yubico

Wdrożenie uwierzytelniania wieloskładnikowego odpornego na phishing przy użyciu kluczy sprzętowych (YubiKey)

Spis treści

Nie każda metoda uwierzytelniania wieloskładnikowego jest sobie równa.

Chociaż uwierzytelnianie wieloskładnikowe (MFA) może stanowić skuteczną pierwszą linię obrony, nie wszystkie jego formy są sobie równe. Tradycyjne metody, takie jak nazwy użytkownika i hasła, można łatwo złamać, natomiast uwierzytelnianie mobilne (np. kody SMS, kody jednorazowe (OTP) czy powiadomienia push) są bardzo podatne na nowoczesne ataki phishingowe, złośliwe oprogramowanie, ataki typu SIM-swap oraz ataki man-in-the-middle (MiTM).

Co więcej, niemal zawsze zdarzają się pracownicy, którzy nie mogą, nie chcą lub nie używają uwierzytelniania mobilnego. Może to być spowodowane słabym zasięgiem w niektórych obszarach geograficznych, niechęcią do korzystania z prywatnych urządzeń w celach służbowych lub brakiem zgody na udzielenie dostępu administratora do swoich urządzeń. Dodatkowo mogą pojawić się ograniczenia wynikające z przepisów związkowych lub wymogów dotyczących zgodności, a niektórzy pracownicy mogą nawet nie posiadać smartfona. Jeśli opcją awaryjną jest powrót do nazw użytkownika i haseł, organizacja staje się jeszcze bardziej narażona na ataki phishingowe i przejęcia kont.

Co to jest MFA odporne na phishing?

Procesy uwierzytelniania wieloskładnikowego (MFA) odporne na phishing opierają się na weryfikacji kryptograficznej między urządzeniami lub między urządzeniem a domeną, co czyni je odpornymi na próby skompromitowania lub obejścia procesu uwierzytelniania. Zgodnie z publikacjami NIST Special Publication (SP) 800-63 i Draft 800-63-4, dwie formy uwierzytelniania spełniają obecnie kryteria MFA odpornego na phishing: **PIV/Smart Card** oraz nowoczesny standard uwierzytelniania **FIDO2/WebAuthn**

Klucz YubiKey zapewnia MFA odporne na phishing

Firma Yubico oferuje YubiKey – klucz U2F, który zapewnia nowoczesne, wieloskładnikowe i bezhasłowe uwierzytelnianie odporne na phishing. Klucze YubiKey obsługują wiele protokołów, w tym Smart Card i FIDO, dzięki czemu zapewniają prawdziwe, masowe uwierzytelnianie MFA odporne na phishing, pomagając organizacjom w przejściu z tradycyjnych na nowoczesne metody uwierzytelniania.

Klucze YubiKey są również proste we wdrożeniu i obsłudze — użytkownicy mogą uwierzytelniać się za pomocą jednego dotknięcia klucza. Ponadto klucze te nie wymagają baterii, nie mają kruchych ekranów, nie potrzebują połączenia z siecią komórkową i są odporne na wodę oraz zgniecenia. Dzięki YubiKey organizacje każdej wielkości mogą chronić pracowników przed współczesnymi cyberzagrożeniami,

jednocześnie zwiększając produktywność, zapewniając łatwość użytkowania i minimalizując koszty związane z resetowaniem haseł przez dział pomocy technicznej.

Sześć kluczowych praktyk, które przyspieszą wdrożenie YubiKey

1) Planowanie

Definiowanie scenariuszy użycia

Stopniowe podejście to najlepszy sposób na zapewnienie płynnego wdrożenia. W pierwszej kolejności skup się na użytkownikach i danych o największej wartości, a następnie rozszerzaj wdrożenie. Ustal priorytety dla przypadków użycia i grup użytkowników, biorąc pod uwagę takie czynniki jak ryzyko, lokalizacja pracowników, wpływ na działalność biznesową oraz łatwość integracji technicznej.

Najważniejsze scenariusze dla nowoczesnego uwierzytelniania odpornego na phishing:

A) Dostęp uprzywilejowany

Ochrona wrażliwych danych i pracowników mających podwyższony dostęp do systemów lub danych.

B) Środowiska bez telefonu

Zabezpieczenie wrażliwych środowisk, w których urządzenia mobilne są niedozwolone (np. centra telefoniczne, zakłady produkcyjne).

C) Stacje współdzielone

Ochrona użytkowników współdzielonych stacji roboczych/urządzeń przy jednoczesnym zachowaniu wygody użytkowania.

D) Bezpieczeństwo łańcucha dostaw

Dostęp i wymiana danych związane z oprogramowaniem i kodem stron trzecich.

E) Praca zdalna

Dodatkowa warstwa ochrony, zapewniająca bezpieczny dostęp do platform VPN, IAP, IAM i IdP.

Grupy użytkowników:

A) Pracownicy biurowi

Wyrafinowane ataki i eskalacje uprawnień sprawiają, że każdy użytkownik staje się użytkownikiem uprzywilejowanym. Zwiększ bezpieczeństwo i produktywność pracowników biurowych.

B) Dostęp stron trzecich

Ochrona dostępu stron trzecich do systemów i danych.

C) Ochrona klientów końcowych

Ochrona dostępu klientów do internetowych usług (w tym płatniczych); budowanie zaufania.

Zgromadzenie kluczowych interesariuszy

Chociaż ilość zasobów przeznaczonych na projekt może się różnić w zależności od skali i zakresu wdrożenia YubiKey, kluczowi interesariusze z zaangażowanych działów mogą mieć pozytywny wpływ na implementację MFA odpornego na phishing w całej organizacji. Ważne jest, aby uzyskać poparcie wszystkich zespołów (IT, Bezpieczeństwo, Finanse, Pomoc Techniczna, HR, OT), co zapewni płynne wdrożenie.

W razie potrzeby zaangażuj ekspertów Yubico.

Niezależnie od tego, na jakim etapie wdrażania MFA jesteś, będziemy Ci towarzyszyć, oferując najlepsze w swojej klasie wsparcie techniczne i operacyjne w zakresie implementacji i wdrożenia YubiKey.

2) Walidacja

Potwierdź proces z małą grupą użytkowników.

Sprawdź proces z małą grupą użytkowników, wybranych spośród priorytetowych przypadków użycia. Posłużą oni do potwierdzenia działania i przekazania informacji zwrotnej. Wykorzystaj przy tym materiały, filmy i spotkania oparte na najlepszych praktykach Yubico. Ćwicz, ucz się, a następnie przejdź do szerszego wdrożenia.

3) Integracja

Upewnij się, że Twoje środowisko jest gotowe na YubiKey

Klucze YubiKey współpracują z ponad 1000 aplikacji i usług, w tym z wiodącymi platformami do zarządzania tożsamością i dostępem (IAM), takimi jak Microsoft, Okta, Ping i Google, a także z aplikacjami VPN, np. Pulse Secure i Cisco AnyConnect. Aby zapewnić płynną integrację kluczy YubiKey w całym Twoim stosie technologicznym, warto odpowiedzieć na kilka kluczowych pytań. Dobrą praktyką jest, aby najpierw odpowiedzieć na te pytania w kontekście priorytetowych przypadków użycia, a następnie wrócić do nich przy każdym kolejnym, rozszerzonym wdrożeniu.

Przejrzyj katalog "Works with YubiKey".

Kto?

Kto potrzebuje dostępu? Pracownicy, kontrahenci, strony trzecie, łańcuch dostaw.

Co?

Jakie podejście do uwierzytelniania zastosujesz?

- **MFA** (hasło i silny drugi czynnik)
- **bezhasłowe** (passwordless)

Gdzie?

Gdzie w Twoim środowisku wymagane jest silne uwierzytelnianie?

- **Kluczowe elementy infrastruktury**, sieć, aplikacje, narzędzia dla programistów.

Jak zarządzasz dostępem?

- **IAM** (Zarządzanie Tożsamością i Dostępem), **IdP** (Dostawca Tożsamości), **PAM** (Zarządzanie Dostępem Uprzywilejowanym), **SSO** (Jednokrotne Logowanie), **VPN** (Wirtualna Sieć Prywatna), **ZTNA** (Dostęp do Sieci oparty na Zerowym Zaufaniu).

Jak?

Jak lokalizacja wpływa na wdrożenie?

- Zdalnie
- Hybrydowo
- W biurze (on-premise)
- W wielu biurach

Jakie typy urządzeń muszą być wspierane?

- Własne (firmowe)
- BYOD (Bring Your Own Device)
- Komputery stacjonarne
- Laptopy
- Smartfony
- Tablety

Przygotowanie do wdrożenia

Po upewnieniu się, że Twoje środowisko jest gotowe na YubiKey, nadszedł czas, aby stworzyć plan wdrożenia kluczy w całej organizacji.

Optymalizacja wdrożenia wymaga zarządzania zmianą w organizacji poprzez skuteczną komunikację, szkolenia i wsparcie. Integratorzy Yubico oferują szereg Usług Profesjonalnych, które pomogą w szybkim wdrożeniu.

4) Uruchomienie

Dostarcz klucze i zaplanuj uruchomienie.

Zależy nam, aby wdrożenie było jak najbardziej płynne dla wszystkich zespołów i użytkowników. Obejmuje to uproszczenie planów wdrożenia, pomoc w odpowiedzi na kluczowe pytania dotyczące dystrybucji kluczy użytkownikom oraz zarządzania cyklem życia YubiKey.

Rekomendacje dotyczące najlepszych praktyk wdrożenia YubiKey

- Zapewnij elastyczność i możliwość wyboru, ponieważ klucze YubiKey są dostępne w różnych rozmiarach i kształtach.
- Dwa klucze YubiKey na osobę, w celu posiadania zapasowego.
- Zabezpiecz się na przyszłość, posiadając dodatkowe klucze na wypadek rotacji pracowników, zgubienia lub kradzieży kluczy.
- Zachęcaj do dbałości o bezpieczeństwo poprzez politykę prywatnego użytku kluczy.
- Zaplanuj wydarzenie, które sprawi, że przyszłość bezpieczeństwa w Twojej organizacji będzie ekscytująca.

Uruchomienie

Wspomóż wdrożenie serią komunikatów startowych, które przedstawią użytkownikom YubiKey. Komunikuj się wcześnie i często. Idealne wiadomości na start wzbudzają entuzjazm użytkowników w związku z nowoczesnymi funkcjami klucza.

5) Adopcja

Wspieraj adopcję i zwiększaj zaangażowanie.

W Yubico wierzymy, że sukcesu nie należy mierzyć liczbą posiadanych kluczy YubiKey, lecz liczbą tych, które są faktycznie używane.

Podczas gdy komunikaty startowe uczą użytkowników, czym są YubiKey i dlaczego są ważne, zespoły wsparcia muszą być przygotowane, aby wyjaśnić, jak ich używać. W tym celu powinny posłużyć się sekcją FAQ, która pomoże odpowiedzieć na wszelkie pytania pojawiające się podczas wdrażania i rozwiązywania problemów (np. co zrobić w przypadku zgubienia klucza).

6) Mierzenie wyników

Raportowanie wpływu na bezpieczeństwo i biznes

Wiemy, że prawda leży w liczbach. Po weryfikacji pilotażu na podstawie poniższych wskaźników, rozszerz wdrożenie na kolejnych użytkowników, aby zwiększyć ogólny wpływ na biznes.

Wskaźniki wdrożenia:

- Liczba rozdanych kluczy
- Liczba aktywowanych użytkowników
- Liczba włączonych aplikacji

Wskaźniki wydajności:

- Skrócenie czasu wsparcia technicznego związanego z resetowaniem haseł
- Wzrost produktywności związany z czasem logowania

Wskaźniki bezpieczeństwa:

- Liczba wyeliminowanych zagrożeń bezpieczeństwa
- Uproszczenie raportowania zgodności i audytów

Wskaźniki dla użytkowników:

- Łatwość wdrożenia
- Łatwość użycia
- Poziom zadowolenia

Nie wiesz, od czego zacząć? Dobra wiadomość jest taka, że nie musisz od razu znać odpowiedzi na wszystkie pytania, np. ile kluczy kupić, jakiego rodzaju, jak zintegrować je ze swoim środowiskiem czy jak przekazać je użytkownikom końcowym. Nieważne, na jakim etapie wdrażania MFA jesteś, będziemy Ci towarzyszyć wraz z naszymi lokalnymi integratorami.