Firma Integrity Partners Sp. z o.o. z siedzibą w Warszawie (00-867), ul. Chłodna 51; NIP 5272620067/KRS 0000347184 (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

MFA – czym jest i jak chroni organizację przed cyberatakami?

Statystyki są bezlitosne. Analiza firmy Check Point z 2025 roku to sygnał alarmowy dla każdej organizacji. Wzrost liczby ujawnionych danych uwierzytelniających o 160% i 14 000 przypadków ujawnienia danych pracowników w ciągu jednego miesiąca pokazują, że cyberzagrożenia dla firm rosną w niezwykłym tempie.

Atakujący nie celują już tylko w systemy, lecz w najsłabsze ogniwo – człowieka. Utrata kontroli nad dostępem do konta e-mail czy sieci firmowej przez pracownika może otworzyć cyberprzestępcom drzwi do całej infrastruktury. Dane klientów, informacje finansowe, własność intelektualna czy strategiczne plany – to wszystko staje się potencjalnym celem ataków.

Czy można w prostu sposób podnieść bezpieczeństwo firmy w sieci? Tak. Rozwiązaniem jest wdrożenie wieloskładnikowego uwierzytelniania. MFA, z angielskiego multifactor authentication, to technologia kluczowa dla ochrony firmowych i prywatnych danych. Czym jest i jak działa? Wyjaśniamy.

Po co przestępcy dane uwierzytelniające?

Przejęte dane uwierzytelniające pracowników to są bardzo cenne dla cyberprzestępców. Nie służą wyłącznie do przejęcia jednego konta, ale stają się punktem wejścia do całej sieci firmowej. Dzięki nim można:

1. Przeprowadzić atak na firmową infrastrukturę

Zdobycie dostępu do konta e-mail pracownika pozwala przestępcom na przeprowadzenie ataków spear-phishingowych. Polegają one na wysyłaniu spersonalizowanych i wyglądających na autentyczne wiadomości do innych pracowników lub klientów. Co więcej, dzięki loginom i hasłom przestępcy mogą również uzyskać dostęp do sieci korporacyjnej, systemów finansowych, baz danych klientów lub poufnych dokumentów. Jest to często pierwszy krok do przeprowadzenia ataku typu ransomware, który szyfruje wszystkie dane firmowe i żąda okupu za ich odblokowanie.

2. Wykraść dane i własność intelektualną

Przez przejęcie konta pracownika, szczególnie z wyższego szczebla, cyberprzestępcy mogą uzyskać dostęp do wrażliwych informacji: danych finansowych, przełomowych projektów, badań i rozwoju, a nawet danych osobowych klientów. Sprzedaż tych informacji na czarnym rynku lub ich publiczne ujawnienie może prowadzić do

ogromnych strat finansowych, utraty zaufania klientów i poważnych konsekwencji prawnych, w tym kar za naruszenie RODO.

3. Wyłudzić pieniądze

Przestępcy często używają przejętych kont do wyłudzania pieniędzy. Mogą podszyć się choćby pod prezesa firmy i wysłać do dyrektora finansowego polecenie wykonania pilnego przelewu do rzekomego dostawcy. Tego typu oszustwa, znane jako Business Email Compromise (BEC), kosztują firmy miliardy dolarów rocznie.

Konsekwencje przejęcia danych uwierzytelniających pracowników są niezwykle poważne. Właśnie dlatego uwierzytelnianie wieloskładnikowe (MFA) nie jest już opcją, a koniecznością dla każdej firmy, która chce podnieść swoje bezpieczeństwo.

---Ważne---

Z badań Microsoft wynika, że ponad 99,9 % skompromitowanych kont nie było zabezpieczonych mechanizmami MFA.

Dlaczego same hasła to za mało?

Hasła uznawane są dziś za niewystarczające zabezpieczenie. Przede wszystkim dlatego że są podatne na liczne ataki i zbyt łatwe do złamania oraz przejęcia. Jak można stracić swoje hasło?

1. Łamanie haseł

Większość ludzi używa prostych, łatwych do zapamiętania haseł, takich jak data urodzenia, imiona bliskich lub sekwencje typu „123456”. Cyberprzestępcy korzystają z automatycznych programów do łamania haseł, które w ciągu kilku sekund mogą przetestować miliony kombinacji. Nawet bardziej złożone hasła mogą zostać złamane przez ataki słownikowe lub siłowe (brute-force).

2. Ataki phishingowe

Coraz bardziej wyrafinowane ataki phishingowe są projektowane tak, aby oszukać odbiorcę i skłonić do dobrowolnego podania hasła. Fałszywe e-maile, które wyglądają jak oficjalne wiadomości od banku, serwisu społecznościowego czy pracodawcy, prowadzą do fałszywych stron logowania. Ofiara wprowadza swoje dane, a cyberprzestępca natychmiast je przechwytuje.

3. Wycieki danych

Nawet jeśli użytkownik stosuje silne hasło, może ono zostać skradzione z serwisu, z którego korzysta. Wycieki ogromnych ilości danych z popularnych platform

internetowych zdarzają się regularnie. W ich wyniku miliony haseł, często w niezaszyfrowanej formie, trafiają na czarny rynek. To jest szczególnie problematyczne, gdy pracownik używa tego samego hasła w wielu serwisach. Cyberprzestępcy wykorzystują to w tzw. atakach typu credential stuffing, w których listy haseł skradzionych z jednego serwisu testują na innych platformach (bankowość internetowa, poczta e-mail czy serwisy biznesowe). Jedno skompromitowane hasło może dać im dostęp do wielu różnych miejsc.

Czym jest MFA i jak działa?

Uwierzytelnianie wieloskładnikowe (MFA) to metoda weryfikacji tożsamości użytkownika, która wymaga podania dwóch lub więcej niezależnych od siebie składników uwierzytelniających. Innymi słowy, żeby zalogować się do konta, nie wystarczy już tylko hasło – trzeba dać dodatkowy „dowód" swojej tożsamości. Tym dowodem może być:

1. Coś, co użytkownik wie (Knowledge Factor): To informacje znane z założenia tylko logującemu się do serwisu. Najczęstszym przykładem jest hasło lub kod PIN.
2. Coś, co użytkownik ma (Possession Factor): To fizyczny przedmiot lub urządzenie, które posiada logujący się. Przykłady to smartfon (na który dostaje kod SMS lub push) czy klucz bezpieczeństwa USB (np. YubiKey).
3. Coś, czym użytkownik jest (Inherence Factor): To unikalne cechy biometryczne, które są nierozerwalnie związane z osobą logującą się. Zaliczamy do nich odcisk palca, skan twarzy (np. Face ID), skan tęczówki, a nawet głos.

W przypadku używania MFA system wymaga podania co najmniej dwóch czynników z różnych kategorii. Na przykład:

- hasło i kod z aplikacji w telefonie,
- hasło i skan odcisku palca.

Dzięki temu, nawet jeśli cyberprzestępca zdobędzie czyjeś hasło (np. w wyniku wycieku danych), nie będzie mógł uzyskać dostępu do konta, ponieważ będzie mu brakować drugiego, niezależnego czynnika uwierzytelnienia.

Dlaczego MFA jest niezbędne? Korzyści z zastosowania uwierzytelniania wieloskładnikowego

Wdrożenie MFA to dziś już nie opcja, a konieczność. MFA znacząco zwiększa bezpieczeństwo. Dodatkowa warstwa ochrony sprawia, że szanse na nieautoryzowany dostęp do konta wyraźnie maleją. MFA chroni użytkowników przed różnego rodzaju zagrożeniami, w tym phishingiem i spear phishingiem, atakami brute force i credential stuffing, przed skutkami wycieku danych oraz przed złośliwym oprogramowaniem i keyloggerami, które rejestrują naciśnięcia klawiszy, co pozwala im wykradać hasła. MFA dodaje ochronę, której takie programy nie są w stanie obejść.

Wdrożenie MFA to także dodatkowe korzyści dla firm:

- **Zgodność z regulacjami i normami**

Wiele współczesnych przepisów i standardów bezpieczeństwa, takich jak RODO (GDPR), DORA, dyrektywa NIS2 czy normy ISO 27001, rekomenduje lub wręcz wymaga stosowania MFA w celu ochrony danych i systemów. Wdrożenie MFA pomaga spełnić te wymogi i uniknąć potencjalnych kar.

- **Zaufanie klientów i partnerów biznesowych**

Firma, która poważnie traktuje bezpieczeństwo swoich danych i danych klientów, budzi większe zaufanie. Stosowanie MFA jest sygnałem dla rynku, że organizacja odpowiedzialnie podchodzi do swoich partnerów biznesowych.

Przegląd składników uwierzytelniania

MFA opiera się na kombinacji co najmniej dwóch różnych typów faktorów. Przyjrzyjmy się im bliżej.

Składniki oparte na wiedzy

- Hasła i kody PIN. Podstawowy i wciąż najpopularniejszy składnik.
- Pytania bezpieczeństwa, np. "Nazwisko panieńskie matki?". Coraz rzadziej stosowane jako główny składnik MFA.

Składniki oparte na posiadaniu

- Tokeny sprzętowe, w tym klucze USB (np. YubiKey, Google Titan Security Key), inteligentne karty (Smart Cards) oraz tokeny z wyświetlaczem (generatory OTP).
- Tokeny programowe (aplikacje uwierzytelniające), w tym aplikacje generujące OTP (Time-based One-Time Password – TOTP), np. Google Authenticator, Microsoft Authenticator, Authy, powiadomienia push oraz dynamicznie generowane kody QR.
- SMS OTP (One-Time Password) (jednorazowy kod wysyłany na zarejestrowany numer telefonu).
- E-mail OTP (kod wysyłany na zarejestrowany adres e-mail).

Składniki biometryczne

- Fizyczna biometria, czyli odcisk palca, skan twarzy (Face ID), skan tęczówki/siatkówki oka, weryfikacja głosu.
- Biometria behawioralna, która analizuje unikalny sposób interakcji użytkownika z urządzeniem (np. rytm pisania na klawiaturze, sposób poruszania myszką, sposób trzymania telefonu). Działa w tle, bez świadomej interakcji użytkownika.

Wybór odpowiednich składników zależy od poziomu wymaganego bezpieczeństwa, wygody użytkownika i specyfiki systemu.

Wdrożenie uwierzytelniania wieloskładnikowego (MFA) w organizacji

Proces ten wymaga planowania, wyboru odpowiednich technologii i komunikacji z pracownikami. Powinien być poprzedzony analizą systemów i oceną ryzyka. Ważny jest także wybór metod MFA. Czy to będzie aplikacja mobilna, tokeny sprzętowe czy może hasła jednorazowe? Dobrze jest oferować pracownikom kilka opcji do wyboru.

W zależności od wielkości organizacji i jej infrastruktury można wybrać różne rozwiązania. Eksperci Integrity Partners rekomendują:

1. Aplikacje uwierzytelniające (np. Microsoft Authenticator, Google Authenticator)

Jest to najpopularniejsze i najprostsze w implementacji rozwiązanie. Aplikacja mobilna generuje kod jednorazowy (TOTP – Time-based One-Time Password), który zmienia się co kilkadziesiąt sekund. Pracownik musi go wprowadzić po podaniu hasła. Aplikacje takie jak Microsoft Authenticator oferują również opcję powiadomień „push" – w takim przypadku użytkownik zatwierdza logowanie jednym kliknięciem.

Warto pamiętać, że w ramach ekosystemu Microsoft 365 włączenie MFA jest intuicyjne i można je wdrożyć w sposób masowy dla całej firmy, korzystając z zasad dostępu warunkowego (Conditional Access).

2. Tokeny sprzętowe (np. YubiKey)

To rozwiązanie przeznaczone przede wszystkim dla pracowników, którzy mają dostęp do najbardziej wrażliwych danych. YubiKey to mały klucz USB, który uwierzytelnia użytkownika po podłączeniu do komputera lub po użyciu NFC. Może działać w oparciu o protokoły takie jak FIDO2, które są odporne na ataki phishingowe, ponieważ klucz weryfikuje adres strony, na którą użytkownik próbuje się zalogować.

Wdrożenie wymaga zakupu urządzeń i konfiguracji ich w systemach firmowych. Jest to idealne rozwiązanie dla administratorów, pracowników IT i zarządu, którzy mają dostęp do kluczowych systemów.

3. Systemy do zarządzania tożsamością i dostępem (IdM/IAM), np. SailPoint

W przypadku dużych, złożonych organizacji, same tokeny czy aplikacje to za mało. W takim przypadku warto rozważyć wdrożenie kompleksowej platformy do zarządzania tożsamościami, np. SailPoint. Pozwala ona na centralne zarządzanie dostępem, automatyzację procesów, np. dodawanie nowych pracowników, zmienianie uprawnień oraz audyt dostępu. MFA staje się w tym przypadku jednym z elementów szerszej strategii bezpieczeństwa, który w przypadku wykrycia zdarzenia charakterystycznego dla kradzieży danych uwierzytelniających może wysłać sygnał do platformy IDM/IAM, aby podjąć działania minimalizujące skuteczność potencjalnego ataku (np. czasowe wyłączenie konta użytkownika w krytycznych systemach).

Świadomość na pierwszym miejscu

Choć MFA może skutecznie zapobiegać różnego rodzaju atakom, samo też nie jest wolne od podatności. Cyberprzestępcy próbują różnych metod, by obejść to zabezpieczenie. Jedną z nich jest MFA fatigue, zwane również jako MFA bombing. Na czym polega? Atakujący:

1. Zna już login i hasło ofiary (np. z wycieku lub phishingu).
2. Próbuje się logować wielokrotnie, wywołując lawinę powiadomień push w aplikacji uwierzytelniającej (np. Microsoft Authenticator).
3. Użytkownik zaczyna dostawać dziesiątki powiadomień typu: „Czy chcesz zatwierdzić logowanie?”.
4. Zmęczony, zirytowany lub rozproszony użytkownik w końcu przypadkowo akceptuje jedno z żądań – i w ten sposób przestępca uzyskuje dostęp.

----**WAŻNE**----

Niebezpieczne SMS-y

Eksperci Integrity Partners przestrzegają także przed używanie SMS-ów jako jednego ze składników uwierzytelniania. Dziś wiemy już, że nie stanowią bezpiecznego rozwiązania. Sam numer telefonu można stosunkowo łatwo przejąć – wystarczy atak typu SIM swapping, w którym przestępca przekonuje operatora do przeniesienia numeru na swoją kartę SIM i w efekcie przejmuje wszystkie przychodzące wiadomości. SMS-y nie są też szyfrowane w infrastrukturze telekomunikacyjnej i mogą zostać przechwycone, zarówno na poziomie sieci, jak i przez złośliwe oprogramowanie na telefonie. Dodatkowo, użytkownicy często padają ofiarą ataków phishingowych w czasie rzeczywistym, w których przepisują kody z SMS-ów do fałszywych formularzy, nieświadomie przekazując je atakującemu.

Jak się chronić przed MFA bombingiem?

1. Włącz uwierzytelnianie numeryczne

Wielu dostawców, w tym Microsoft, oferuje opcję uwierzytelniania numerycznego. Zamiast akceptować powiadomienie jednym kliknięciem, użytkownik musi wpisać na telefonie konkretny numer, który pojawił się na ekranie logowania. To zmusza do świadomej, celowej akcji i niemal całkowicie eliminuje ryzyko przypadkowego zatwierdzenia.

2. Używaj kluczy bezpieczeństwa (np. YubiKey)

Klucze sprzętowe takie jak YubiKey to najskuteczniejsza ochrona przed tego typu atakami. Działają one w oparciu o protokół FIDO2, który uwierzytelnia użytkownika bez konieczności interakcji z powiadomieniem. Taki system jest odporny na phishing i MFA Bombing.

3. Wdrażaj zasady dostępu warunkowego

Dla organizacji to jedno z najlepszych rozwiązań. Zasady dostępu warunkowego w usługach takich jak Microsoft Entra ID pozwalają na automatyczne blokowanie podejrzanych logowań. Mogą między innymi ograniczać logowanie z nieznanych lokalizacji geograficznych, blokować dostęp po wykryciu zbyt dużej liczby nieudanych prób logowania w krótkim czasie lub wymagać dodatkowej weryfikacji w przypadku logowania z nietypowego urządzenia.

4. Edukuj pracowników

Nawet najlepsze zabezpieczenia zawiodą, jeśli pracownicy nie będą świadomi zagrożenia. Istotna jest więc nieustanna edukacja pracowników w zakresie zasad bezpieczeństwa i metod, jakimi posługują się atakujący.

Uwierzytelnianie wieloskładnikowe istotny składnik bezpieczeństwa cyfrowego. Jest odpowiedzią na rosnącą liczbę cyberataków i konieczność odejścia od polegania wyłącznie na hasłach. Wdrożenie MFA w organizacji znacząco utrudnia przestępcom dostęp do poufnych danych. Połączone z edukacją i podnoszeniem świadomości pracowników może stać się kluczowym sposobem na walkę z zagrożeniami.