Biometria - wygoda czy zagrożenie?

Kategoria: Styl życia
Opublikowano: piątek, 05, lipiec 2024 08:44
Tomasz Smaś

Biometria jest coraz częściej wykorzystywana nie tylko jako metoda zabezpieczania urządzeń elektronicznych, ale również płatności. Choć cechy biometryczne są unikalne dla każdego człowieka, nie oznacza to, że są w 100 proc. bezpieczne. Skalę zagrożeń dopiero poznamy, mówią eksperci z HackerU Polska - choć dodają, że są sposoby ochrony przed nimi.

Skany tęczówki oka, nagrania głosu, kształt twarzy czy odciski palców są coraz częściej wykorzystywane jako metody odblokowania telefonu, dostępu do biur czy domów po autoryzację transakcji w sklepach i bankach. Choć są unikalne dla każdego człowieka mogą być niewystarczającą formą ochrony - przestępcy również na nie znaleźli swoje metody. Istnieją jednak sposoby na zabezpieczenie się przed takim zagrożeniem.

Odcisk palca czy wzór tęczówki są absolutnie niepowtarzalne, stąd wydają się być idealnym zabezpieczeniem i metodą autoryzacji. Tym bardziej, że możliwe są wielostopniowe metody, wykorzystujące zarówno skan tęczówki jak i owal twarzy. Dlatego też coraz częściej wykorzystywane są przez sklepy jako metody płatnicze. Zresztą jedna z największych sieci sprzedaży książek i wydawnictw muzycznych w Polsce wraz z Mastercard i PayEye w czerwcu, w kilku swoich salonach rozpoczęła testy tej nowej metody płatniczej.

W 2023 r. globalny rynek rozwiązań w zakresie tożsamości cyfrowej, którego głównym elementem jest biometria, warty był 34,5 mld. dolarów i według prognoz analityków firmy Statista w nadchodzących latach będzie szybko rósł.

Co ciekawe odciski palców stosowane były jako metoda autoryzacji, choćby transakcji, już od setek lat. Tymczasem, jak zwracają uwagę eksperci z HackerU, w ciągu ostatnich kilku lat hakowanie danych biometrycznych stało się coraz popularniejszym sposobem uzyskiwania przez przestępców dostępu do wrażliwych danych. Niestety udaje im się ominąć tradycyjne środki bezpieczeństwa, takie jak hasła i kody PIN, korzystając ze specjalnych narzędzi i technik w celu uzyskania dostępu do poufnych informacji. Atak taki może zostać przeprowadzony poprzez przechwycenie danych podczas ich transmisji lub pobranie ich z miejsca przechowywania, jak choćby baza danych. Gdy atakujący zdobędzie dane biometryczne, może je wykorzystać do podszywania się pod ofiarę i uzyskania dostępu do jej kont lub poufnych informacji.

Przekonała się o tym brytyjska firma Arup, tracąc 25 milionów dolarów, gdy oszuści wykorzystali cyfrowo sklonowany wizerunek dyrektora finansowego, który zlecił przelewy podczas wideokonferencji. Hakerzy użyli zarówno przekazu wideo z wizerunkiem dyrektora jak i idealnie skopiowali jego głos co zmyliło pracowników, którzy w ten sposób autoryzowali przelew.

Choć istnieje ponad 20 różnych rodzajów danych biometrycznych, takich jak odciski palców (linie papilarne czy skan naczyń krwionośnych), twarz lub głos to każdy z nich może zostać naruszony na kilka różnych sposobów.

- Nie ma czegoś takiego jak niezawodne bezpieczeństwo. Choć niektóre dane biometryczne (np. tęczówka lub siatkówka oka) mogą być trudniejsze do złamania niż inne formy identyfikacji, takie jak hasło czy PIN, zdeterminowani hakerzy mogą znaleźć sposób na ominięcie również takich zabezpieczeń poprzez działania socjotechniczne (np. pobranie odcisków palców i zrobienie kopii czy użycie zdjęcia ofiary w kontekście przełamania zabezpieczeń opartych o rozpoznawanie twarzy) – mówi Maciej Cieśla - Head of Cybersecurity HackerU Polska

Kategoria: Styl życia
Opublikowano: piątek, 05, lipiec 2024 08:44
Tomasz Smaś
Odsłony: 1609

Jednym ze sposobów na ich zdobycie jest użycie urządzenia zwanego skimmerem. Można go umieścić w bankomatach lub innych skanerach linii papilarnych. Skimmer zbiera informacje ze skanu palca, a następnie tworzy fałszywy odcisk, za pomocą którego można uzyskać dostęp do danego urządzenia. Inną techniką hakowania danych biometrycznych jest fałszowanie. Technika ta polega na użyciu fałszywego odcisku palca lub tęczówki, który wygląda na tyle podobnie do prawdziwego, że można oszukać skaner. Atak ten może zostać przeprowadzony poprzez zrobienie zdjęcia palca lub tęczówki danej osoby albo wykonanie wręcz modelu palca. Kolejny sposób naruszenia bezpieczeństwa danych biometrycznych jest tak zwany „atak polegający na powtórzeniu". Ten ostatni polega na przechwyceniu komunikacji klienta np. z bankiem i powtórzenie takiego samego zlecenia w oparciu o podane już dane uwierzytelniające, ale na nowy np. przelew.

Dane biometryczne są cenne, w 2015 r. amerykańskie Biuro ds. Zarządzania Personelem padło ofiarą ataku, w wyniku którego przestępcy przejęli dane 5,6 miliona osób, co czyni to jednym z największych znanych naruszeń danych biometrycznych. Rok później badacze z Michigan State University udowodnili, że możliwe jest stworzenie fałszywych odcisków palców, które mogą oszukać skanery linii papilarnych. Dokonali tego w laboratorium dysponując cyfrowymi skanami odcisków oraz drukarkami żelatynowymi i atramentowymi. Dlatego dzisiaj coraz częściej stosowane są skany układu naczyń krwionośnych w palcu, a nie samych linii papilarnych.

Co więcej wraz z rozwojem technologii deepfake hakowanie biometryczne stało się znacznie bardziej wyrafinowane, ale jednocześnie bardziej dostępne dla cyberprzestępców. Opcją jest tworzenie wizerunku osoby, ale także jej głosu z wykorzystaniem jej zdjęć czy filmów zamieszczanych choćby w mediach społecznościowych.

- *Dane biometryczne służące do odblokowania urządzenia nie są łatwe do uzyskania, ponieważ zazwyczaj są przechowywane na urządzeniu w postaci zaszyfrowanego kodu binarnego. Jednak otwieranie aplikacji zawierających dane biometryczne lub umożliwianie im korzystania z nich nie zawsze jest odpowiednim rozwiązaniem. Czasami konsumenci przekazują swoje dane, nawet zupełnie nie wiedząc, kto stoi za aplikacją, która je otrzymuje. Co więcej tajemnicą są dalsze sposoby wykorzystywania zebranych danych* - mówi Patryk Bogdan - konsultant ds. cyberbezpieczeństwa oraz trener w HackerU Polska

Co więcej nawet jeśli są tylko przechowywane na serwerze lub w chmurze to wówczas mogą zostać wykradzione, co udaje się nawet ze zbiorami danych gromadzonych przez rządy. Może to nastąpić również podczas przechwycenia transmisji danych pomiędzy urządzeniem użytkownika a pamięcią masową.

- *Biometria jest dobrym zabezpieczeniem, jednak naprawdę skuteczna będzie tylko wtedy, gdy jest stosowana jako część uwierzytelniania wieloskładnikowego, czyli korzysta się z więcej niż jednego sposobu uwierzytelniania* - podsumowuje Maciej Cieśla - Head of Cybersecurity HackerU Polska.

Podstawowe pytanie jakie należy sobie zadać to komu się przekazuje swoje dane biometryczne. Nie da się ich zmienić, więc dany podmiot niejako na zawsze zyskuje do nich dostęp. Co innego, gdy trafią do banku, a co innego, gdy ma je dopiero tworzący się startup z drugiego końca świata.

Źródło: IP