Dobre praktyki dotyczące silnych haseł i uwierzytelniania wieloskładnikowego.

Spis treści

Dobre praktyki dotyczące silnych haseł i uwierzytelniania wieloskładnikowego

Stosowanie silnych haseł jest niezbędne do ochrony naszych danych osobowych i finansowych przed cyberprzestępcami. Przestępcy kradną dane uwierzytelniające, uzyskując nieautoryzowany dostęp do cennych kont. Jednocześnie istnienie darknetu, w którym kupowane i sprzedawane są skradzione dane uwierzytelniające, napędza cyfrowy czarny rynek. Oprócz zrozumienia zagrożeń, organizacje muszą również zapoznać się z najnowszymi technologiami i strategiami obronnymi, które mogą chronić je przed ciągłym napływem cyberataków.

Znaczenie silnych haseł i uwierzytelniania wieloskładnikowego

Silne hasła mają kluczowe znaczenie w dzisiejszym cyfrowym świecie, ponieważ technologie takie jak uczenie maszynowe (*ang. Machine Learning - ML*) i karty z procesorami graficznymi (*ang. Graphics Processing Unit - GPU*) ułatwiają atakującym łamanie haseł. Równie ważne jest stosowanie unikalnych haseł. Nawet jeśli masz silne hasło do jednego konta, naruszenie bezpieczeństwa jednej platformy może narazić inne konta, jeśli mają one te same dane uwierzytelniające. Połączenie siły i unikalności hasła ma kluczowe znaczenie dla zwiększenia bezpieczeństwa w Internecie.

Ponadto wdrożenie uwierzytelniania wieloskładnikowego (MFA - multi-factor authentication) jest absolutną koniecznością. Zapewnia dodatkową warstwę ochrony przed nieautoryzowanym dostępem, znacznie wzmacniając bezpieczeństwo. Co więcej, połączenie MFA z rozwiązaniami pojedynczego logowania (SSO- single sign-on) tworzy mocną i wygodną dla użytkownika kombinację. Wdrożenie (SSO) pozwala użytkownikom logować się do wielu aplikacji przy użyciu jednego zestawu danych uwierzytelniających, co upraszcza dostęp. w połączeniu z uwierzytelnianiem wieloskładnikowym (MFA) metoda ta może zmniejszyć utrudnienia, zapewnić wysoki poziom bezpieczeństwa i zwiększyć wydajność operacyjną.

Czym jest MFA?

Uwierzytelnianie wieloskładnikowe (MFA) to środek bezpieczeństwa, który chroni osoby fizyczne i organizacje, wymagając od użytkowników podania co najmniej dwóch czynników uwierzytelniających w celu uzyskania dostępu do aplikacji, konta lub wirtualnej sieci prywatnej (VPN). Rozwiązanie zapewnia wielowarstwowe zabezpieczenia wirtualne, aby zagwarantować, że każda osoba uzyskująca dostęp do systemu, mogła zostać zautoryzowana oraz uwierzytelniona.

Jak działa uwierzytelnianie wieloskładnikowe (MFA)?

Użytkownik najpierw proszony jest o podanie nazwy użytkownika i hasła, czyli standardowych danych logowania, ale następnie musi zweryfikować swoją tożsamość w inny sposób. Najczęściej wymaga to wprowadzenia kodu przesłanego pocztą

elektroniczną, SMS-em, za pośrednictwem aplikacji mobilnej do uwierzytelniania lub na urządzenie dodatkowe, ale inne formy mogą obejmować sprzęt skanujący dane biometryczne lub wcześniej ustalone pytania zabezpieczające.

Ten drugi, a nawet trzeci czynnik w procesie uwierzytelniania służy do weryfikacji, czy żądanie użytkownika jest autentyczne i nie zostało naruszone.

Przykłady uwierzytelniania wieloskładnikowego

MFA wykorzystuje trzy popularne metody uwierzytelniania w celu weryfikacji tożsamości użytkownika:

1. **Wiedza**: Jest to czynnik, który użytkownicy znają najlepiej. Użytkownik jest proszony o podanie informacji, które zna, takich jak hasło, osobisty numer identyfikacyjny (PIN), klucz bezpieczeństwa lub odpowiedź na pytanie zabezpieczające.
2. **Posiadanie**: ten czynnik weryfikuje tożsamość użytkownika za pomocą czegoś, co posiada. Na przykład poprzez wysłanie kodu na telefon komórkowy.
3. **Cechy wrodzone**: ten czynnik weryfikuje osobę na podstawie unikalnych cech osobistych, takich jak uwierzytelnianie biometryczne lub rozpoznawanie głosu.

Oprócz powyższych czynników, czynnik lokalizacji i/lub czynnik czasu mogą zapewnić dodatkowe warstwy ochrony w określonych środowiskach.

Najważniejsze zalety korzystania z uwierzytelniania wieloskładnikowego

MFA zapewnia ochronę zarówno organizacji, jak i indywidualnych użytkowników. Korzyści związane z bezpieczeństwem organizacji mogą obejmować:

1. **Zwiększoną ochronę**: Naruszenia bezpieczeństwa powodują utratę zasobów, zwłaszcza danych, czasu i pieniędzy. MFA pomaga chronić te cenne aktywa.
2. **Bezpieczne środowisko pracy zdalnej**: Pracownicy mający łatwy dostęp do wszystkich systemów i danych potrzebnych do wykonywania pracy są bardziej produktywni. Firmy stosujące MFA pomagają utrzymać elastyczność i sprawność środowiska pracy zdalnej.
3. **Ochrona wielowymiarowa**: Stosowanych jest wiele warstw zabezpieczeń, dzięki czemu w przypadku celowego lub przypadkowego naruszenia jednej warstwy ochrony, warstwy drugorzędne i trzeciorzędne (i tak dalej) zapewniają wsparcie, gwarantując organizacji maksymalny poziom ochrony.

Zalecenia dotyczące wdrażania uwierzytelniania wieloskładnikowego

1. Zapewnij wygodę obsługi dla użytkownika – np. biometria, hasła jednorazowe.
2. Wzmocnij MFA za pomocą SSO – jednokrotne logowanie do wielu aplikacji.
3. Wdrożenie adaptacyjnego MFA - uwierzytelnianie wielopoziomowe uwzględniające dane kontekstowe np. adres IP, lokalizacja.

4. Wprowadź MFA w całej organizacji spójnie dla wszystkich użytkowników, urządzeń i działów organizacji.
5. Wypróbuj metody bez haseł - logowanie za pomocą serwisów społecznościowych, dane biometryczne itp.
6. Przeprowadzaj regularne audyty MFA - optymalizacja procesów MFA ma kluczowe znaczenie dla utrzymania kompleksowego bezpieczeństwa.
7. Promuj świadomość bezpieczeństwa aplikacji.

Rozwiązania poprawiające cyberodporność

Poniżej przedstawiono rozwiązania, które organizacje powinny rozważyć w celu dalszego wzmocnienia swojego bezpieczeństwa.

- **Zapobieganie rozprzestrzenianiu się złośliwego oprogramowania za pomocą systemów EDR:** Nowoczesne systemy wykrywania i reagowania na zagrożenia na punktach końcowych (EDR - endpoint detection and response) odgrywają kluczową rolę. Mają uniemożliwić rozprzestrzenianie się oprogramowania wewnątrz sieci. Stanowią one integralną część nowoczesnego cyberbezpieczeństwa.
- **Wykrywanie wycieku danych uwierzytelniających za pomocą usług rekonesansu**: Jednym z największych wyzwań jest identyfikacja sytuacji, w której dane uwierzytelniające organizacji zostały naruszone i są sprzedawane w darknecie. Korzystając z usług rekonesansu, organizacje mogą proaktywnie wykrywać potencjalne naruszenia i reagować na nie z wyprzedzeniem
- **Potrzeba szybkości i automatyzacji we współczesnym cyberbezpieczeństwie**: Systemy wykrywające naruszenia bezpieczeństwa stale monitorują ruch sieciowy, punkty końcowe i przepływ danych w celu identyfikacji wszelkich podejrzanych działań lub obecności naruszonych danych uwierzytelniających. Po wykryciu incydentu platformy SOAR (security orchestration, automation, and response) służą jako centrum operacyjne, są wyposażone w dostosowane do potrzeb playbooki, które określają szereg automatycznych działań, które należy podjąć w przypadku wykrycia określonych zagrożeń.