należy również uwzględnić łatwe do przewidzenia składowe hasła, jak nazwa firmy, czy usługi. Dodawanie tego typu elementów do hasła tylko nieznacznie zwiększa jego bezpieczeństwo. Przykładowo, hasło zaq1@wsxCERT, można uznać za równie słabe jak zaq1@wsx, w przypadku użycia przez wyłudzającego dane.

Hasła silne i łatwe do zapamiętania
Silne hasło można zbudować na wiele sposobów. Najbardziej oczywistym wydaje się wylosowanie bardzo długiego ciągu znaków i wykorzystanie menedżera haseł do jego zapisania. Takie hasło jest jednak trudne do zapamiętania przez człowieka. Przykładem sytuacji, w której potrzebne jest silne, łatwe do zapamiętania hasło jest hasło do bazy danych menedżera haseł, albo do konta użytkownika w systemie operacyjnym – gdy nie mamy jeszcze dostępu do menedżera.

Jak budować silne hasła
W celu stworzenia silnego hasła, które będziemy w stanie zapamiętać, można używać zasady pełnych zdań. Należy unikać znanych cytatów czy powiedzeń, ale po modyfikacji mogą nam one posłużyć jako inspiracja. Tak stworzone hasło powinno składać się z przynajmniej pięciu słów.
WlazlKostekNaMostekIStuka – jest (to znaczy było, przed użyciem go tutaj) silnym hasłem, które można łatwo zapamiętać.
Inną wartą polecenia metodą jest budowanie hasła z opisu wyimaginowanej sceny, której obraz jest łatwy do zapamiętania i jednoznacznego opisania:
zielonyParkingDla3malychSamolotow – jest przykładem takiego hasła. Przy czym należy zwrócić uwagę, że scena, którą opisuje nasze hasło, powinna zawierać jakiś element nierealistyczny albo abstrakcyjny. Wynika to z tego, że ludzie mają tendencję do używania obiektów, z którymi mieli ostatnio styczność, widzą je, albo są w ich pobliżu, jako składowe wymyślonego hasła. Pozwala to na użycie mniejszego słownika przy próbie łamania haseł, poprzez dostosowanie go pod konkretną osobę lub grupę osób.

Kolejnym pomysłem na generowanie silnego hasła jest użycie słów z kilku języków.
Przykładem takiego hasła może być:
DwaBialeLatajaceSophisticatedKroliki. Jego siła bierze się z tego, że próby łamania haseł opartych o całe zdanie muszą zostać wykonane metodą słownikową, a takie słowniki najczęściej zawierają słowa/zwroty z jednego języka.

Hasła pozornie silne
Dotychczasowe, powszechnie stosowane zalecenia tworzenia haseł nie prowadziły do budowania haseł silnych. Pozornie silne hasła, takie jak:
Galwaniczny123$
zaq1@WSXcde3$RFV
admin.1admin.1admin.1admin.1
nie są dostatecznie silne, aby oprzeć się atakowi w przypadku wycieku bazy danych, w której się znajdują. W bazach danych hasła zazwyczaj są przechowywane w formie zabezpieczonej, ale odkrycie ich pierwotnej formy jest możliwe. Hasła schematyczne i tworzone zgodnie z przewidywalnymi regułami są proste do "złamania" za pomocą coraz doskonalszych narzędzi wykorzystujących słowniki i listy reguł modyfikujących każde słowo ze słownika. Takie podejście do łamania zabezpieczonych haseł pozwala w prosty sposób wygenerować powyższe hasła, nawet jeśli w pełnej formie nie były dostępne w użytym słowniku. Zarówno słowniki jak i zestawy reguł są publicznie dostępne a moc obliczeniowa potrzebna do przeprowadzenia skutecznego ataku jest stosunkowo niewielka. Znikomy jest też czas na to potrzebny i koszt takiej operacji.
Przykład:
Powyższe hasła są przykładami haseł złamanych podczas z testu wewnętrznego CERT Polska. Pracownicy CERT Polska zostali poproszeni o wygenerowanie prawdopodobnych do użycia haseł i zabezpieczenie ich przestarzałym algorytmem (SHA1). Złamanie powyższych haseł zajęło poniżej 5 minut.
Natomiast w przypadku haseł odpowiednio długich, zbudowanych zgodnie z przedstawionymi powyżej zaleceniami, potrzeba użycia mocy obliczeniowej a także czas i koszt ataku rosną wielokrotnie.

UWAGA!
Według naszej najlepszej wiedzy nie istnieje aktualnie publicznie dostępne narzędzie oraz metoda pozwalająca na skuteczny atak na hasła zbudowane zgodnie z przedstawionymi wcześniej rekomendacjami. Teoretyczny, optymalnie przeprowadzony atak na przykładowe hasło WlazlKostekNaMostekIStuka, zabezpieczone przestarzałym algorytmem SHA1 zająłby co najmniej setki lat. Oczywiście od momentu użycia go w tym dokumencie, jego wartość jako sekretu jest znikoma.

Podsumowanie
Odpowiednie podejście zarówno do polityki haseł jak i ich tworzenia i zarządzania nimi jest istotnym problemem dla administratorów i użytkowników systemów informatycznych. W tym dokumencie zostały przedstawione i omówione rekomendacje, które powinny spełniać nasze Firmowe systemy, aby zapewnić odpowiedni poziom bezpieczeństwa haseł użytkowników. Ponadto przedstawione zostały zalecenia jak pracownicy winni tworzyć i zarządzać silnymi hasłami, wraz z przykładami rozwiązań technologicznych upraszczających ten proces. Zwraca się również uwagę na przestarzałe zalecenia i ich negatywny wpływ na bezpieczeństwo. Na przykładzie haseł pozornie silnych pokazano, jak niewielkie nakłady finansowe w połączeniu ze standardowymi metodami, stanowią realne zagrożenie w przypadku wycieków haseł nieodpowiednio zabezpieczonych oraz niedostatecznie silnych.

Źródło: CERT Polska