OUCH! Styczeń 2023

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Biometria

Wstęp

Czy używanie haseł jest dla ciebie męczące? Masz dość pamiętania wszystkich haseł lub wpisywanie ich za każdym razem podczas logowania do serwisów? A może jesteś sfrustrowany koniecznością wymyślania nowych haseł lub okresową ich zmianą? Mamy dla Ciebie dobrą wiadomość. Istnieje takie rozwiązanie jak biometria. Poniżej przedstawimy czym są dane biometryczne i w jaki sposób ułatwiają życie.

Po pierwsze, dlaczego hasła?

Hasła są częścią uwierzytelniania oraz pewnego rodzaju procesem potwierdzającym czy jesteś tym, za kogo się podajesz. Zazwyczaj są dwie informacje, którymi możesz potwierdzić swoją tożsamość: coś co wiesz (np. hasło) oraz coś co posiadasz (np. karta płatnicza lub urządzenie mobilne). Tradycyjnie uwierzytelnianie odbywa się za pomocą haseł. Hasła zostały wdrożone, ponieważ było to jedno z najłatwiejszych do zaimplementowania rozwiązań uwierzytelniających. Jednak z biegiem lat nasze życie stało się o wiele bardziej skomplikowane. Każdy z nas posiada wiele kont, znacznie więcej niż ktokolwiek by się tego spodziewał. Nikogo już nie dziwi używanie ponad 100 haseł w życiu prywatnym oraz zawodowym.

Cyberprzestępcy na przestrzeni lat dopracowali techniki odgadywania, kradzieży i łamania haseł. To dlatego istnieje tak wiele zasad dotyczących haseł, takich jak odpowiednia długość hasła (więc są trudne do odgadnięcia) i używanie unikalnego hasła dla każdego konta (więc jeśli jedno z twoich kont zostanie przejęte, to inne konta są nadal bezpieczne). Problem z wszystkimi wymaganiami dotyczącymi haseł jest taki, że bycie bezpiecznym staje się problematyczne, szczególnie w zapamiętywaniu tak wielu haseł. Istnieją takie programy jak menedżery haseł, które znacznie pomagają w zapamiętywaniu haseł, poprzez przechowywanie ich wszystkich w jednej bazie, do której musisz pamiętać zaledwie jedno hasło. Ale czy istnieje lepszy sposób? To właśnie tutaj pojawia się biometria, która zapewnia trzecią rzecz do potwierdzenia tożsamości - czyli coś czym jesteś.

Biometria

Podobnie jak hasła, dane biometryczne to kolejny sposób na potwierdzenie kim jesteś. Różnica polega na tym, że zamiast coś pamiętać (hasła) używasz elementu tego kim jesteś aby potwierdzić tożsamość, np. używasz odcisku palca lub skanu twarzy, aby uzyskać dostęp do telefonu.

Biometria jest znacznie prostsza, ponieważ nie musisz nic pamiętać ani wpisywać. Po prostu uwierzytelniasz się używając tego kim jesteś. Istnieje wiele różnych rodzajów danych biometrycznych, poza odciskiem palca czy skanu twarzy, wyróżniamy m.in. głos, sposób chodzenia, wygląd tęczówki, postura. Jednak odcisk palca czy rozpoznawanie twarzy, to dwie najczęściej używane dane biometryczne, zwłaszcza w przypadku urządzeń mobilnych. Chociaż dane biometryczne mają ogromną liczbę zalet, mają również pewne wady. Jedną z największych jest to, że danych biometrycznych nie zmienisz jeśli cyberprzestępcy skopiują odcisk palca lub twarz.

Passkeys

W ciągu najbliższych miesięcy lub lat powinieneś zacząć widzieć biometrię zastępującą hasła za pomocą nowej technologii o nazwie Passkeys. Technologia ta jest obecnie wdrażana przez firmy Microsoft, Apple i Google, i wkrótce powinna być wdrażana na coraz większej liczbie witryn internetowych. Passkeys zastąpią hasła, umożliwiając udowodnienie kim jesteś poprzez proste użycie biometrii połączonej z urządzeniem mobilnym. Gdy będziesz zakładał konto w serwisie internetowym (np. Google lub Apple), zamiast tworzyć hasło, rejestrujesz swoje urządzenie mobilne. W konsekwencji tego, logujesz się do witryny, uwierzytelniając się za pomocą urządzenia mobilnego przy użyciu danych biometrycznych, takich jak odcisk palca lub rozpoznawanie twarzy. Witryna ufa urządzeniu mobilnemu, a samo urządzenie mobilne potwierdza użytkownika danymi biometrycznymi. Co ważne, dane biometryczne (odcisk palca lub wizerunek twarzy) nie są przesyłane do żadnej strony internetowej. Zamiast tego, są bezpiecznie przechowywane lokalnie na urządzeniu. Passkey jest pewnego rodzaju unikalnym kluczem tworzonym dla każdej witryny, które urządzenie wysyła do witryny, chroniąc jednocześnie dane biometryczne użytkownika. Chociaż żadne rozwiązanie nie jest idealne, biometria i rozwiązania takie jak Passkeys, mogą pomóc w utrzymaniu bezpieczeństwa, jednocześnie upraszczając je.

Redaktor gościnny

Dr Johannes Ullrich jest dziekanem ds. badań w kolegium SANS Technology Institute. Mając ponad 20-letnie doświadczenie w branży, obecnie monitoruje bieżące zagrożenia prowadząc SANS Internet Storm Center. Prowadzi zajęcia z SEC522 (Web Application Security) oraz SEC503 (Intrusion Detection).
Twitter: @johullrich & LinkedIn: https://www.linkedin.com/in/johannesullrich/.

Źródła

Menedżer haseł: https://www.sans.org/newsletters/ouch/password-managers/
Więcej o Passkeys (ang.): https://www.sans.org/blog/what-is-phishing-resistant-mfa/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz