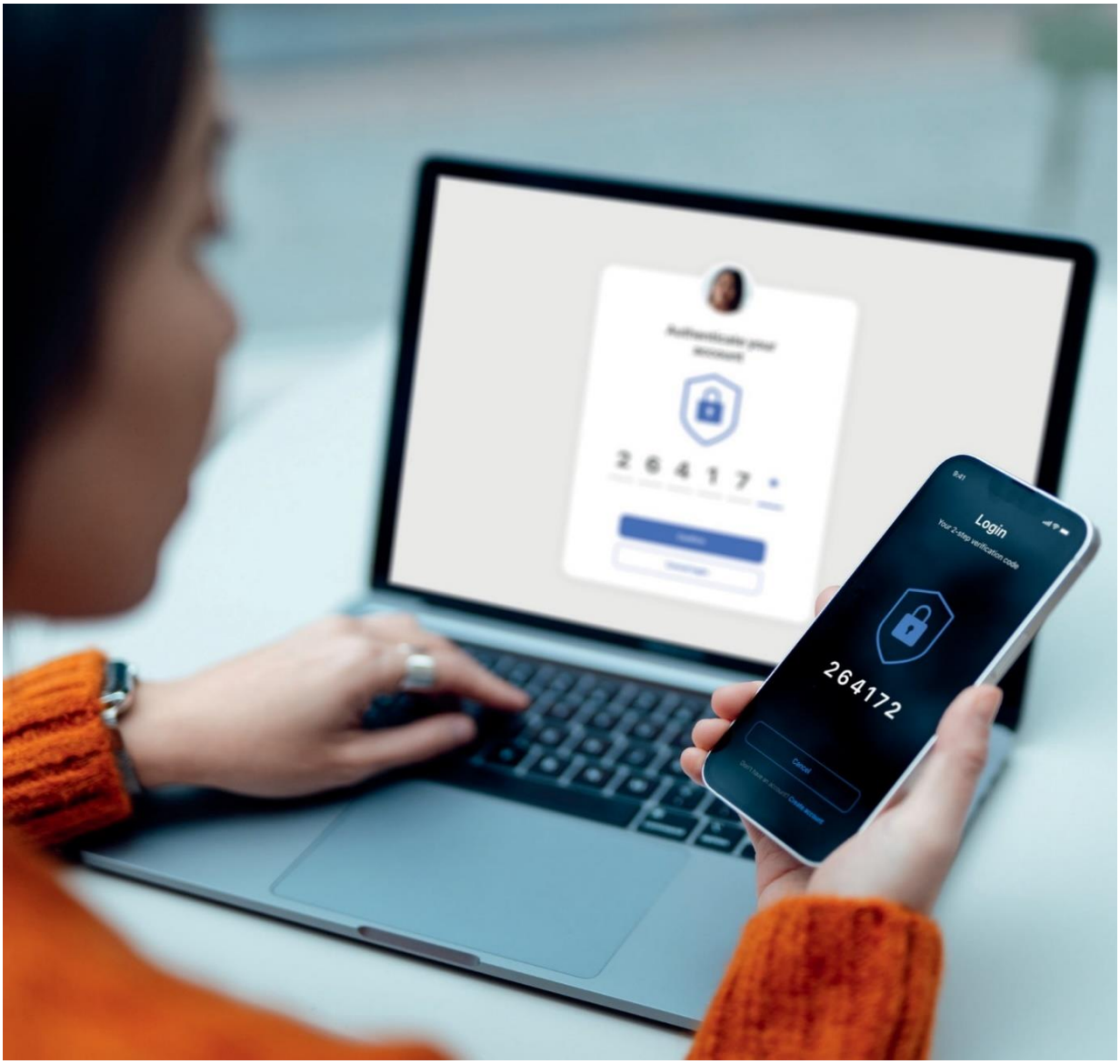

Uwierzytelnianie wieloskładnikowe MFA – wielopoziomowy system ochrony

„Firma Orange Polska S.A z siedzibą w Warszawie, Al. Jerozolimskie 160, 02-326 Warszawa, NIP: 5260250995 / KRS 0000010681 (dalej partner PWCyber), udziela Ministerstwu Cyfryzacji zgody na wykorzystanie i publikację materiałów przekazanych w ramach Programu PWCyber (zwanych dalej „Materiałami"), w szczególności: tekstów, grafik, diagramów, infografik, prezentacji oraz innych treści edukacyjnych. Partner oświadcza, że materiały nie naruszają praw osób trzecich".

Spis treści

ORANGE 1
Uwierzytelnianie wieloskładnikowe MFA – wielopoziomowy system ochrony 1
Spis treści 2
Co to jest MFA 3
3+1 – czyli wybierz odpowiednią kombinację składników 3
Przykładowe metody MFA 4

Czasy, kiedy do bezpiecznego korzystania z internetu wystarczał login i hasło bezpowrotnie minęły. Dziś login i hasło to za mało, a jeśli chcesz zapewnić odpowiedni poziom bezpieczeństwa – szczególnie danych wrażliwych, krytycznych systemów informatycznych, niezbędne jest używanie dodatkowego uwierzytelniania na wielu poziomach. Uwierzytelnianie wieloskładnikowe znacząco ograniczy ryzyka, związane z potencjalnym przejęciem Twojego konta, a nawet Twojej cyfrowej tożsamości.

Co to jest MFA

MFA (Multi-Factor Authentication) to metoda uwierzytelniania, która wymaga od ciebie podania co najmniej dwóch niezależnych czynników w celu potwierdzenia tożsamości. Składają się na nią trzy główne elementy: coś, co użytkownik zna np. hasło, coś, co ma np. laptop, telefon, a także coś, co jest twoją unikalną cechą fizyczną np. biometria. Warto wspomnieć także o czwartej możliwości jaką jest uwierzytelnienie za pomocą danych lokalizacyjnych. Dzięki MFA masz dodatkowe warstwy ochrony, co znacząco utrudnia nieautoryzowany dostęp do wrażliwych danych. Przy rosnącej liczbie i złożoności cyberataków, metoda ta jest istotną częścią indywidualnego i firmowego cyberbezpieczeństwa. To obecnie „must have” w walce z coraz bardziej wyrafinowanymi cyberzagrożeniami jak m.in. wszechobecny phishing, wycieki, socjotechnika, kradzież tożsamości etc.

3+1 – czyli wybierz odpowiednią kombinację składników

Na początku artykułu wspomniałem o głównych elementach składających się na uwierzytelniania MFA. Skuteczne wdrożenie MFA to odpowiedni dobór i kombinacja tych elementów, dostosowanych do specyfiki danej firmy. Najlepiej wykorzystaj co najmniej dwa składniki, aby zmaksymalizować ochronę przed różnorodnymi cyberzagrożeniami.

Każdy ze składników jest niezależny od pozostałych. Oznacza to, że przejęcie przez atakującego jednego z nich np. urządzenia nie pozwala przestępcy na uzyskanie pełnego dostępu do systemu.

1. Podstawowy składnik odnosi się do informacji, które musisz zapamiętać i podać podczas uwierzytelniania. To zwykle hasło lub kod PIN. Jest on łatwy do wprowadzenia, ale także najbardziej podatny na socjotechnikę.
2. Drugi składnik wymaga od ciebie posiadania przedmiotu – telefonu, laptopa, tokena, karty inteligentnej, który służy do potwierdzenia tożsamości. Jego zaletą jest to, że atakujący musiałby fizycznie zdobyć Twój przedmiot, co jest znacznie trudniejsze niż odgadnięcie lub wykradzenie hasła. Ryzyko stanowi zgubienie lub kradzież urządzenia.

3. Trzeci składnik opiera się na twoich unikalnych cechach fizycznych lub behawioralnych - danych biometrycznych, jak odcisk palca, skan twarzy, rozpoznawanie głosu czy skan siatkówki oka. Zazwyczaj biometria jest dodatkowym składnikiem również przy korzystaniu z aplikacji uwierzytelniających na telefonie – np. Microsoft Authenticator. Metoda ta wymaga szczególnej ostrożności w zakresie przetwarzania danych.
4. Ciekawym uzupełnieniem MFA może być czwarta kategoria, która uwzględnia twoją lokalizację, zwykle określaną na podstawie adresu IP lub danych GPS. Może to być szczególnie przydatne, gdy chcesz ograniczyć dostęp do wrażliwych danych tylko z określonych lokalizacji, czy zastosować tzw. „geofencing" np. dla powierzchni firmowej.

Przykładowe metody MFA

Uwierzytelnianie wieloskładnikowe (MFA) wykorzystuje różne metody do weryfikacji tożsamości użytkowników. Każda z nich ma swoje zalety i potencjalne ograniczenia.

Kod SMS: przede wszystkim jest to sposób łatwy do uruchomienia i dostępny nawet na feature-phonach. Plusem jest na pewno uzyskanie wiedzy o ataku na nasze konto w momencie otrzymania SMS-a. Minusy – możliwość przejęcia treści SMS-a przy użyciu socjotechniki lub zastosowania innych technik ataku oraz fakt, że serwisy powoli odchodzą od SMS-ów.

Wiadomość push: ponownie jak przy SMS-ie w momencie otrzymania pusha wiemy, że ktoś usiłuje zalogować się na nasze konto. Metoda używana jest przez największe serwisy (Google, Meta, Microsoft). Potencjalnie podatna na socjotechnikę, ale wystarczy po prostu wyrobić w sobie nawyk szczegółowego czytania każdego komunikatu push w momencie jego otrzymania.

Tokeny sprzętowe:

Urządzenia, które generują jednorazowe kody lub służą jako klucze dostępu. Tokeny sprzętowe oferują wysoki poziom bezpieczeństwa, ponieważ są bardzo trudne do skopiowania i przejęcia przez cyberprzestępcę. Ich główną wadą jest konieczność ich zakupu (zazwyczaj min. dwóch by mieć zapasowy na wypadek zgubienia – oznacza to również konfigurację obydwu w każdym systemie) i posiadania zawsze przy sobie.

Biometria:

Do weryfikacji tożsamości wykorzystują unikalne cechy fizyczne lub behawioralne użytkownika. Są one coraz powszechniej stosowane ze względu na wygodę użytkowania i wysoki poziom bezpieczeństwa. Najpopularniejsze metody biometryczne to:

- Odciski palców: Stosowane w smartfonach i laptopach.
- Rozpoznawanie twarzy: Popularne w nowszych urządzeniach mobilnych i systemach dostępu.
- Skanowanie siatkówki lub tęczówki oka: wysoki poziom bezpieczeństwa, ale wymaga specjalistycznego sprzętu.
- Rozpoznawanie głosu: Przydatne szczególnie w systemach telefonicznych.

Niezaprzeczalną wadą biometrii jest brak możliwości jej zmiany, co niestety może rodzić trudności, jeśli doszłoby do uszkodzenia lub utraty nośnika danych biometrycznych na naszym ciele, czy np. „ataku" przez skierowanie zablokowanego urządzenia w naszą twarz i skorzystanie z jej rozpoznawania.

Karty inteligentne:

Zawierają mikroprocesor, który przechowuje dane uwierzytelniające. Karty te są często używane w środowiskach korporacyjnych i rządowych, gdzie wymagany jest wysoki poziom bezpieczeństwa. Użytkownik musi mieć kartę i znać PIN, aby uzyskać dostęp.

Lokalizacja geograficzna:

Może obejmować weryfikację adresu IP lub danych GPS z urządzenia mobilnego. Ta metoda jest szczególnie przydatna w organizacjach, które chcą ograniczyć dostęp do określonych lokalizacji geograficznych czy ułatwić korzystanie z systemów np. w swoich placówkach.