Transakcje

Analiza porównawcza mechanizmów uwierzytelniania

2024

MIKOŁAJ PACEK, BARTOSZ GRZYBOWSKI, DAWID RYBA, MATEUSZ WIRKIJOWSKI, MIESZKO MAKOWSKI, PATRYK MOTYLSKI

Spis treści

Hasła klasyczne

To najprostszy i najbardziej tradycyjny mechanizm uwierzytelniania, polegający na wpisaniu tajnego ciągu znaków, który zna jedynie użytkownik.

Hasła są najbardziej uniwersalnym i szeroko stosowanym mechanizmem uwierzytelniania. Można je używać na komputerach, telefonach, stronach internetowych, aplikacjach mobilnych, oraz w wielu systemach operacyjnych.

Tworzenie i wprowadzanie haseł jest proste, ale wymaga od użytkownika ich zapamiętania. Może to prowadzić do problemów, jeśli użytkownicy wybierają słabe, łatwe do zapamiętania hasła, które są mniej bezpieczne.

Aspekty techniczne

Wdrożenie systemu opartego na hasłach jest bardzo tanie i nie wymaga specjalistycznego sprzętu ani oprogramowania. Niemal każdy system może obsługiwać hasła bez dodatkowych kosztów.

Bezpieczeństwo

W przypadku hasła, zabezpieczenia zależą głównie od jego złożoności i długości. Dobrze dobrane, długie hasła są trudniejsze do złamania, ale ...

Wygoda

W praktyce użytkownicy często wybierają krótkie, łatwe do odgadnięcia hasła. Dlatego warto korzystać z managera haseł.

Odporność na ataki

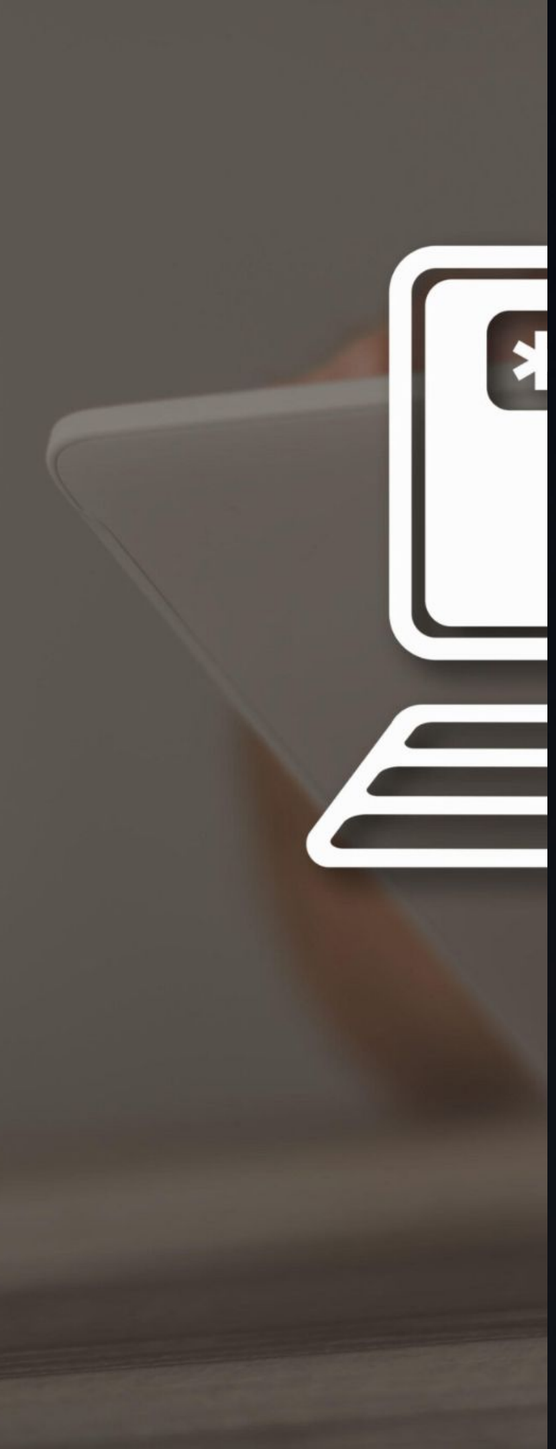
Hasła są podatne na różnorodne ataki, takie jak phishing, brute force, keyloggery czy ataki typu dictionary. Jeśli użytkownicy stosują te same hasła na różnych platformach, jeden wyciek może prowadzić do nieautoryzowanego dostępu do wielu usług. Ataki z wykorzystaniem słabych haseł, zwłaszcza tych krótkich lub popularnych (np. "123456"), są powszechne.

Dwuskładnikowa autoryzacja

to mechanizm zabezpieczający dostęp poprzez zastosowanie dwóch odrębnych warstw ochrony. Użytkownik po wprowadzeniu hasła użytkownik musi dodatkowo potwierdzić swoją tożsamość za pomocą drugiego czynnika

Takie podejście minimalizuje ryzyko nieautoryzowanego dostępu, ponieważ po przełamaniu przez atakującego jednej warstwy zabezpieczenia istnieje jeszcze jedna zupełnie odrębna, a złamanie dwóch naraz jest znacznie trudniejsze.

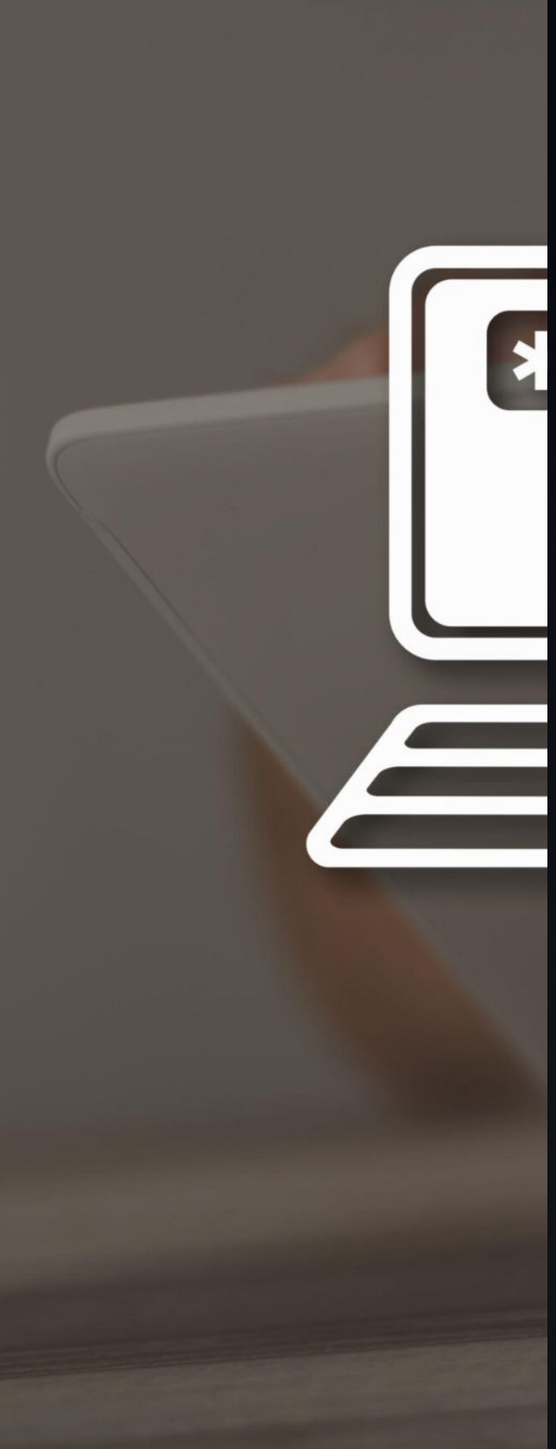
Popularne formy 2FA obejmują kody SMS, aplikacje uwierzytelniające czy fizyczne tokeny. Wprowadzenie tego mechanizmu minimalizuje ryzyko nieautoryzowanego dostępu i zwiększa zaufanie użytkowników do systemu.



Dwuskładnikowa autoryzacja

Możliwe formy wdrożenia:

- Tokeny sprzętowe
- Klucze bezpieczeństwa
- Weryfikacja SMS
- Powiadomienia PUSH
- Aplikacje uwierzytelniające
- Weryfikacja e-mail

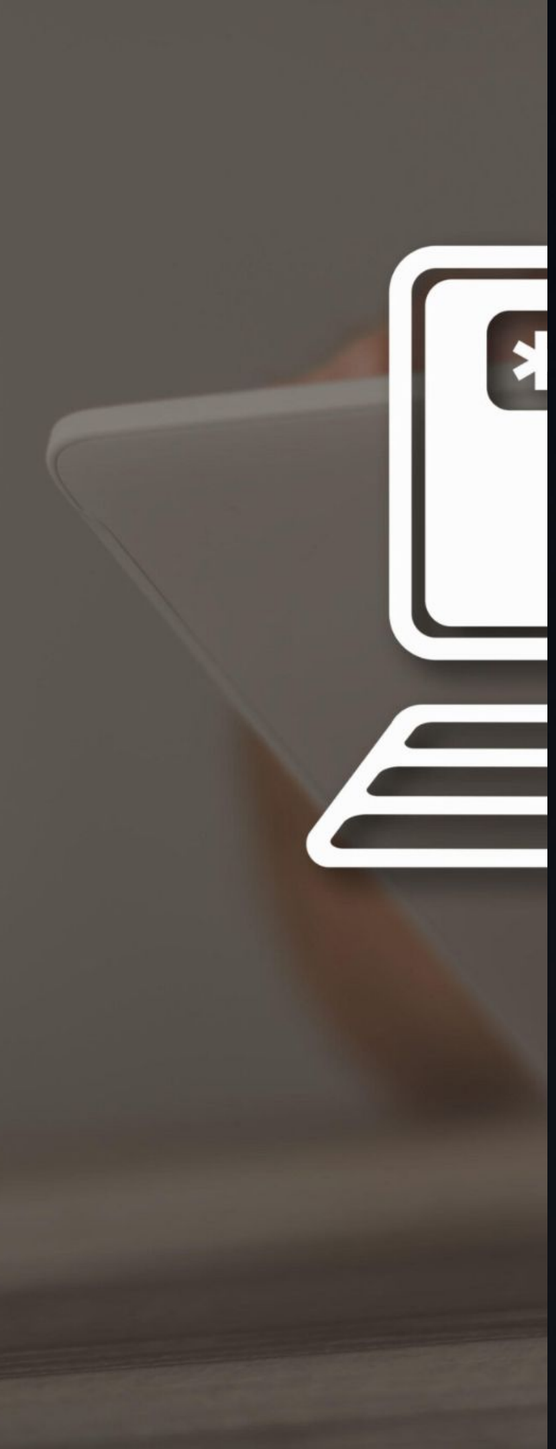


Dwuskładnikowa autoryzacja

Możliwe formy wdrożenia:

- **Tokeny sprzętowe**
  - Klucze bezpieczeństwa
  - Weryfikacja SMS
  - Powiadomienia PUSH
  - Aplikacje uwierzytelniające
  - Weryfikacja e-mail

To fizyczne urządzenia, które generują jednorazowe kody (np. RSA SecurID). Użytkownik wpisuje kod generowany przez urządzenie podczas logowania. Tokeny sprzętowe są odporne na ataki online, ponieważ działają offline i nie są połączone z internetem. Chociaż bardzo bezpieczne, wymagają noszenia dodatkowego urządzenia, co może być niewygodne dla użytkowników.

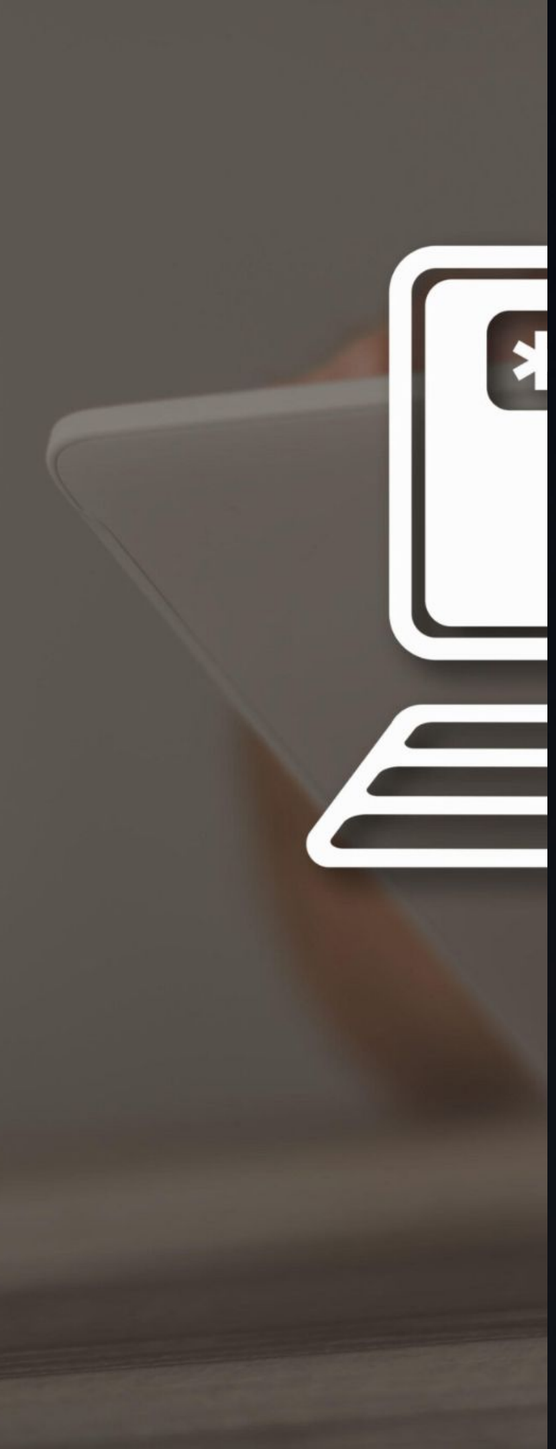


Dwuskładnikowa autoryzacja

Możliwe formy wdrożenia:

- Tokeny sprzętowe
- **Klucze bezpieczeństwa**
- Weryfikacja SMS
- Powiadomienia PUSH
- Aplikacje uwierzytelniające
- Weryfikacja e-mail

Klucze bezpieczeństwa, jak np. YubiKey lub Google Titan, działają w oparciu o protokoły takie jak FIDO U2F i są podłączane bezpośrednio do portu USB lub łączą się z urządzeniem przez NFC lub Bluetooth. Umożliwiają bezpieczną autoryzację logowania przez jedno kliknięcie kluczu, eliminując potrzebę przepisywania kodów. Są wygodne i bardzo bezpieczne, choć wymagają fizycznego dostępu do klucza.

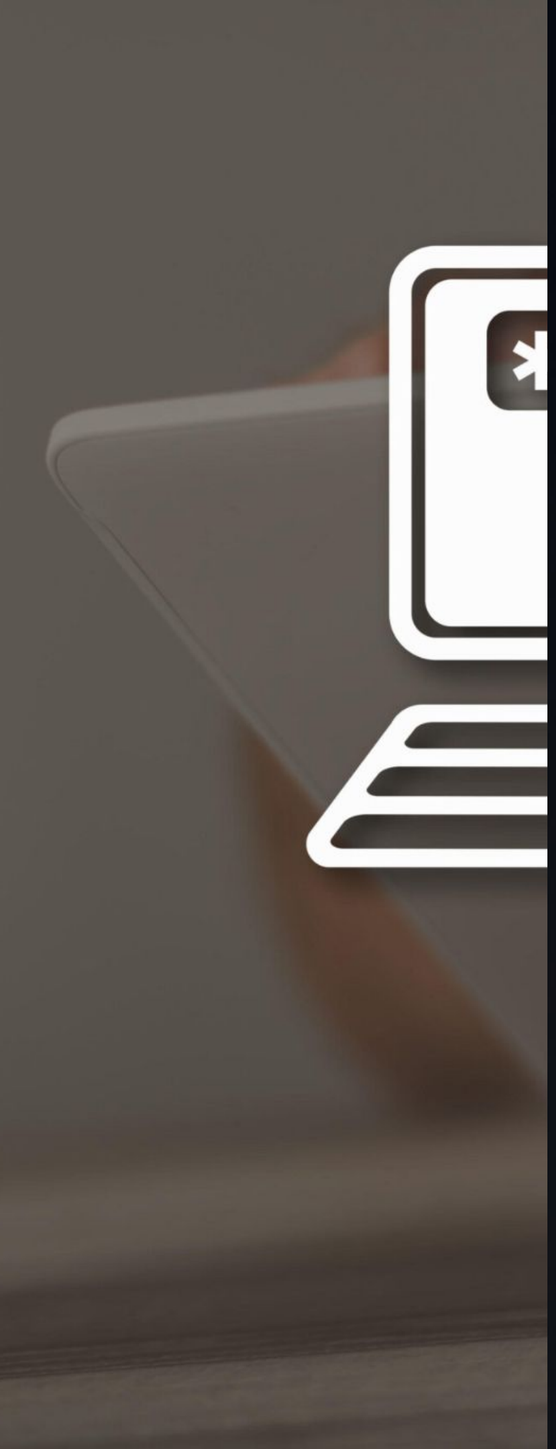


Dwuskładnikowa autoryzacja

Możliwe formy wdrożenia:

- Tokeny sprzętowe
- Klucze bezpieczeństwa
- **Weryfikacja SMS**
- Powiadomienia PUSH
- Aplikacje uwierzytelniające
- Weryfikacja e-mail

Użytkownik otrzymuje kod jednorazowy w wiadomości SMS, który następnie wpisuje podczas logowania. Ta metoda jest bardzo popularna i łatwo dostępna, ponieważ nie wymaga specjalnych aplikacji – wystarczy telefon. Warto jednak zauważyć, że jest podatna na ataki typu SIM swapping, gdzie atakujący przejmuje numer telefonu użytkownika.

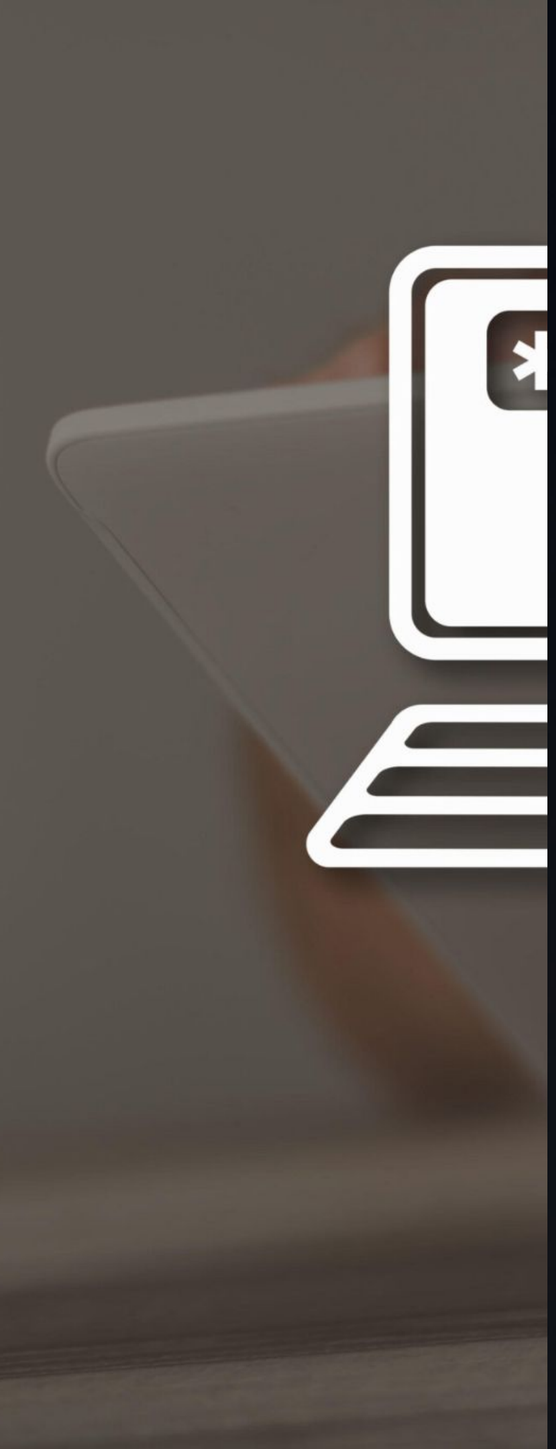


Dwuskładnikowa autoryzacja

Możliwe formy wdrożenia:

- Tokeny sprzętowe
- Klucze bezpieczeństwa
- Weryfikacja SMS
- **Powiadomienia PUSH**
- Aplikacje uwierzytelniające
- Weryfikacja e-mail

Aplikacje, takie jak Duo Mobile czy Microsoft Authenticator, wysyłają na telefon użytkownika powiadomienie push z prośbą o potwierdzenie logowania. Wystarczy jedno kliknięcie, aby je zatwierdzić, co sprawia, że metoda ta jest szybka, wygodna i często bardziej bezpieczna niż SMS-y, ponieważ wymaga bezpośredniego dostępu do urządzenia mobilnego.

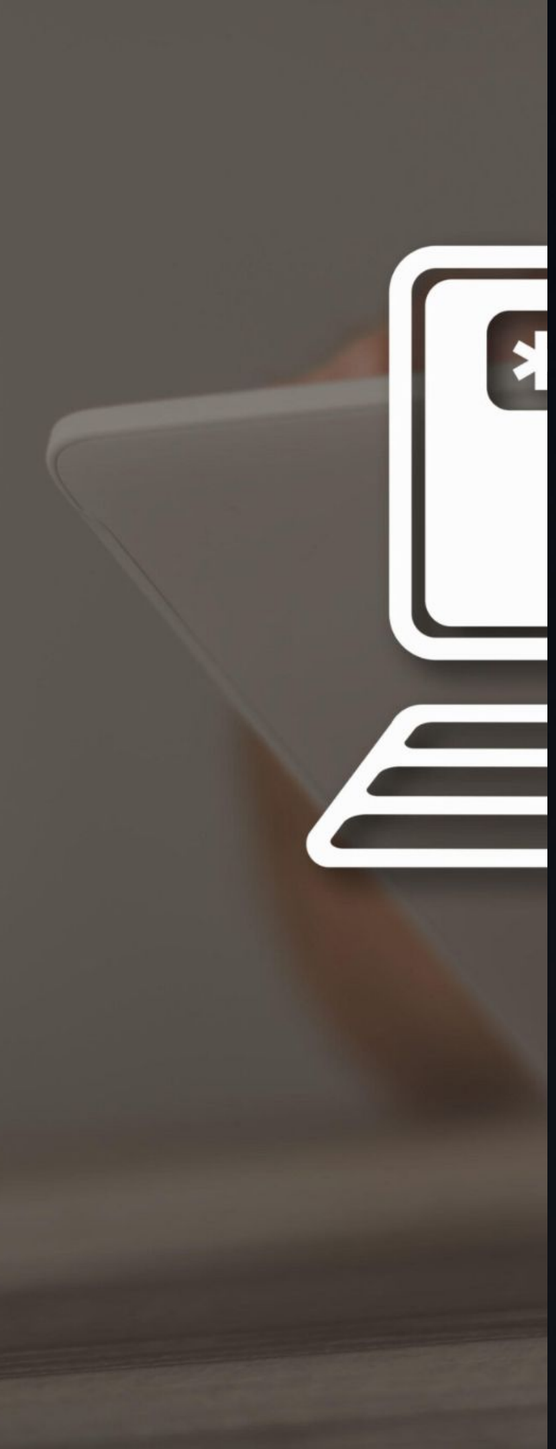


Dwuskładnikowa autoryzacja

Możliwe formy wdrożenia:

- Tokeny sprzętowe
- Klucze bezpieczeństwa
- Weryfikacja SMS
- Powiadomienia PUSH
- **Aplikacje uwierzytelniające**
- Weryfikacja e-mail

Klasyczne aplikacje do generowania kodów, takie jak Google Authenticator, Authy czy Microsoft Authenticator, tworzą jednorazowe kody (TOTP) ważne przez określony czas, które użytkownik wpisuje przy logowaniu. Aplikacje te działają offline, co zmniejsza ryzyko przechwycenia kodów przez atakujących, i są wygodną alternatywą dla SMS-ów.



Dwuskładnikowa autoryzacja

Możliwe formy wdrożenia:

- Tokeny sprzętowe
- Klucze bezpieczeństwa
- Weryfikacja SMS
- Powiadomienia PUSH
- Aplikacje uwierzytelniające
- Weryfikacja e-mail

Kod jednorazowy lub link potwierdzający wysyłany jest na adres e-mail użytkownika. Choć jest to mniej bezpieczne niż inne metody, e-mail może stanowić dodatkowy poziom uwierzytelnienia, jeśli jest stosowany razem z inną formą 2FA. Niestety, metoda ta jest narażona na ryzyko, jeśli konto e-mail użytkownika jest słabo zabezpieczone.

Aspekty techniczne

Wprowadzenie 2FA nie wymaga zazwyczaj kosztownego sprzętu ani skomplikowanego oprogramowania.

Bezpieczeństwo

2FA oferuje wysoki poziom poufności, gdyż dostęp do konta wymaga dwóch niezależnych składników autoryzacji.

Wygoda

Dla użytkownika końcowego proces korzystania z 2FA jest zazwyczaj prosty i intuicyjny – wymaga jedynie dodatkowego kroku w logowaniu

Klucze sprzętowe

To zewnętrzne urządzenie najczęściej przypominające pendrive’a, stosowane do potwierdzania tożsamości użytkownika, często korzystające z protokołów takich U2F lub FIDO2.

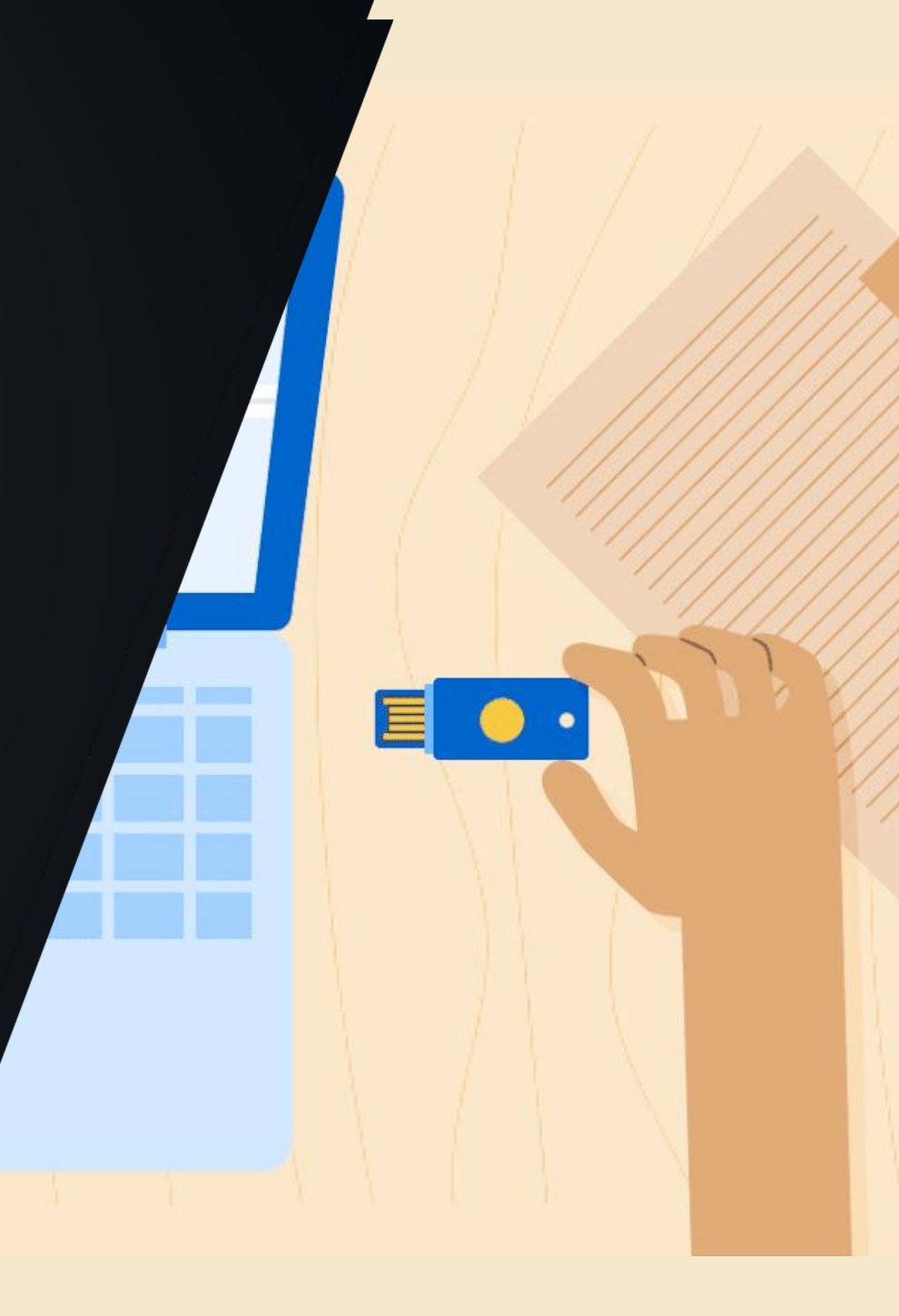
Można je używać na komputerach, telefonach, stronach internetowych, aplikacjach mobilnych, oraz w wielu systemach operacyjnych.

Gama funkcjonalności kluczy i ich różne modyfikacje umożliwiają dobre dostosowanie do potrzeb użytkownika.

Aspekty techniczne

Bezpieczeństwo

Funkcjonalność



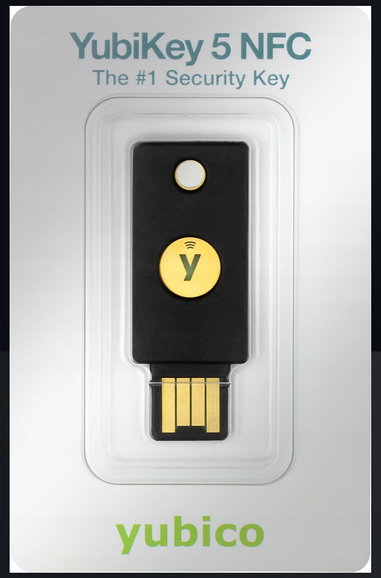
Podatności

ATAKI

Utrata

Złamanie kodu

Przykłady kluczy sprzętowych dostępnych na rynku



YUBIKEY 5C NFC

233 zł

GOOGLE TITAN SECURITY KEY

121,82 zł

ONLY KEY DUO-DUAL USB C/USB A

207 zł

KENSINGTON K64708JP

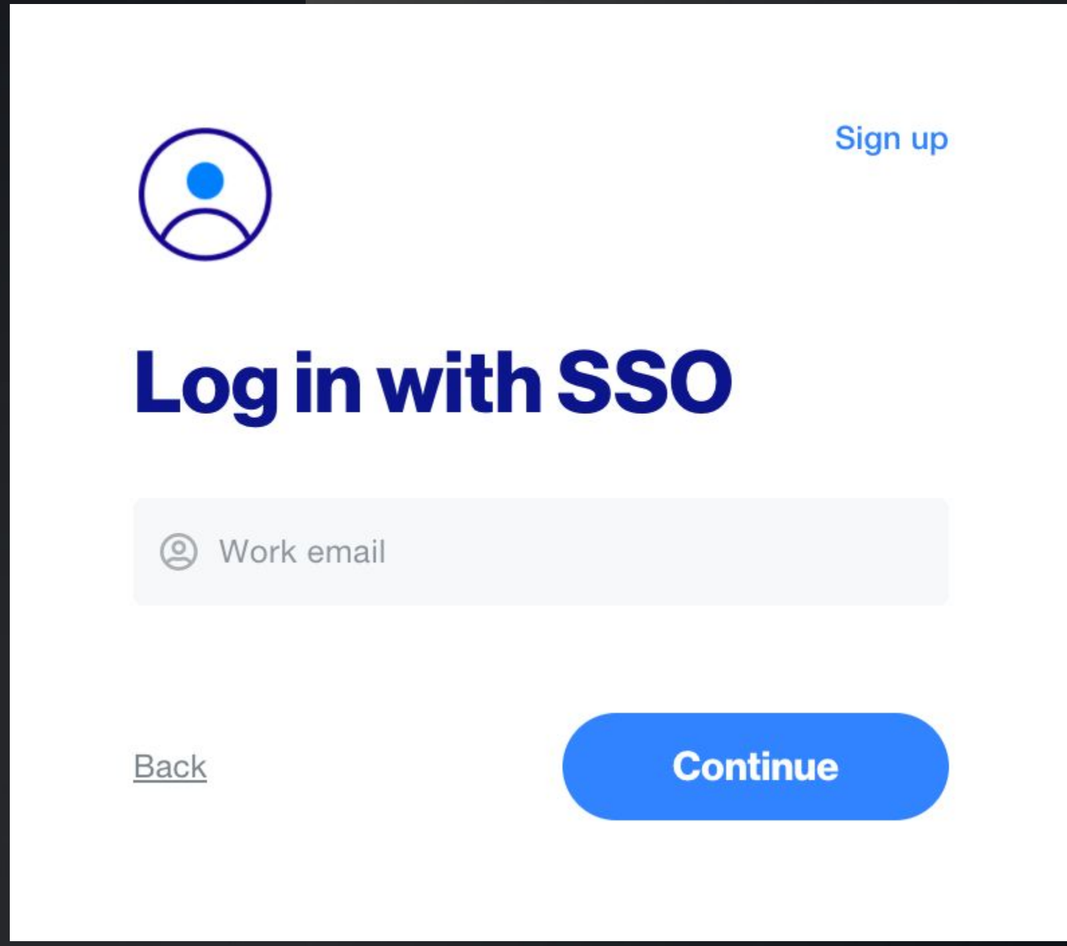
231,67 zł

Single Sign-On

To mechanizm uwierzytelniania, który pozwala użytkownikowi zalogować się jednorazowo i uzyskać dostęp do wielu aplikacji i systemów bez potrzeby powtarzania procesu logowania.

Single Sign-On (SSO) znacznie ułatwia zarządzanie tożsamością w złożonych środowiskach IT. Dzięki SSO użytkownik wprowadza dane uwierzytelniające tylko raz, co redukuje potrzebę zapamiętywania wielu haseł.

Mechanizm ten poprawia wygodę korzystania z systemów i zmniejsza ryzyko związane z wielokrotnym używaniem słabych haseł. Jednocześnie centralne zarządzanie sesjami w SSO umożliwia administratorom szybsze wyłączanie dostępu w razie konieczności, zwiększając poziom bezpieczeństwa całej infrastruktury.



Aspekty techniczne

SSO pozwala na lepsze kontrolowanie dostępu do zasobów, a także szybkie reagowanie w przypadku ewentualnych naruszeń.
Administratorzy również mają ułatwiony sposób monitorowania działań użytkowników.

Bezpieczeństwo

Warto jednak pamiętać, by sam system SSO, był odpowiednio zabezpieczony i chroniony przed wyciekiem danych np za pomocą MFA.

Wygoda

Użytkowanie z SSO jest bardzo proste, wystarczy zalogować się w systemie, a wszystkie dostępy do zasobów z nim zintegrowanych zostaną przekazane użytkownikowi

Odporność na ataki

- Złamanie dostępu do SSO przez atakującego może skutkować przejęciem dostępu do wszystkich zasobów.

- Właśnie z tego powodu SSO, jest często wspierane dodatkowym zabezpieczeniem w postaci np MFA, które znacznie podnosi poziom bezpieczeństwa.

Warto również zaznaczyć, że systemy SSO są także podatne na ataki:

- phishingowe oraz MiTM, lecz stosowanie silnego zabezpieczenia (co jest ułatwione dzięki potrzebie zapamiętania jednego hasła zamiast kilku do każdego z osobnych zasobów) może ograniczyć ryzyka wynikające z tego typu ataków.

Biometria

Jako mechanizm uwierzytelniania, służy do identyfikacji użytkowników na podstawie ich cech charakterystycznych. Mogą być to cechy fizyczne jak i behawioralne.

Przykłady identyfikatorów biometrycznych:

- Odcisk palca,
- DNA,
- Tęczówka,
- Rogówka,
- Bicie serca,
- Pisanie na klawiaturze,
- Głos,
- Geometria dłoni.

Skanery linii papilarnych oraz kamery już od dłuższego czasu stanowią standard rynkowy. Koszty oraz wygoda użytkownika determinowane są głównie przez wybrany identyfikator, na podstawie którego będziemy rozpoznawać użytkownika.

Aspekty techniczne

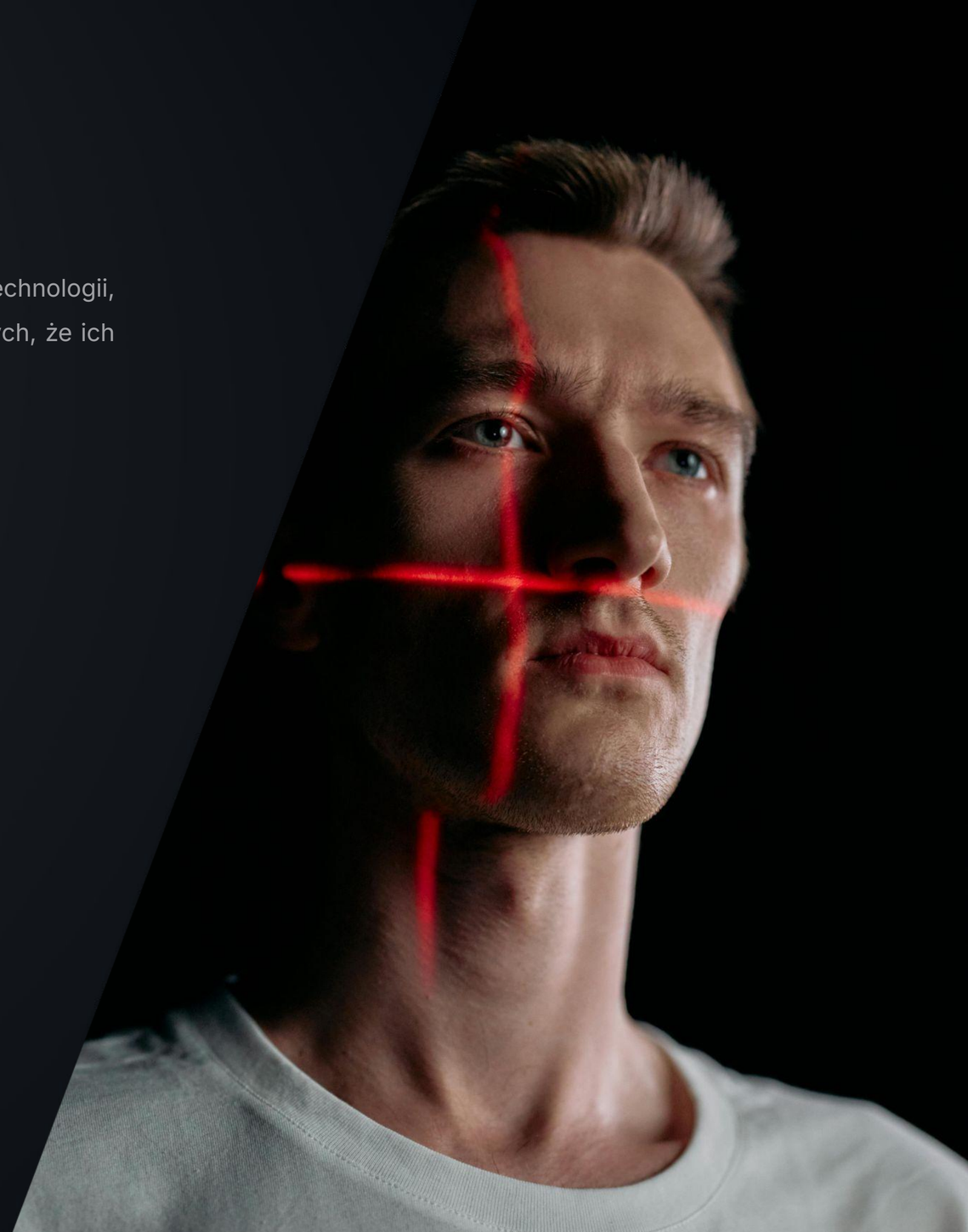
Wymogi techniczne różnią się w zależności od wybranych technologii, jednak wiele rozwiązań jest już na tyle popularnych i powszechnych, że ich zastosowanie nie wiąże się z nadmiernymi inwestycjami.

Bezpieczeństwo

Powiązanie z unikalnymi cechami użytkownika sprawia, że rozwiązanie to zapewnia solidną ochronę. Decyzja o tym, czy użytkownik jest faktycznie tym, za kogo się podaje, opiera się na obliczonym prawdopodobieństwie.

Wygoda

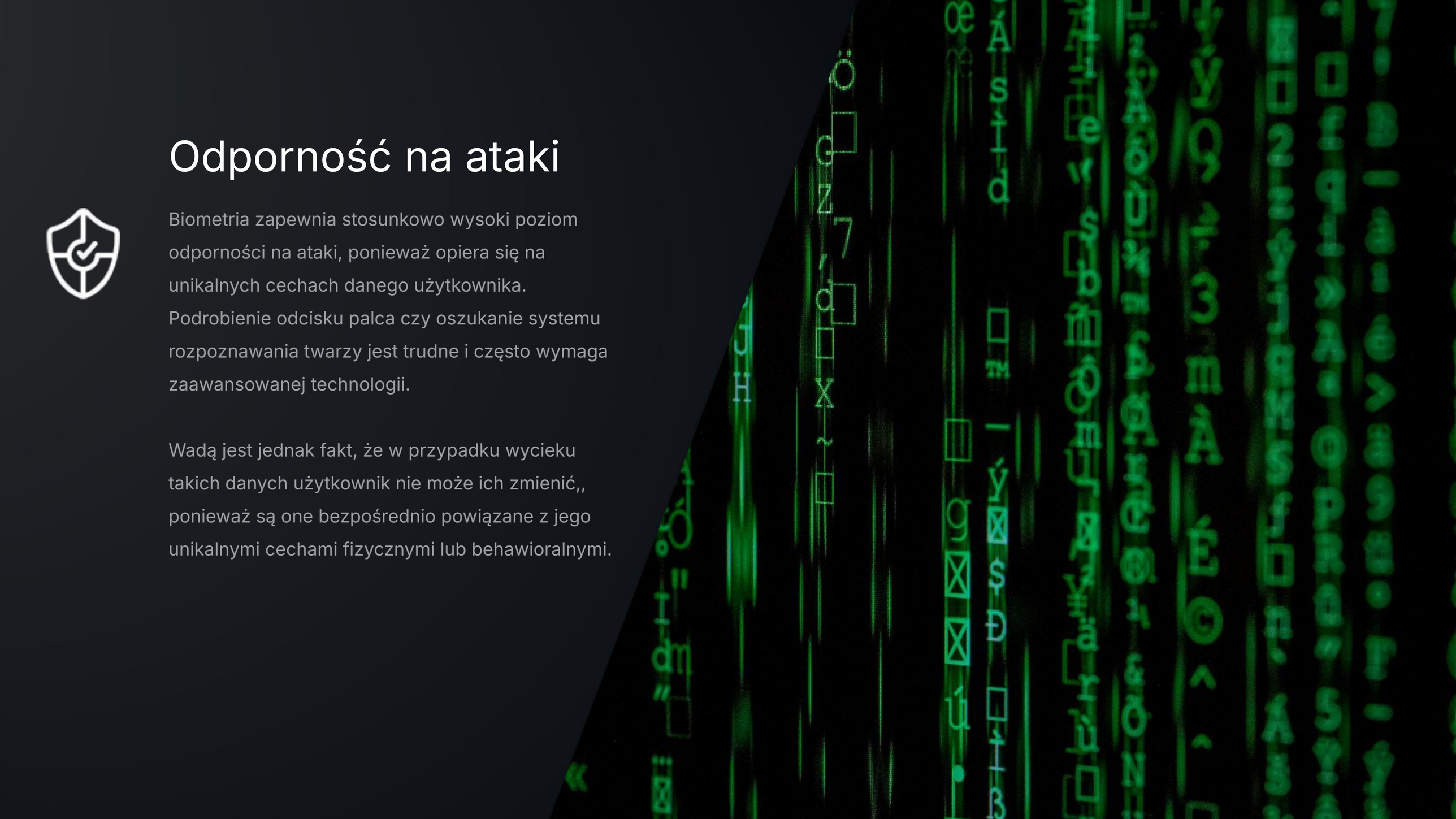
Biometria jest stosunkowo przyjazna dla użytkowników końcowych, ponieważ najczęściej wymaga minimalnej interakcji z ich strony. Współczesne mechanizmy wdrażane do codziennego użytku są wysoce zautomatyzowane.



Odporność na ataki

Biometria zapewnia stosunkowo wysoki poziom odporności na ataki, ponieważ opiera się na unikalnych cechach danego użytkownika. Podrobienie odcisku palca czy oszukanie systemu rozpoznawania twarzy jest trudne i często wymaga zaawansowanej technologii.

Wadą jest jednak fakt, że w przypadku wycieku takich danych użytkownik nie może ich zmienić,, ponieważ są one bezpośrednio powiązane z jego unikalnymi cechami fizycznymi lub behawioralnymi.



Przykłady rozwiązań dostępnych na rynku - skanery

FS80H USB FINGERPRINT SCANNER

~150 zł

BIOLITE N2

~3000 zł

LG4000

~1000 zł

ICAM TD100

~7500 zł

Przykłady rozwiązań dostępnych na rynku - DNA

HOME DNA KIT

~350 zł

BADANIE CAŁOGENOMOWE

~7500 zł

O Auth 2.0

Zwykle używany jako protokół autoryzacji, umożliwia aplikacjom dostęp do zasobów użytkownika w innej usłudze, bez konieczności podawania loginu i hasła do tej aplikacji. Do uwierzytelniania może korzystać np. z tokenu **JWT.**

JWT (JSON Web Token)

JWT (JSON Web Token) - stosowany do uwierzytelniania bądź autoryzacji w aplikacjach. Jest samowystarczalny i lekki. Serwer przy początkowym uwierzytelnieniu tworzy token i wysyła go do klienta, który potem pokazuje właśnie ten token zamiast ponownego procesu logowania.

Uniwersalność

OAuth2.0 i JWT są niezwykle uniwersalnymi narzędziami, który można wykorzystać zarówno w aplikacjach jak i w API. Wykorzystywane przez wielu dostawców tożsamości, co pozwala na łatwą integrację i zachęca do wykorzystania.

Koszty wdrożenia

Zarówno O Auth jak i JWT są darmowymi narzędziami, których jedynym kosztem jest sama implementacja.

Funkcjonalność

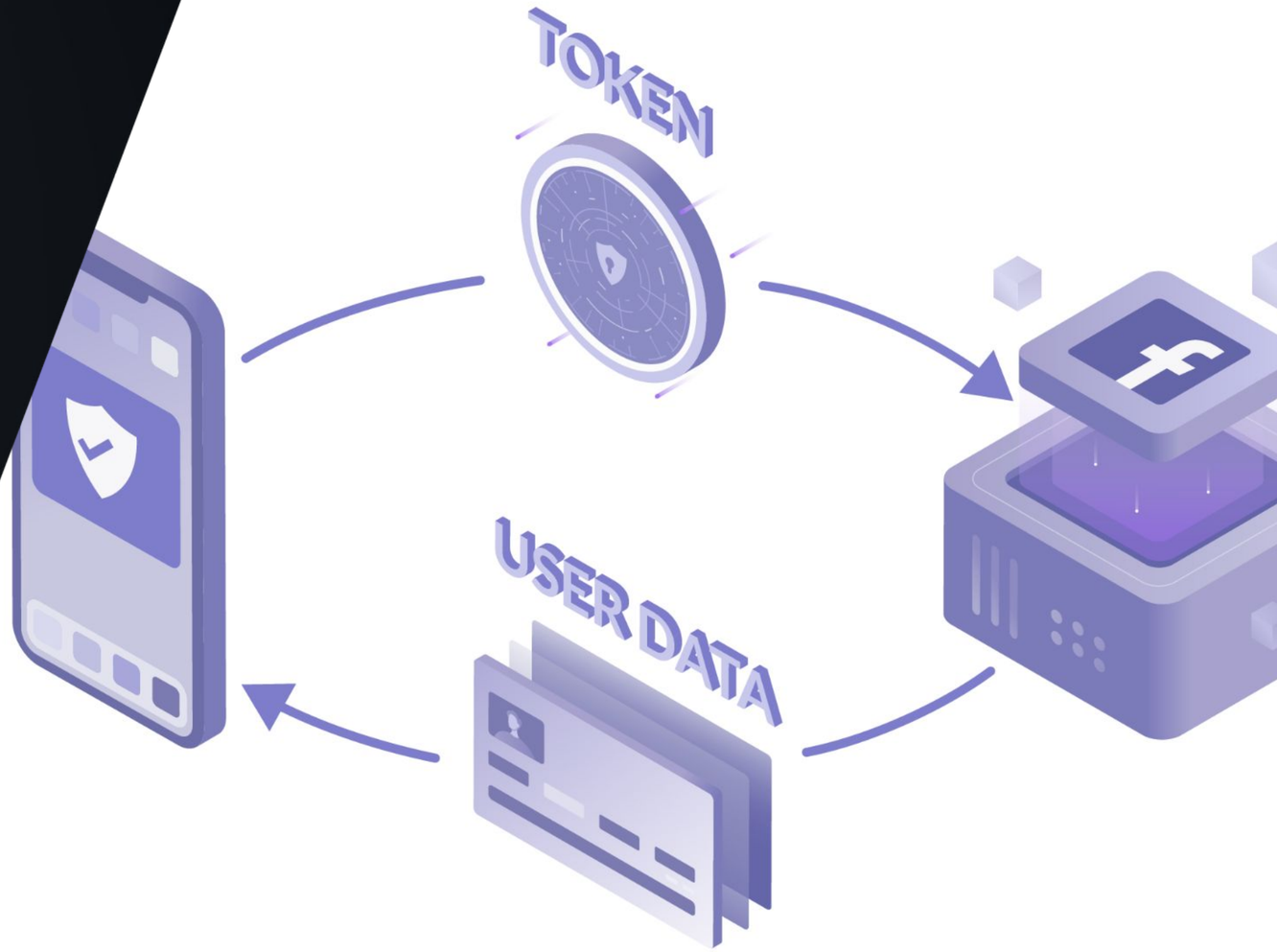
O Auth pozwala wprowadzić bardzo wygodne logowanie jednokrotne oraz integrację z kontami użytkownika z innych serwisów.

Odporność na ataki

O Auth 2.0 i JSON Web Token oferują zaawansowane mechanizmy obrony przed atakami takimi jak Cross-Site Request Forgery, czy man-in-the-middle.

Jednakże te technologie nie są zabezpieczone przed specyficznymi atakami, wykorzystującymi wyciek tokenu poprzez XSS lub manipulacje algorytmem podpisu.

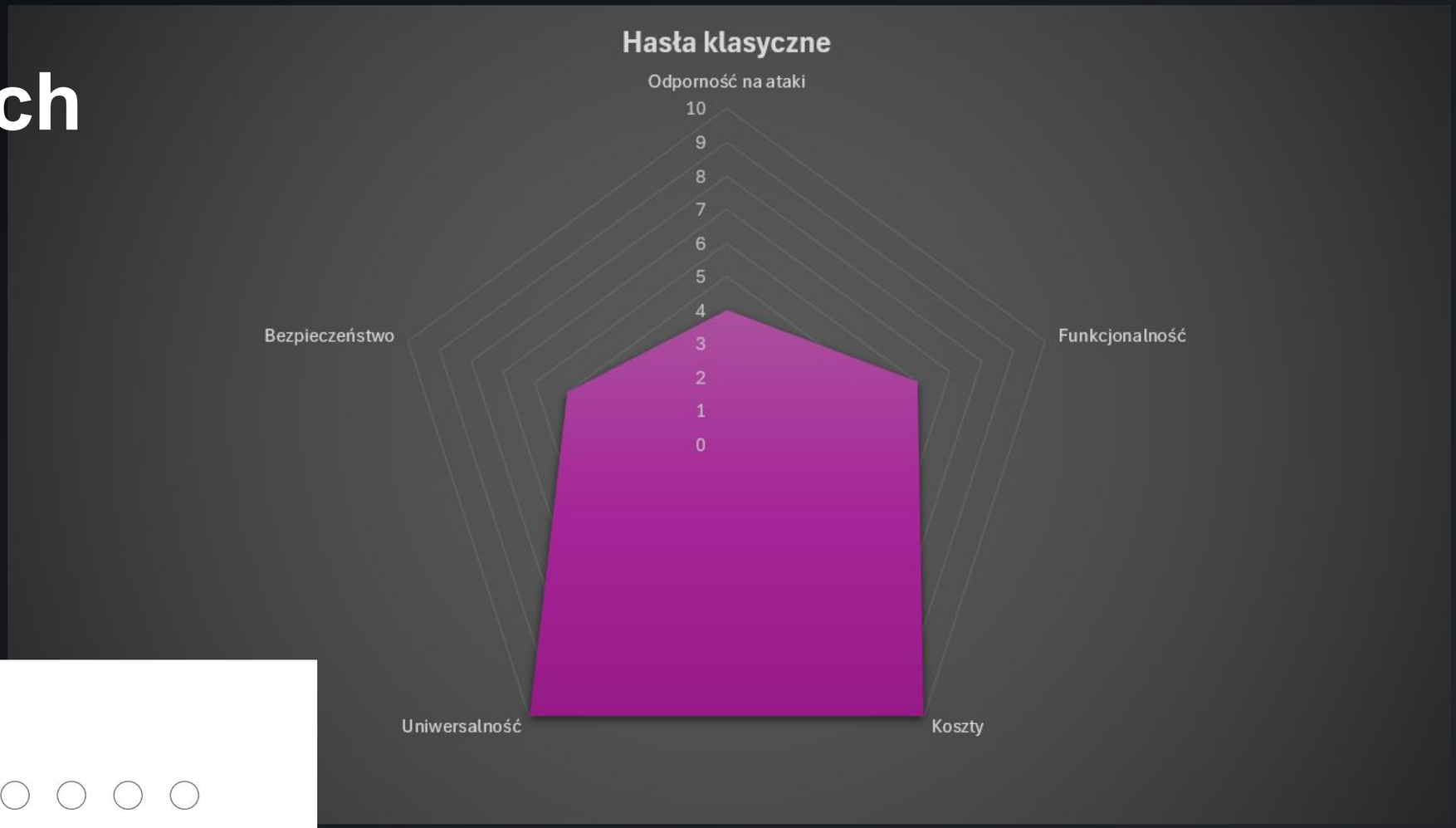
Odporność na ataki zależy od doświadczenia i wiedzy programistów implementujących te technologie.

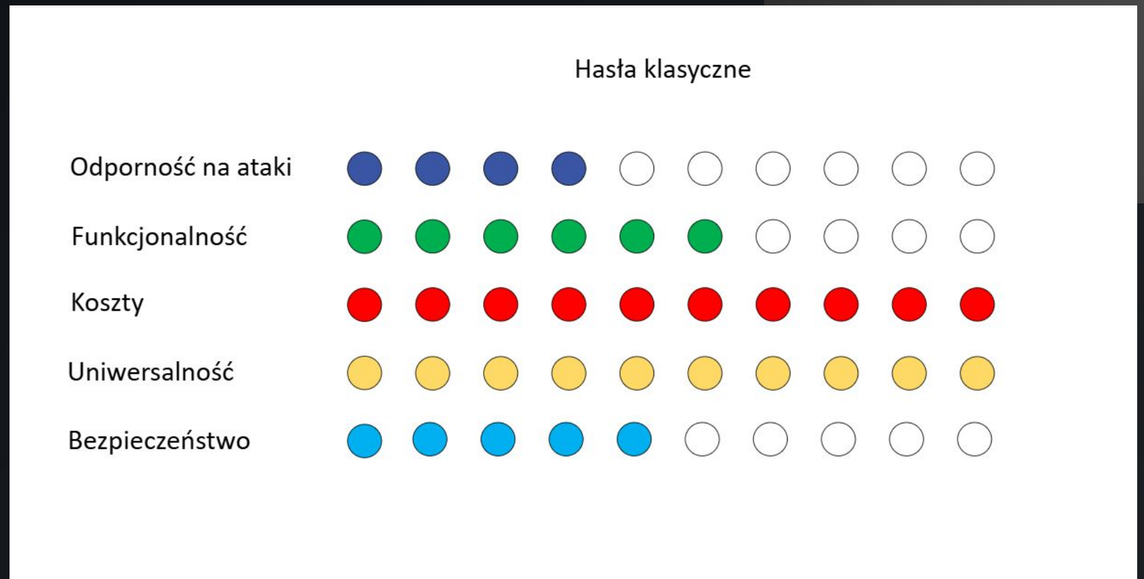


Oceny wszystkich mechanizmów

Hasła Klasyczne

Hasła klasyczne to proste i tanie rozwiązanie, które sprawdza się w podstawowych zastosowaniach. Jednak ich ograniczona odporność na ataki i niższy poziom bezpieczeństwa mogą stanowić problem w bardziej wymagających środowiskach.

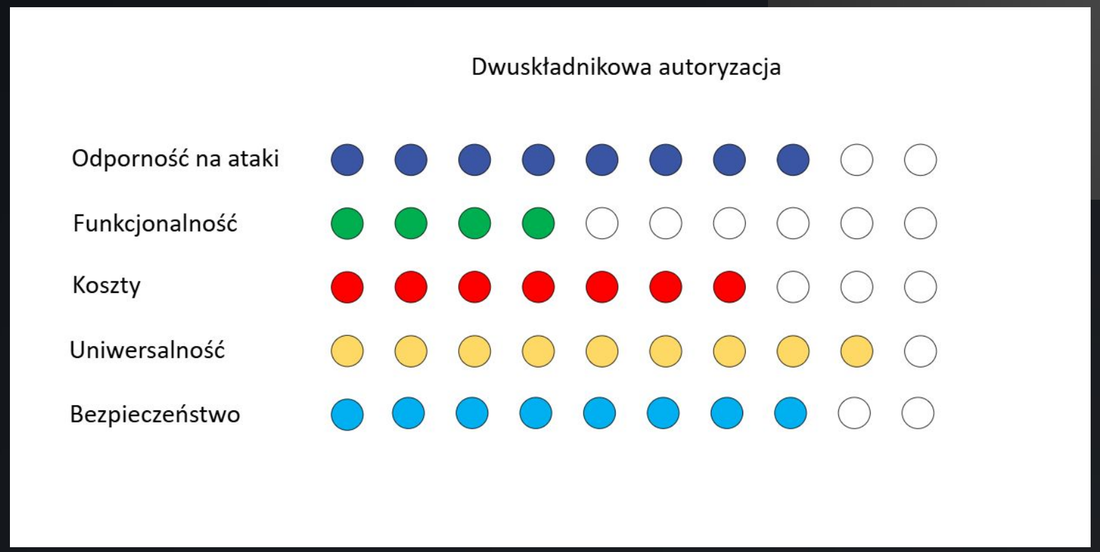




Oceny wszystkich mechanizmów

Dwuskładnikowa autoryzacja

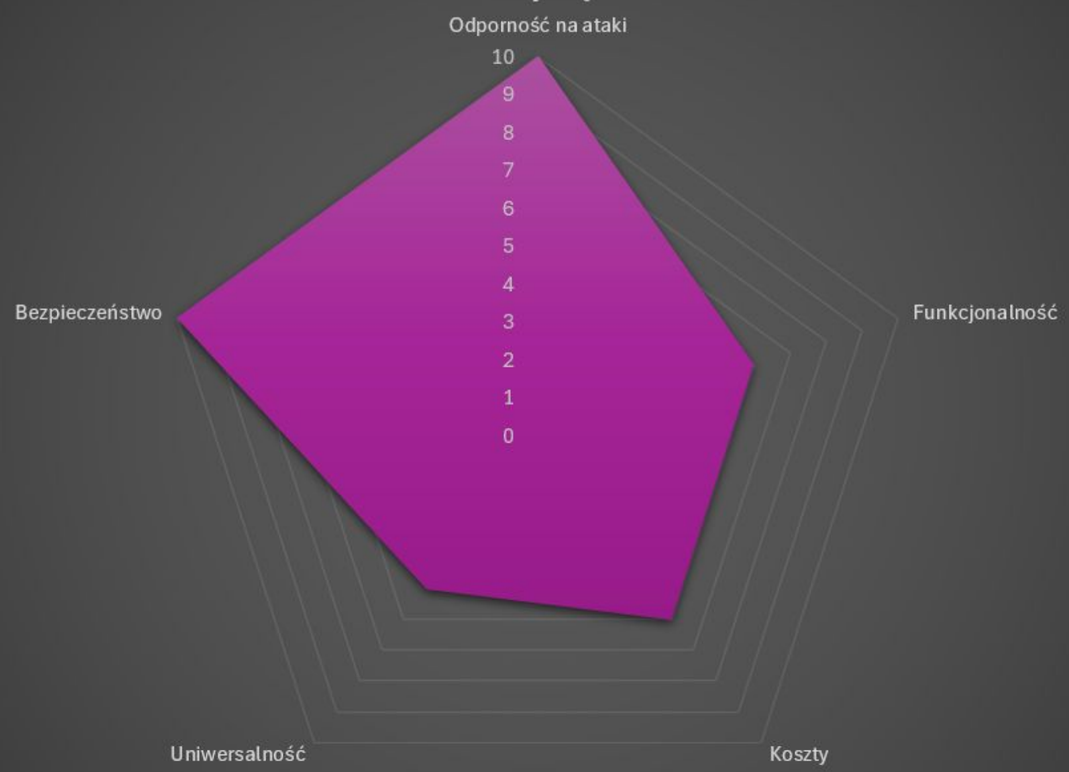
Dwuskładnikowa autoryzacja wyróżnia się wysokim poziomem bezpieczeństwa i odpornością na ataki dzięki dodatkowej warstwie ochrony. Jest uniwersalna w zastosowaniach, ale jej wdrożenie może wiązać się z wyższymi kosztami oraz pewnymi ograniczeniami funkcjonalnymi w zależności od integracji z istniejącymi systemami.



Oceny wszystkich mechanizmów

Klucze sprzętowe

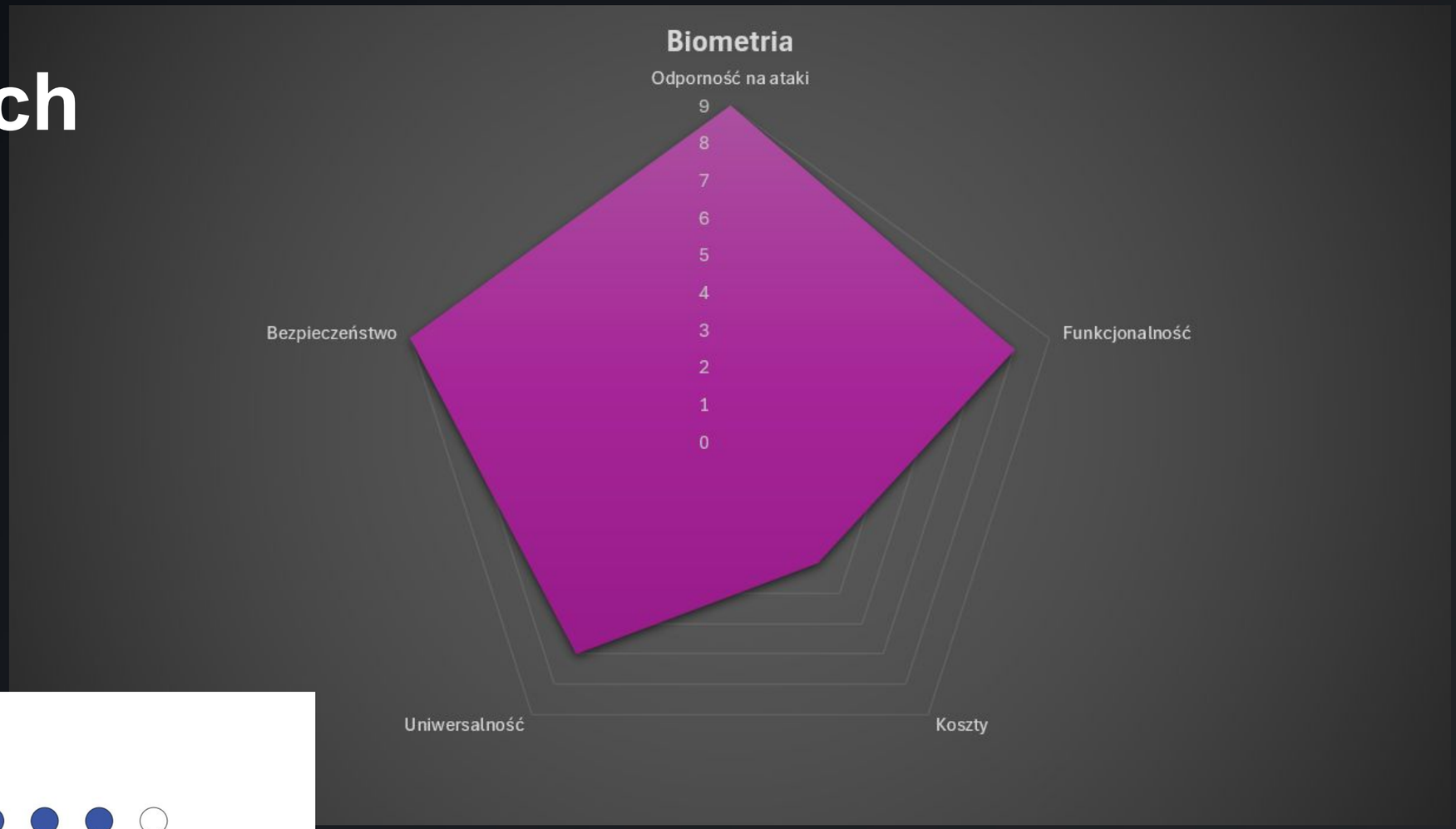
Klucze sprzętowe zapewniają wysoki poziom bezpieczeństwa i odporności na ataki. Są jednak drogie i mogą być mniej funkcjonalne w niektórych zastosowaniach, ograniczając swoją uniwersalność.

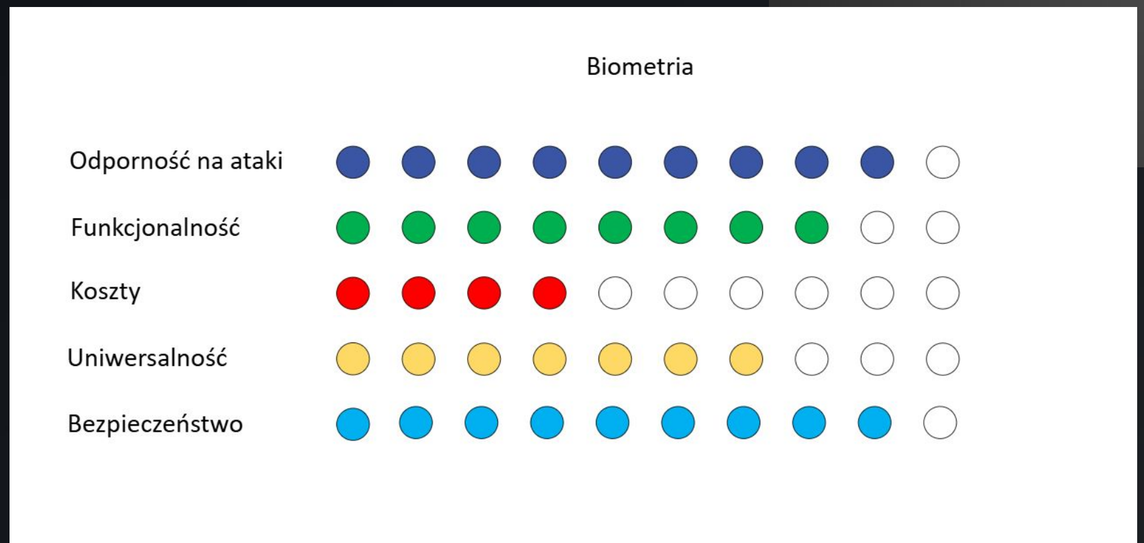


Oceny wszystkich mechanizmów

Biometria

Biometria jest rozwiązaniem dosyć odpornym na ataki, bezpiecznym oraz uniwersalnym. Przy wykorzystaniu zaawansowanych technik rozpoznawania może być jednak kosztowna.

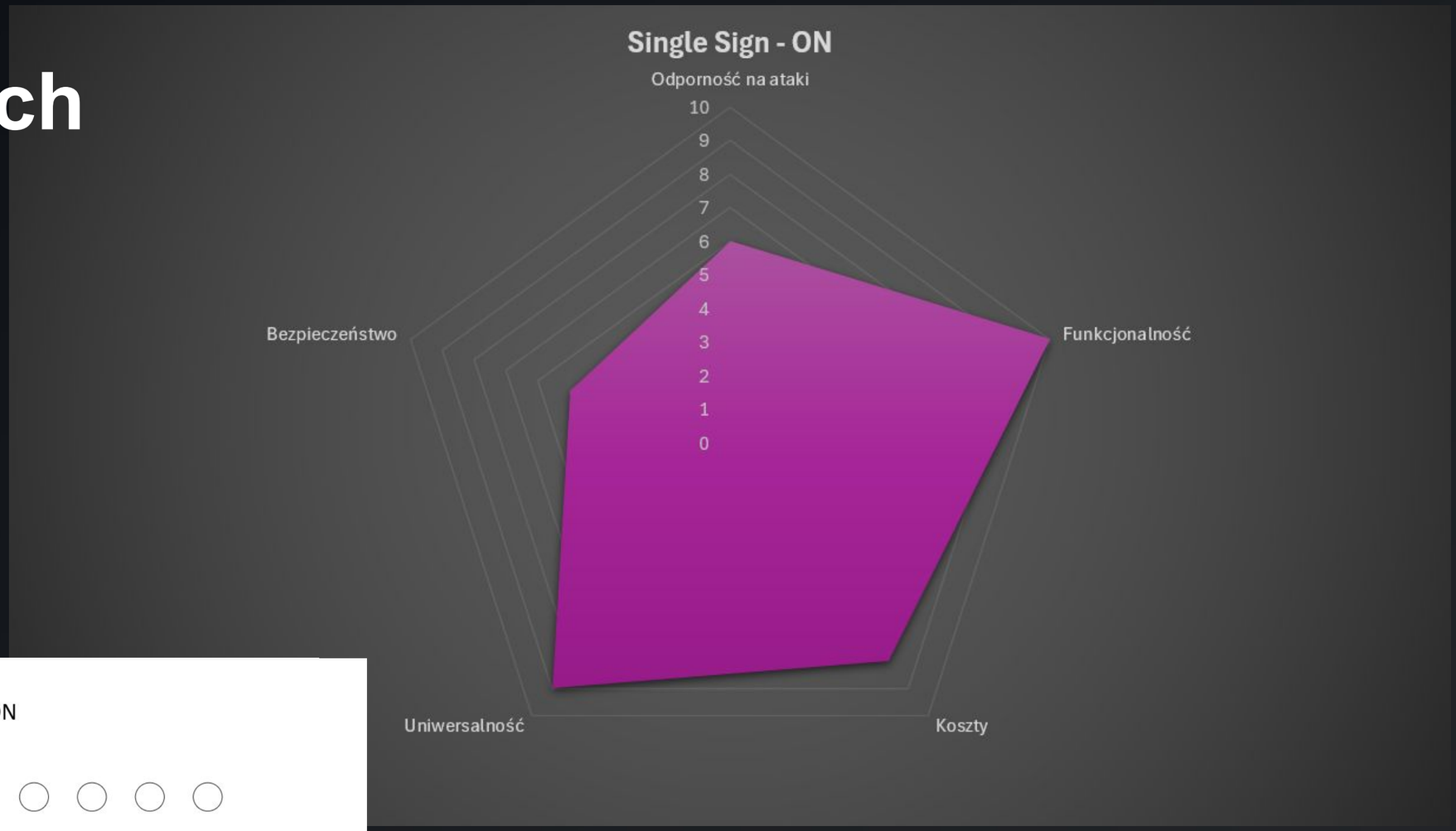


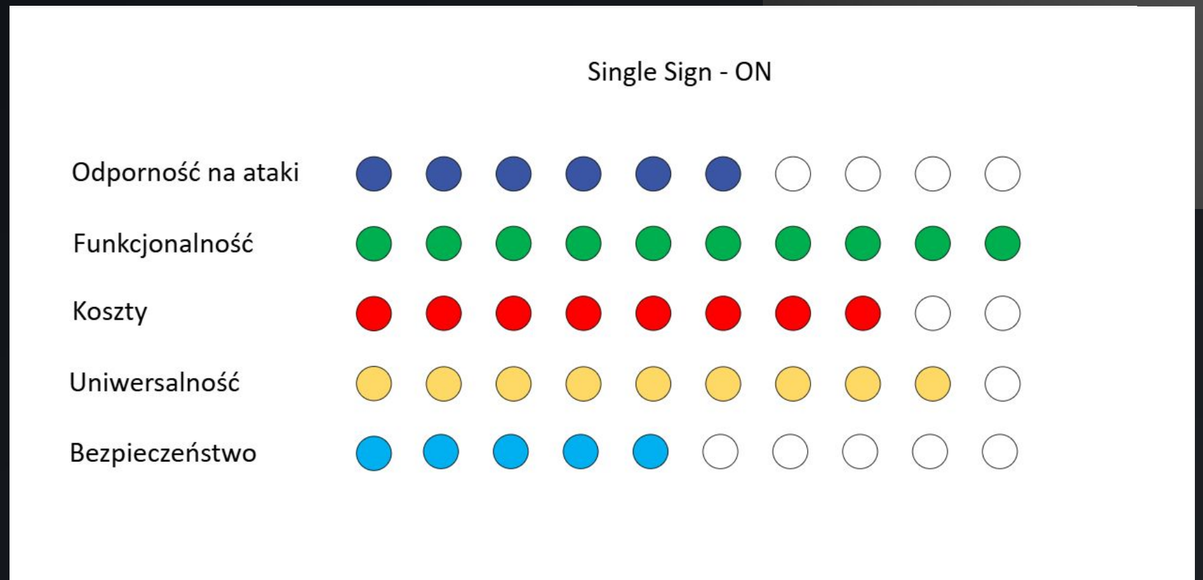


Oceny wszystkich mechanizmów

Single Sign-On

SSO jest bardzo funkcjonalne ze względu na łatwość użytkowania i swoją uniwersalność w integracji z innymi systemami, jednakże potrzebuje innych narzędzi, by zapewnić bezpieczeństwo

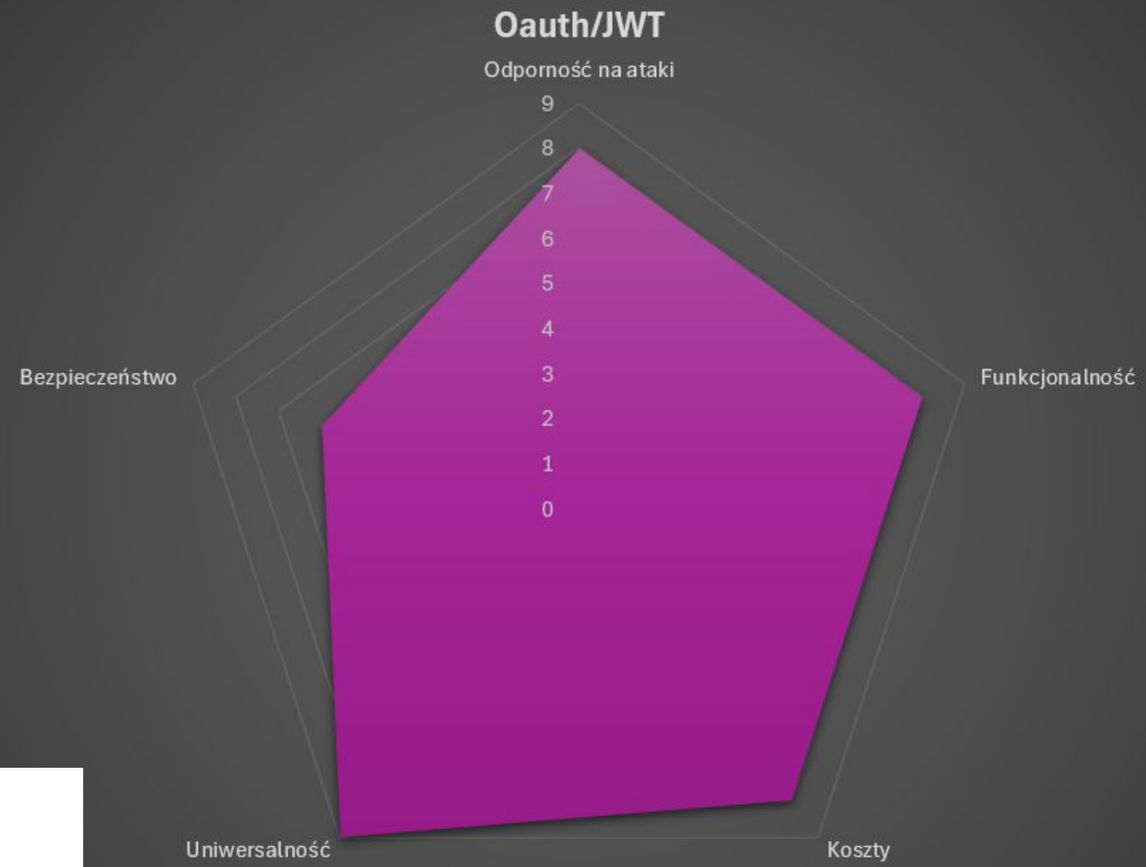


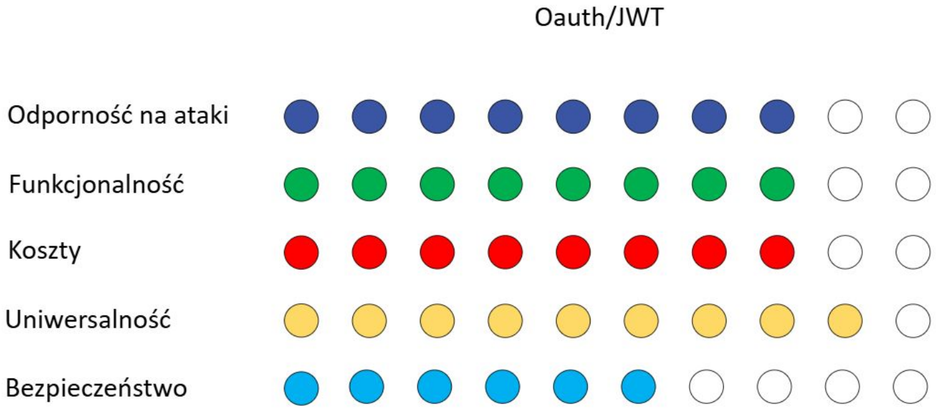


Oceny wszystkich mechanizmów

Oauth/JWT

Dzięki swojej elastyczności i funkcjonalności te mechanizmy cieszą się wysoką oceną. Bezpieczeństwo w tym przypadku zależy głównie od implementacji programistów.

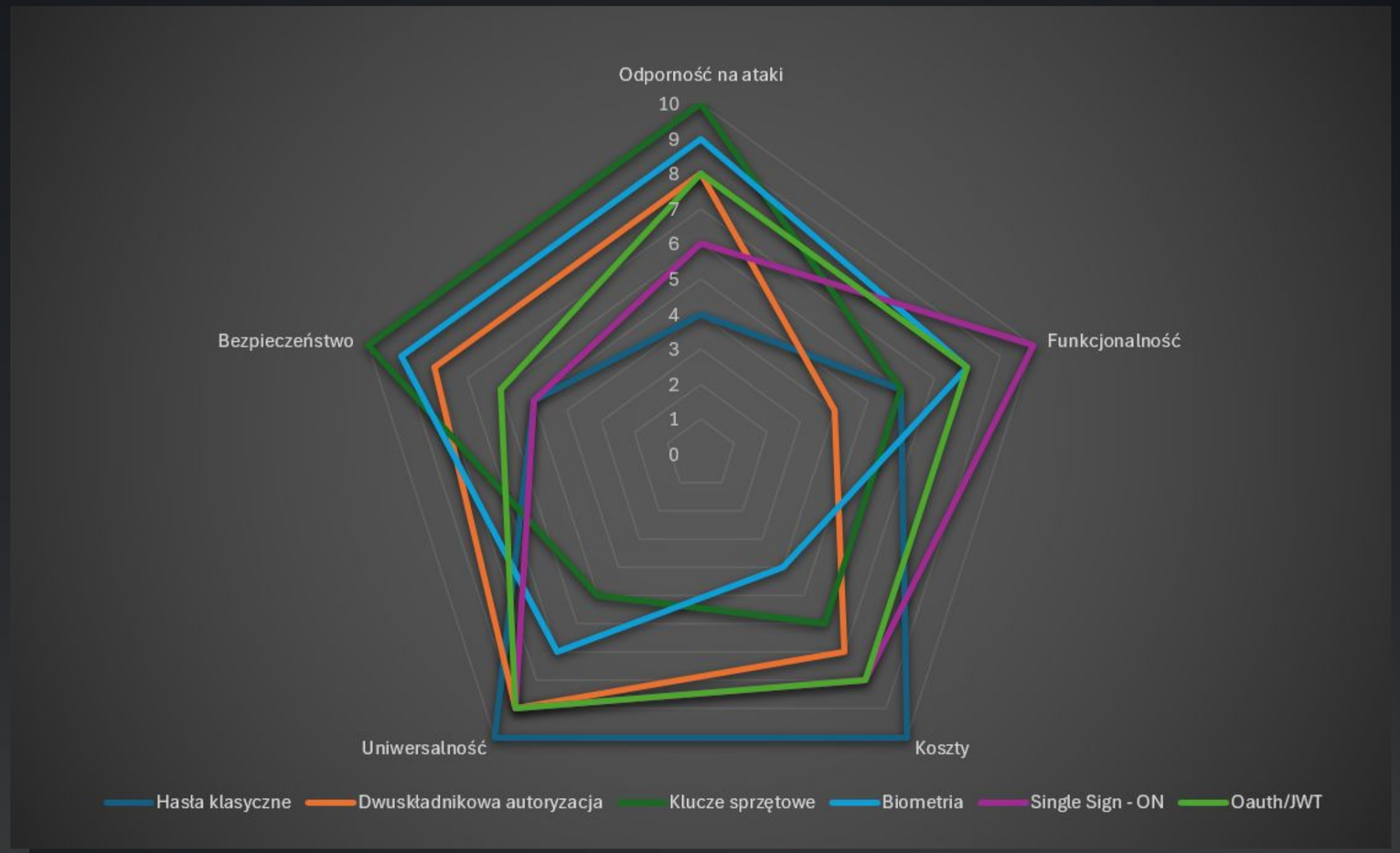




Podsumowanie

Porównanie przedstawionych form uwierzytelniania na jednym wykresie

Wszystkie formy uwierzytelniania mają swoje mocne i słabe strony, jedne są samowystarczające inne zaś wymagają implementacji dodatkowych rozwiązań w celu sensownego użytkowania



Dziękujemy

Analiza porównawcza mechanizmów uwierzytelniania

2024

MIKOŁAJ PACEK, BARTOSZ GRZYBOWSKI, DAWID RYBA, MATEUSZ WIRKIJOWSKI, MIESZKO MAKOWSKI, PATRYK MOTYLSKI

Bibliografia

https://www.x-kom.pl/g-4/c/3450-klucze-sprzetowe.html?page=2

https://store.google.com/us/product/titan_security_key?hl=en-US&pli=1

https://www.amazon.com/Kensington-K64708JP-VeriMark-Guard-Fingerprint/dp/B09DCYNZNC

https://crp.to/p/