Jak wybrać najlepszą metodę uwierzytelniania wieloskładnikowego (MFA)?

Weryfikacja tożsamości użytkowników i kontrola jego dostępu są kluczowe dla Zarządzania Tożsamością i Dostępem (IAM) w każdej organizacji. Uwierzytelnianie użytkowników wspiera funkcje IAM, takie jak audyt, analityka czy autoryzacja. Jest ważne dla specjalistów ds. IAM, bezpieczeństwa i zarządzania ryzykiem. Chociaż samo uwierzytelnianie nie stanowi wystarczającego zabezpieczenia, jest niezbędne do zapewnienia kontroli sieci, bezpieczeństwa aplikacji i danych oraz ograniczenia oszustw i nadużyć.

W procesie uwierzytelniania najistotniejsze są użyteczność i bezpieczeństwo. Cechy te muszą być zrównoważone, aby zapewnić wymagany poziom bezpieczeństwa w sposób, który nie wpływa negatywnie na komfort użytkowania.

Obecnie najczęściej używane metody uwierzytelniania to:

- Token sprzętowy OTP (One Time Password)
- Token softwarowy OTP - aplikacje uwierzytelniające
- OTP przez SMS
- Weryfikacja biometryczna
- Powiadomienie push

Poniżej przedstawiamy popularne metody uwierzytelniania skupiając się na dwóch najistotniejszych elementach: poziomie bezpieczeństwa i doświadczeniu użytkownika (user experience).

Token sprzętowy OTP

W tej metodzie uwierzytelniania użytkownik oprócz znajomości nazwy użytkownika i hasła do swojego konta, posiada token sprzętowy.

To urządzenie elektroniczne tworzy ograniczone w czasie lub oparte na zdarzeniu jednorazowe hasło (OTP). Podczas uwierzytelniania użytkownik po podaniu nazwy użytkownika i hasła wprowadza do portalu uwierzytelniania kod wygenerowany przez token lub aplikację.

Zarówno serwer, jak i token mają to samo ziarno tzw. seed. W oparciu o nie za każdym razem generują ten sam kod. Wykorzystanie tokenów sprzętowych polega na potwierdzeniu posiadania przez użytkownika drugiego czynnika - czyli czegoś, co fizycznie posiada (token). Nie jest to wygodne rozwiązanie dla samego użytkownika, który musi nosić ze sobą taki token.

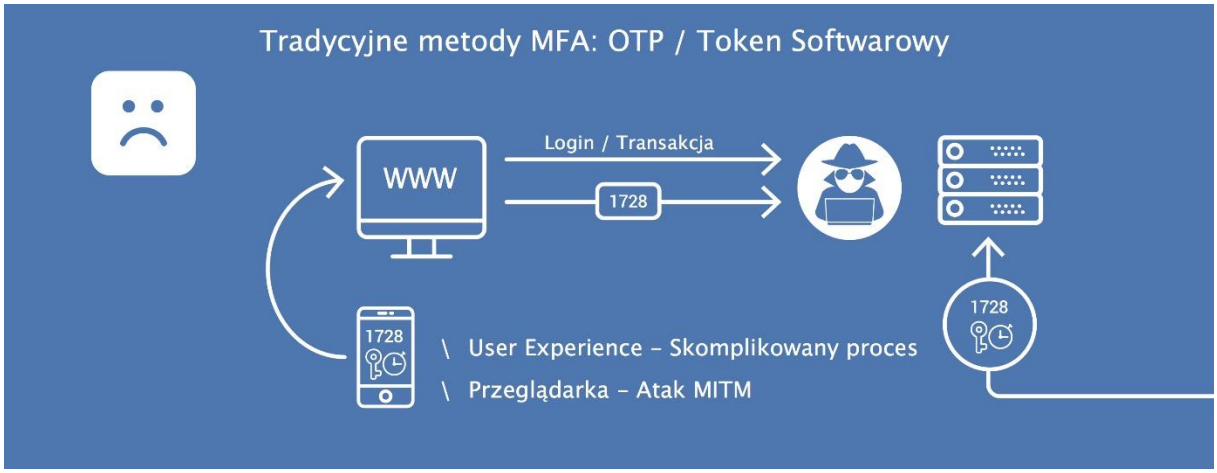
Dane wejściowe tokenów sprzętowych są jawne, jedyną wartością tajną jest seed. Jeżeli dane te nie są odpowiednio chronione, mogą zostać skradzione z serwera lub od dostawcy tokena sprzętowego. W 2011 r. w wyniku cyberataku na serwery producenta tokenów, firmy RSA, wykradziono miliony numerów seryjnych tokenów[1], narażając klientów na ataki hakerskie.

[1] Security Firm Offers to Replace Tokens After Attack, The New York Times, June 6, 2011

Token softwarowy OTP - aplikacje uwierzytelniające

Dzięki tej metodzie użytkownik otrzymuje OTP (jednorazowe hasło) z preinstalowanej aplikacji, które następnie wprowadza do formularza uwierzytelniania.

Aplikacje tokenów softwarowych są wygodniejsze w użyciu niż tokeny sprzętowe, ponieważ nie wymagają od użytkowników noszenia dodatkowego sprzętu. Oferują podobną funkcjonalność do tokenów sprzętowych, mają też podobne wady i zalety. W przypadku tokenów softwarowych dodatkowym zagrożeniem jest możliwość kradzieży wartości seed przy użyciu złośliwego oprogramowania (malware) i replikowanie tego samego tokena na innym telefonie.



OTP przez SMS

Tradycyjną i prawdopodobnie najpopularniejszą metodą uwierzytelniania wieloskładnikowego jest Out of Band (OOB) za pośrednictwem SMS-a wysyłanego na urządzenie mobilne[2]. Metoda ta jest jednak najbardziej podatna na zagrożenia bezpieczeństwa i wpływa negatywnie na doświadczenie użytkownika (User Experience).

W przyszłości wykorzystanie SMS jako metody uwierzytelniania może nie być zgodne ze standardami bezpieczeństwa teleinformatycznego rekomendowanymi przez NIST (National Institute of Standards and Technology)

Za pomocą OTP przez SMS użytkownik otrzymuje wiadomość tekstową SMS z losowym kodem (OTP o ograniczonym czasie). Użytkownik musi następnie wprowadzić kod do portalu uwierzytelniania lub aplikacji, w której podał nazwę użytkownika i hasło.

Gartner przewiduje, że w 2019 r. przedsiębiorstwa korzystające z tradycyjnych systemów uwierzytelniania OOB za pomocą SMS-ów odnotują ponad dwukrotnie większą liczbę naruszeń bezpieczeństwa związanych z uwierzytelnianiem niż te, które korzystają z powiadomień typu mobile push.[3]

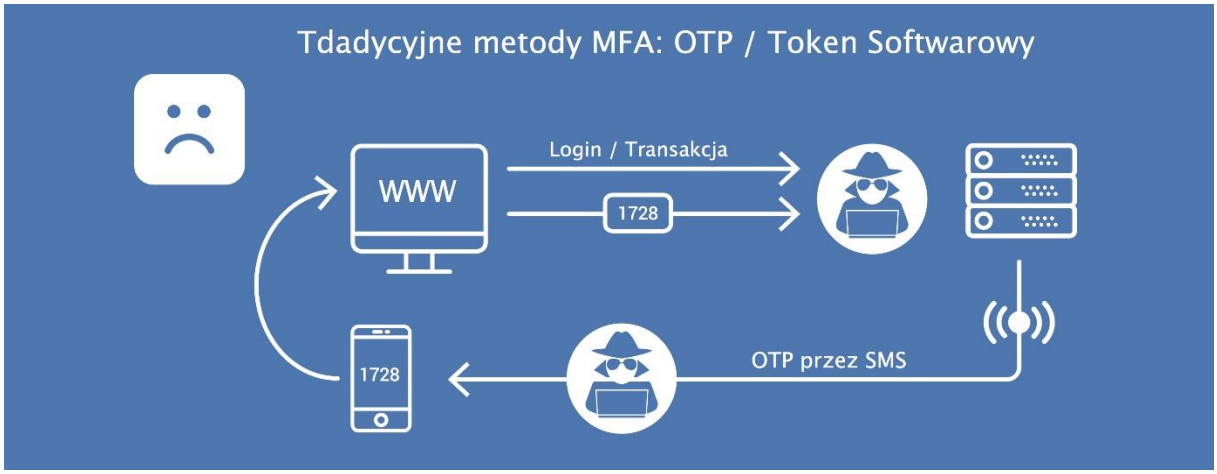
[2] Technology Insight for Phone-as-a-Token Authentication, Gartner, p.11, March 10, 2017, ID: G00319826
[3] Technology Insight for Phone-as-a-Token Authentication, Gartner, p.3, March 10, 2017, ID: G00319826

Wiadomości SMS są najsłabszym ogniwem bezpieczeństwa w uwierzytelnianiu MFA. Ataki na działaczy politycznych w Iranie, Rosji i USA wykazały, że hakerzy mogą "w locie" przechwytywać wiadomości SMS[4] [5]. Innym słabym elementem tej metody jest nieostrożny użytkownik, który oczekuje otrzymania SMS-a z kodem od jakiegokolwiek nadawcy - to właśnie fałszywe wiadomości uwierzytelniające są popularną taktyką stosowaną w atakach phishingowych.

Operatorzy sieci komórkowych nie gwarantują bezpieczeństwa swoich sieci, a roaming dodatkowo zmniejsza szanse na zapewnienie silnego poziomu bezpieczeństwa. Ponadto ogólnie wiadomo, że szyfrowanie stosowane w sieciach komórkowych jest słabe[6].

Niedawno NIST *(National Institute of Standards and Technology)* opublikował przewodnik[7], w którym odradza się wykorzystywania SMS-ów do uwierzytelniania.

Uwierzytelnianie za pomocą SMS-ów jest też niewygodne - co potwierdzają sami użytkownicy. Podczas korzystania z OTP przez SMS muszą oni skopiować informacje OTP z urządzenia odbierającego do formularza logowania. W związku z tym musi to być krótki „ciąg znaków", co wpływa na zmniejszenie bezpieczeństwa.



Weryfikacja biometryczna

Kolejną opcją jest uwierzytelnianie biometryczne. Mogą to być statyczne metody, takie jak odcisk palca lub dynamiczne, jak behawioralne czynniki biometryczne. Statyczna biometria jest uważana za stosunkowo niedokładną.

Zdaniem NIST "biometryczne współczynniki fałszywego dopasowania i fałszywego niedopasowania nie dają pewności w uwierzytelnianiu subskrybenta."[8] Na przykład w 2014 r. hakerzy twierdzili, że "sklonowali" odcisk palca niemieckiej minister obrony na podstawie zdjęcia jej ręki zrobionego na konferencji prasowej.[9]

Ponieważ po logowaniu nie ma danych do analizy, biometria behawioralna jest mniej przydatna do uwierzytelniania.

[4] So Hey You Should Stop Using Texts for Two-Factor Authentication, WEIRD magazine, Jun 26, 2016
[5] More than 86% of the world's iPhones can still be hacked with just a text, Business Insider, Aug. 29, 2016
[6] More than 86% of the world's iPhones can still be hacked with just a text, Business Insider, Aug. 29, 2016
[7] DRAFT Special Publication 800-63B, Digital Identity Guidelines, NIST, Apr 30 2017
[8] DRAFT Special Publication 800-63B, Digital Identity Guidelines, NIST, Apr 30 2017
[9] Politician's ngerprint 'cloned from photos' by hacker, BBC News, Dec 29, 2014

Indywidualne behawioralne czynniki biometryczne są trudniejsze do skopiowania. Rozwiązania wykorzystujące biometrię behawioralną mogą stworzyć dokładniejszy obraz użytkownika badając zakres wzorców behawioralnych, które są stale aktualizowane i ulepszane. Ponieważ już po zalogowaniu użytkownika aplikacja nie ma danych behawioralnych do analizy, biometria behawioralna stała się mniej przydatna do uwierzytelniania, znajdując zamiast tego zastosowanie w innych obszarach np. w wykrywaniu oszustw.

Innym problemem związanym z czynnikami biometrycznymi jest przechowywanie informacji. Zwykle proces uwierzytelniania odbywa się lokalnie (np. za pomocą odcisku palca na urządzeniu użytkownika). Powodem dla którego dane biometryczne nie są przechowywane na serwerze jest problem wynikający z zapewnienia bezpiecznego scentralizowania poufnych i wrażliwych danych.

Powiadomienia push

Główną zaletą powiadomień push jest to, że tylko właściciel aplikacji może wysłać powiadomienie, co uniemożliwia przeprowadzenie ataku phishingowego przez stronę trzecią.

Metoda ta zapewnia równowagę między zapewnieniem bezpieczeństwa a wygodnym użytkowaniem. W przeciwieństwie do wiadomości SMS i biometrii, eksperci NIST uważają uwierzytelnianie za pomocą powiadomień push jako odpowiedni system uwierzytelniania.[10]

Do końca 2019 r. 50% przedsiębiorstw stosujących obecnie uwierzytelnianie za pomocą telefonu przejdzie na uwierzytelnianie za pomocą powiadomień push.

Według Gartnera do końca 2019 r. 50% wszystkich przedsiębiorstw korzystających obecnie z uwierzytelniania telefonicznego (takich jak hasło jednorazowe i SMS) przejdzie na uwierzytelnianie za pomocą powiadomień push. Ten trend wzrostowy jest widoczny już od 2017 r.

Problem z powiadomieniem push polega na tym, że szyfrowanie odbywa się w dwóch etapach: dostawca usług do serwera push (np. Apple lub Google) i serwer push na urządzenie mobilne. W procesie tym dane są ujawniane na serwerze push, co oznacza, że poufne informacje, w tym OTP, nie mogą być przesyłane przez powiadomienia push. Powiadomienie push powinno być używane jedynie do wybudzenia aplikacji, aby ta mogła wysłać żądanie do serwera. W takim przypadku uwierzytelnianie będzie korzystało z systemu PKI (Public Key Infrastructure), co z kolei wiąże się z zagrożeniami i słabymi punktami SSL.
Wszystkie te problemy bezpieczeństwa, słabe punkty i luki w uwierzytelnianiu MFA rozwiązuje Octopus Authenticator.

Octopus Authenticator

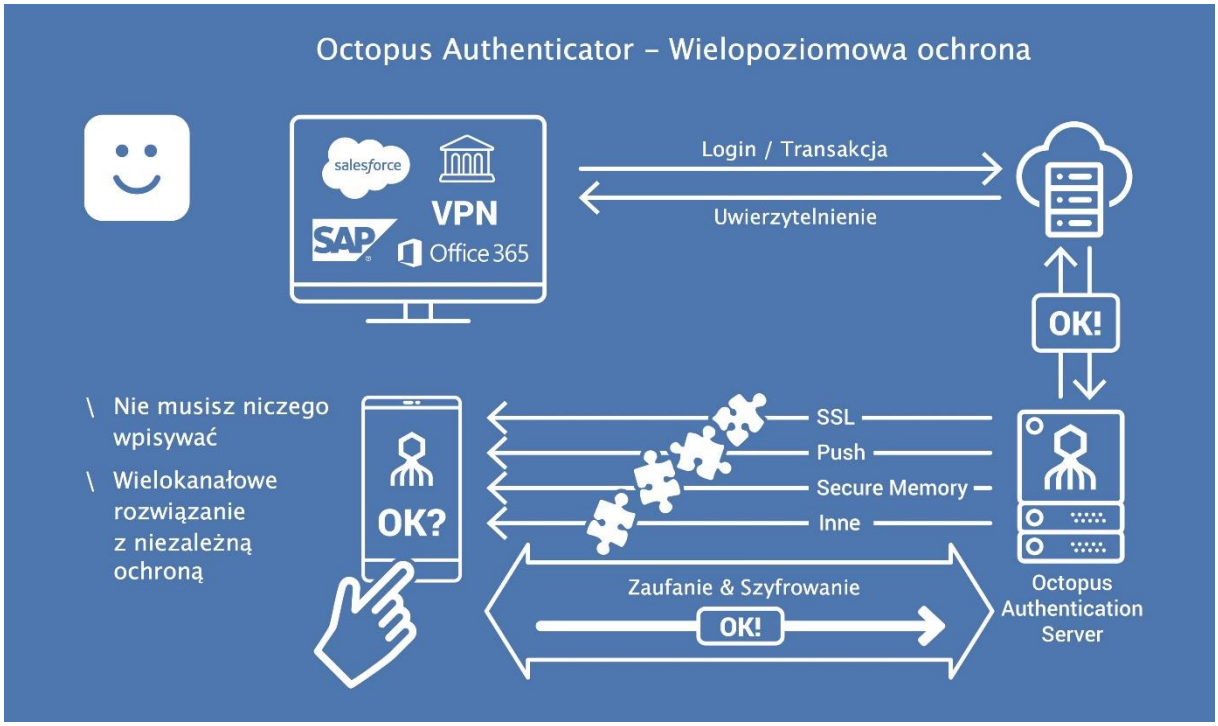
Octopus Authenticator firmy Secret Double Octopus jest obecnie najnowocześniejszą metodą uwierzytelniania w trybie push. To jedyne dostępne rozwiązanie, które wykorzystuje technologię poufnego udostępniania (Secret Sharing) w celu wyeliminowania wszystkich słabych punktów bezpieczeństwa uwierzytelniania. Zastosowanie Octopus Authenticator uniemożliwia cyberprzestępcom przeprowadzenie ataku nawet w przypadku kradzieży klucza, podsłuchu czy innych ataków MITM. Ponadto wprowadzenie znacznie zwiększonego poziomu bezpieczeństwa nie wpływa na komfort użytkowania - "złożoność" rozwiązania jest całkowicie ukryta przed użytkownikiem, a zatwierdzenie odbywa się jedynie za pomocą jednego dotknięcia w odpowiedzi na jasne i zrozumiałe powiadomienie push.

Jako eksperci w dziedzinie uwierzytelniania możemy pomóc firmom zapewnić bezpieczeństwo ich systemów dzięki zastosowaniu najbardziej zaawansowanej metody uwierzytelniania jaka jest obecnie dostępna.

[10] DRAFT Special Publication 800-63B, Digital Identity Guidelines, NIST, Apr 30 2017

SECRET DOUBLE OCTOPUS

QDP
Efektywność i bezpieczeństwo IT



Firma **Secret Double Octopus** opracowała jedyną na świecie technologię bezkluczowego uwierzytelniania wielowarstwowego, zapewniającą ochronę tożsamości i danych w środowiskach chmurowych, mobilnych i IoT. W oparciu o algorytmy Secret Sharing, pierwotnie opracowane w celu ochrony kodów startowych broni jądrowej, technologia Secret Double Octopus chroni dostęp do krytycznych informacji przed atakami cyberprzestępców, eliminując tym samym zagrożenia takie, jak ataki brute force, Man-In-The-Middle, manipulacje PKI, kradzież klucza czy luki bezpieczeństwa urzędów certyfikacji.

Przedstawicielem firmy Secret Double Octopus w Polsce jest QDP Sp. z o.o.

QDP Sp. z o.o.
ul. Ślężna 104, 53-111 Wrocław
tel. 71 356 49 40

Centrum Kompetencyjne
ul. Nabielaka 6, 00-743 Warszawa
tel. 22 160 51 77

Info@qdp.com.pl
www.qdp.com.pl