Wzmacnianie Bezpieczeństwa Tożsamości
Uwierzytelnianie Wieloskładnikowe
Przewodnik dla Kupujących

„Firma Cisco Systems Poland sp. z o. o., NIP 1181092318 / KRS: 0000019909 (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

Wyprzedzanie ewoluujących zagrożeń

W ostatnich latach wieloskładnikowe uwierzytelnianie (MFA) stało się niezbędną obroną w każdej strategii cyberbezpieczeństwa. Wymagając potwierdzenia wielu czynników przed zezwoleniem na dostęp, MFA chroni Twoje aplikacje i dane oraz pomaga zapewnić, że tylko autoryzowani użytkownicy mogą logować się do sieci firmowych.

Jednak wraz z pojawieniem się nowych typów zagrożeń, takich push-bombing[1], inżynieria społeczna i spear phishing[2], organizacje muszą zrobić więcej niż polegać wyłącznie na MFA. Choć MFA jest potężne i niezbędne, nie może być jedynym narzędziem w Twoim arsenale do identyfikowania, wykrywania i odpowiedniego reagowania na te nowe typy zagrożeń.

Więc czym są te nowe narzędzia i dlaczego są ważne?

- Logowanie bezhasłowe
- Uwierzytelnianie oparte na ryzyku
- Adaptacyjne zasady dostępu
- Narzędzia do widoczności tożsamości

Aby pozostać chronionymi, organizacje muszą zwiększyć skuteczność MFA za pomocą potężnych rozwiązań nowej generacji, takich jak logowanie bezhasłowe, uwierzytelnianie oparte na ryzyku (RBA), adaptacyjne zasady dostępu i narzędzia do widoczności tożsamości. Te nowe ulepszenia i dodatki do Twojego systemu zabezpieczeń służą temu samemu celowi: odpieraniu nawet najbardziej wyrafinowanych ataków.

Ale nie każde rozwiązanie jest takie samo. Niektóre rozwiązania zapewniają jedynie minimum potrzebne do spełnienia wymogów zgodności i często zawierają ukryte koszty związane z wdrożeniem, obsługą i utrzymaniem. Wiele tradycyjnych rozwiązań jest nieporęcznych, podatnych na błędy i wymaga obszernego szkolenia użytkowników oraz wsparcia — co kosztuje Twoich pracowników czas i produktywność. Narzędzia bezpieczeństwa mogą być kompromisem między skutecznością a wydajnością pracowników, a dobre doświadczenie użytkownika końcowego jest elementem koniecznym do rozważenia.

[1] Bombardowanie MFA - uporczywe nękanie użytkownika kolejnymi powiadomieniami *push* nakłaniającymi do akceptacji transakcji.
[2] Spear phishing to ukierunkowana forma phishingu, która ma na celu atakowanie konkretnych osób lub organizacji.

68% naruszeń bezpieczeństwa dotyczyło niezłośliwego czynnika ludzkiego, takiego jak osoba padająca ofiarą ataku inżynierii społecznej lub popełniająca błąd.

Verizon 2024 Raport z Badań Naruszeń Danych

W tym przewodniku znajdziesz:

- Dokładny wgląd na rozszerzenie Twojej ochrony bezpieczeństwa tożsamości poza minimalnym MFA
- Przegląd ukrytych kosztów rozwiązań bezpieczeństwa tożsamości i sposobu określenia zwrotu z inwestycji (ROI)
- Czego szukać, aby upewnić się, że Twoje rozwiązanie może chronić przed ryzykiem naruszenia danych
- Listę zasobów potrzebnych do wdrożenia, udostępniania i integracji Twojego rozwiązania
- Przegląd różnych strategicznych inicjatyw biznesowych i sposobu, w jaki Twoje rozwiązanie się w nie wpisuje

Idąc dalej niż MFA: Kryteria które należy rozważyć przy ocenie różnych rozwiązań

Wpływ na Bezpieczeństwo

Czy Twoje rozwiązanie może chronić przed nieautoryzowanym dostępem i zapewniać widoczność użytkowników i urządzeń w Twoim środowisku? Jak skutecznie rozwiązanie zmniejsza ryzyko naruszenia danych? Czy Twoje rozwiązanie może zapewnić kontrolę dostępu dla urządzeń zarządzanych i niezarządzanych? Czy Twoje rozwiązanie ostrzega o nietypowych lub podejrzanych aktywnościach logowania? Jak rozwiązanie będzie aktualizowane w przypadku nowych metod ataków?

Strategiczne Inicjatywy Biznesowe

Czy Twoje rozwiązanie jest kompatybilne z innymi inicjatywami biznesowymi, takimi jak zero trust, umożliwienie pracy zdalnej lub wdrażanie aplikacji chmurowych? Czy spełnia wymogi zgodności specyficzne dla branży?

Całkowity Koszt Posiadania

Czy Twoje rozwiązanie zapewnia wartość od razu, czy też wiąże się z ukrytymi kosztami dla Twojej organizacji? Czy może współpracować z nowoczesnymi i starszymi systemami? Czy rozwiązanie może pomóc skonsolidować wiele rozproszonych narzędzi? Jakie są przewidywane koszty pomocy technicznej lub potencjalne oszczędności wynikające z zgłoszeń związanych z hasłami?

Czas dostarczenia wartości

Jak szybko możesz uruchomić rozwiązanie w swoim środowisku? Jak łatwo możesz wdrożyć użytkowników końcowych? Ile planowania jest wymagane przed wdrożeniem?

Wymagane Zasoby

Jakie zasoby są wymagane do wdrożenia i udostępniania rozwiązania użytkownikom? Czy rozwiązanie jest zaprojektowane tak, aby zmniejszyć bieżące zadania administracyjne?

Sugerowane KPI dla MFA i Bezpieczeństwa Tożsamości

- % kont użytkowników skonfigurowanych do używania uwierzytelniania wieloskładnikowego
- % kont użytkowników używających silnych form MFA (FIDO2[3], bezhasłowe, klucze dostępu, dopasowywanie numerów)
- % kont gości z MFA
- % zgłoszeń do pomocy technicznej związanych z uwierzytelnianiem
- liczba ryzykownych zdarzeń uwierzytelniania rozwiązanych w danym okresie

Wpływ na Bezpieczeństwo

Najważniejsze aspekty bezpieczeństwa rozwiązania uwierzytelniającego to:

1. skuteczność w zwalczaniu zagrożeń związanych z kradzieżą danych uwierzytelniających lub przejęciem konta, oraz
2. podstawowe bezpieczeństwo i niezawodność

Głównym celem jest zmniejszenie ryzyka naruszenia dla Twojej organizacji. Jeśli rozwiązanie jest łatwo omijane lub nie zapewnia kompleksowej ochrony, która nadąża za nowymi danymi o zagrożeniach i reaguje na nie, nie warto go wdrażać.

Ochrona Wszystkich Aplikacji

Dla użytkowników końcowych, pojedyncze logowanie (SSO) zapewnia dostęp do wielu aplikacji za pomocą jednego loginu (używając jednej głównej kombinacji nazwy użytkownika i hasła) — i zmniejsza liczbę haseł, eliminując złe nawyki związane z hasłami, takie jak słabo skonstruowane hasła i ponowne użycie haseł. Dla administratorów, SSO służy jako ujednolicony punkt widoczności dla dzienników uwierzytelniania i dostępu, oraz skuteczny punkt egzekwowania zasad w celu stosowania polityk bezpieczeństwa dla każdej aplikacji w zależności od jej profilu ryzyka.

[3] Fast IDentity Online 2 to otwarty standard uwierzytelniania użytkowników, którego celem jest wzmocnienie sposobu, w jaki ludzie logują się do usług online, w celu zwiększenia ogólnego zaufania.

Zmniejszenie Zależności od Haseł

Hasła są dużym wyzwaniem dla zapewnienia bezpieczeństwa przedsiębiorstwa. Przeciętne przedsiębiorstwo używa dziś ponad 1000 aplikacji chmurowych. To zbyt wiele haseł, aby IT mogło nimi bezpiecznie zarządzać, a użytkownicy mogli je zapamiętać. Skutkuje to zmęczeniem hasłami, i nic dziwnego, że słabe i skradzione hasła są jednymi z głównych przyczyn naruszeń. Eliminacja haseł z uwierzytelniania brzmi bardzo atrakcyjnie; jednak, jak w przypadku każdej nowej technologii, rozsądnie jest przyjąć przemyślane podejście do wdrażania uwierzytelniania bezhasłowego.

Wdrożenie bezhasłowego uwierzytelniania to proces, który wymaga stopniowych zmian zarówno dla użytkowników, jak i środowisk IT. Zapytaj dostawców zabezpieczeń, jak ich produkty mogą pomóc Ci wdrożyć bezhasłowe środowisko bez tworzenia luk w zabezpieczeniach lub powodowania problemów dla IT.

Włączenie opcji pojedynczego logowania (SSO) wraz z MFA to świetny sposób na rozpoczęcie procesu wdrażania bezhasłowego środowiska bez kompromisów w kwestii bezpieczeństwa.

Jeśli możesz się do czegoś zalogować przez internet, powinieneś to chronić czymś więcej niż tylko nazwą użytkownika i hasłem.

Adaptacyjne Zasady i Kontrole

Zaawansowane rozwiązanie do uwierzytelniania wieloskładnikowego pozwala administratorom definiować zasady i poziomy dostępu za pomocą adaptacyjnych kontroli, równoważąc bezpieczeństwo i łatwość użycia w oparciu o użytkowników, grupy, urządzenia, sieci i zaangażowane aplikacje. Jedną z zasad bezpieczeństwa zero trust jest to, że granularne zasady dają dostęp do krytycznych danych tylko tym, którzy ich potrzebują.

Sprawdź, czy rozwiązanie pozwala tworzyć i egzekwować zaawansowane zasady i kontrole, które można zastosować w środowiskach z wrażliwymi danymi – niezależnie od tego, czy są one dostępne przez internet, czy w sieci prywatnej.

Przykłady adaptacyjnych zasad i kontroli obejmują:

- Wymaganie od administratorów i personelu IT wykonywania bezpieczniejszego uwierzytelniania dwuskładnikowego za pomocą biometrii lub klucza bezpieczeństwa opartego na FIDO za każdym razem, gdy logują się, aby chronić dostęp uprzywilejowany.
- Zezwolenie użytkownikom na rzadsze uwierzytelnianie podczas korzystania z tego samego urządzenia.
- Blokowanie próby logowania z obcych krajów, w których nie prowadzisz działalności, i blokowanie dostępu z anonimowych sieci, takich jak Tor.

- Zezwolenie użytkownikom na dostęp do krytycznych aplikacji tylko z urządzeń zarządzanych przez firmę.
- Zdefiniowanie, w jaki sposób użytkownicy uzyskują dostęp do wrażliwych systemów, takich jak serwery zawierające dane finansowe.
- Ustawienie bardziej rygorystycznej polityki dla serwerów z danymi płatniczymi klientów w porównaniu do publicznych serwerów plików.

Podczas gdy tradycyjne rozwiązania, takie jak zapory sieciowe i systemy kontroli dostępu do sieci (NAC), mogą to robić, zazwyczaj ograniczają się do ochrony zasobów lokalnych. Ale skupiając się tylko na lokalnej sieci, te rozwiązania pozostawiają wiele luk w zabezpieczeniach i zerowe pokrycie dla aplikacji chmurowych. Szukaj rozwiązania, które oferuje ochronę wykraczającą poza sieć lokalną i naprawdę chroni dostęp z dowolnego urządzenia i z dowolnej lokalizacji.

Średnio ponad 40% kont nie ma włączonych silnych form MFA.

Duo Trusted Access Report

Wdrażanie Uwierzytelniania Opartego na Ryzyku

Oprócz zmniejszenia zależności od haseł, uwierzytelnianie oparte na ryzyku jest bardzo skuteczną metodą blokowania atakującym nieautoryzowanego dostępu — zwłaszcza gdy decyzje o ryzyku są oparte na benchmarkach różnych organizacji i najlepszych praktykach branżowych.

Rozwiązanie dostępu powinno ciągle oceniać ryzyko dostępu, badając sygnały, takie jak lokalizacja użytkownika, urządzenie, przeglądarka i zachowanie dostępu przy każdej próbie logowania. Posiadanie tego kontekstu umożliwia zautomatyzowaną i dynamiczną odpowiedź na żądanie logowania, „wzmacniając" uwierzytelnianie, gdy jest to konieczne, stosując zasadę zero trust „nigdy nie ufaj, zawsze weryfikuj".

Jeśli możesz się do czegoś zalogować przez internet, powinieneś to chronić czymś więcej niż tylko nazwą użytkownika i hasłem.

Widoczność i Analityka

W idealnej sytuacji, Twoje nowe rozwiązanie powinno dawać wgląd w konta twoich użytkowników i urządzenia, których używają do uzyskiwania dostępu do aplikacji i danych Twojej organizacji. Zaawansowane rozwiązanie uwierzytelniające powinno dawać Ci szybki obraz profilu bezpieczeństwa wszystkich tożsamości i urządzeń w Twoim środowisku, zapewniając, że wszyscy użytkownicy są skonfigurowani z MFA i pozwalając chronić przed znanymi lukami. Ponieważ dane są użyteczne tylko wtedy, gdy są dostępne, upewnij się, że Twój pulpit nawigacyjny zapewnia kompleksowy

widok z lotu ptaka wraz z możliwością szybkiego powiększania lub filtrowania do bardziej szczegółowych informacji.

Twoje rozwiązanie tożsamości powinno zawierać szczegółowe dzienniki dotyczące Twoich użytkowników, urządzeń, administratorów i metod uwierzytelniania. Rozwiązanie powinno umożliwiać łatwe eksportowanie tych dzienników do narzędzi SIEM i pomagać w tworzeniu niestandardowych raportów, idealnych dla analityków bezpieczeństwa i audytorów zgodności.

Wybierz rozwiązanie, które daje Ci widoczność prób uwierzytelniania, w tym dane o adresach IP, anonimowych sieciach, krajach na czarnej liście i innych – przydatne do określania, gdzie i kiedy mogą wystąpić pewne ataki. Zapytaj, czy dostawca może wykrywać i automatycznie ostrzegać administratorów w przypadku ryzykownego zachowania logowania lub podejrzanych zdarzeń, takich jak rejestracja nowego urządzenia do uwierzytelniania lub logowanie z nieoczekiwanej lokalizacji.

Weryfikacja Stanu Urządzenia

Rozważ rozwiązanie, które oferuje kompleksowe możliwości weryfikacji urządzeń na laptopach, komputerach stacjonarnych i urządzeniach mobilnych. Rozwiązanie powinno zapewnić, że urządzenia uzyskujące dostęp do Twojego środowiska są zgodne z kryteriami bezpieczeństwa Twojej organizacji. Obejmuje to weryfikację, czy urządzenia mają zainstalowane krytyczne poprawki oprogramowania i umożliwienie samoobsługi użytkownika końcowego, gdzie ma to zastosowanie.

Sprawdź, czy rozwiązanie może wykorzystywać telemetrię z agentów bezpieczeństwa punktów końcowych i narzędzi do zarządzania urządzeniami w ramach oceny postawy.

Elastyczność

Wymiana rozwiązania jest kosztowna, więc wybierz takie, które może skalować się, aby obsługiwać nowych użytkowników, integracje i urządzenia – niezależnie od tego, gdzie się znajdują, w tym w siedzibie firmy i w chmurze. Sprawdź, czy Twój dostawca oferuje różne metody uwierzytelniania, w tym aplikacje na smartfony, biometrię, inteligentne urządzenia noszone, oddzwanianie telefoniczne, kody dostępu i tokeny sprzętowe, aby zaspokoić potrzeby każdego użytkownika.

Strategiczne Inicjatywy Biznesowe

Oceniając nowe rozwiązanie bezpieczeństwa, rozważ, jak może ono integrować się z bieżącymi lub przyszłymi inicjatywami biznesowymi, w tym z systemami starszymi, zasadą „przynieś własne urządzenie” (*ang. Bring Your Own Device - BYOD*), pracą zdalną lub przyjęciem aplikacji chmurowych. Inne czynniki biznesowe do rozważenia to wymogi regulacyjne dotyczące zgodności, które różnią się w zależności od branży i lokalizacji.

Wdrożenie usług chmurowych

Podczas gdy wiele Twoich aplikacji i serwerów może znajdować się w siedzibie firmy, implementacje chmurowe rozprzestrzeniły się w ciągu ostatnich kilku lat. Sprawdź, czy rozwiązanie uwierzytelniające może łatwo integrować się z Twoimi aplikacjami chmurowymi. Dodatkowo, jeśli odchodzisz od zarządzania oprogramowaniem i sprzętem w siedzibie firmy, powinieneś rozważyć przyjęcie chmurowego rozwiązania uwierzytelniającego, które może skalować się w miarę potrzeb. Upewnij się, że Twoje rozwiązanie uwierzytelniające chroni to, co ważne zarówno dziś, jak i w przyszłości.

Przynieś Własne Urządzenie (BYOD) — Ochrona Pracy Zdalnej

Wiele organizacji pozwala pracownikom używać ich osobistych urządzeń do wykonywania pracy. Oceniając rozwiązania uwierzytelniające, rozważ, jak są one kompatybilne z Twoim środowiskiem BYOD. Czy użytkownicy mogą używać swoich własnych urządzeń do ukończenia uwierzytelniania?

Sprawdź, czy Twoje rozwiązanie uwierzytelniające zapewnia aplikację mobilną, która działa ze wszystkimi różnymi urządzeniami mobilnymi i zdalnymi, których używają Twoi pracownicy, w tym Windows, Apple iOS i Android. Dla elastyczności, upewnij się, że rozwiązanie działa z innymi metodami, takimi jak klucze bezpieczeństwa, powiadomienia push, generatory kodów i oddzwanianie telefoniczne.

Czy Twoje rozwiązanie uwierzytelniające może wykrywać potencjalne luki w urządzeniach używanych przez Twoich pracowników? Zapytaj swojego dostawcę, jak możesz uzyskać większą widoczność i kontrolę nad swoim środowiskiem chmurowym i mobilnym, bez konieczności rejestrowania przez użytkowników ich osobistych urządzeń w rozwiązaniach mobilności przedsiębiorstwa (takich jak zarządzanie urządzeniami mobilnymi/MDM).

Jeśli nie jest łatwe w użyciu, Twoi użytkownicy go nie użyją. Oceń użyteczność swojej aplikacji mobilnej, zarówno dla użytkowników (rejestracja, aktywacja i codzienne uwierzytelnianie), jak i administratorów (zarządzanie użytkownikami i rozwiązaniem).

Monitorowanie i Raportowanie

Upewnij się, że Twoje rozwiązanie zawiera szczegółowe dzienniki aktywności użytkowników, dzięki czemu możesz tworzyć niestandardowe raporty, idealne do analizy bezpieczeństwa i dla audytorów zgodności. Uzbrojony w szczegóły dotyczące statusów jailbreak, poziomów poprawek, przeglądarek i innych, możesz również podjąć działania, aby zapobiec otwarciu sieci na znane luki. Monitorowanie daje również wgląd w wszelkie anomalie zachowań użytkowników lub niemożliwe geograficznie logowania – jeśli Twój użytkownik loguje się z jednej lokalizacji, a następnie loguje się z tymi samymi danymi uwierzytelniającymi z innej lokalizacji na świecie, Twój zespół bezpieczeństwa będzie o tym wiedział.

Walidacja i Zgodność

Jeśli masz do czynienia z jakimkolwiek rodzajem wrażliwych danych, takich jak dane osobowe (PII), chronione informacje zdrowotne (PHI), dane płatnicze klientów itp., musisz upewnić się, że Twoje rozwiązanie dwuskładnikowe może spełnić wszelkie wymogi regulacyjne dotyczące zgodności.

Dodatkowo, Twój dostawca MFA musi być w stanie dostarczyć aktualny dowód zgodności dla Twoich audytorów. Zapytaj swojego dostawcę, czy jego firma i rozwiązanie są corocznie lub regularnie audytowane przez niezależnego audytora zewnętrznego.

Sprawdź, czy chmurowa usługa dostawcy używa dostawców usług zgodnych z PCI DSS (Payment Card Industry Data Security Solution), ISO (International Organization for Standardization) 270001 i SOC (Service Organization Controls) 2. Wystarczy jedno słabe ogniwo w łańcuchu bezpieczeństwa wykonawców, aby naruszenie wpłynęło na Twoją organizację.

Pamiętaj, wystarczy jedno słabe ogniwo w łańcuchu bezpieczeństwa, aby naruszenie wpłynęło na Twoją organizację.

Całkowity Koszt Posiadania

Całkowity koszt posiadania obejmuje wszystkie bezpośrednie i pośrednie koszty posiadania produktu – dla rozwiązania uwierzytelniania wieloskładnikowego mogą to być ukryte koszty, takie jak początkowe, kapitałowe, licencyjne, wsparcia, utrzymania, operacyjne i wiele innych nieprzewidzianych wydatków w czasie, takich jak usługi profesjonalne oraz bieżące koszty operacyjne i administracyjne.

Jak możesz mieć pewność, że uzyskujesz najlepszy zwrot z inwestycji w bezpieczeństwo? Rozważ:

Koszty Początkowe

Sprawdź, czy model zakupu Twojego dostawcy wymaga płatności za urządzenie, użytkownika lub integrację – jest to ważne, jeśli Twoja firma planuje skalować i dodawać nowe aplikacje lub usługi w przyszłości. Wiele usług hostowanych zapewnia model licencjonowania na użytkownika, z płaską miesięczną lub roczną opłatą za każdego zarejestrowanego użytkownika. Badając koszty licencjonowania, upewnij się, że potwierdzisz, czy licencje są nazwane (zablokowane na jeden identyfikator użytkownika) czy przenoszalne, czy są dodatkowe opłaty za dodatkowe urządzenia lub skonfigurowane integracje, lub opłaty za dostawę dla różnych metod czynnika. Oszacuj, ile będzie kosztować wdrożenie uwierzytelniania wieloskładnikowego dla wszystkich aplikacji i użytkowników.

Oprogramowanie/Sprzęt Administracyjny

Czy jest to wliczone w licencję na oprogramowanie? Często wymagane jest dodatkowe oprogramowanie do zarządzania – bez niego klienci nie mogą wdrożyć MFA. Czy usługa wymaga zakupu i konfiguracji sprzętu w Twoim środowisku? Potwierdź początkowe i powtarzające się koszty tego sprzętu oraz zbadaj typowy czas i zaangażowanie pracy potrzebne do skonfigurowania tych narzędzi. w przypadku dostępu administracyjnego z warstwowymi uprawnieniami w zależności od wersji licencji, potwierdź, że cała funkcjonalność, na której polegasz, jest dostępna, lub zbierz pełną listę niezbędnych dopłat.

Konsolidacja Dostawców

Podczas gdy środowiska sieciowe z tradycyjnym modelem ochrony sieci polegają na kilku kluczowych usługach w celu utrzymania widoczności i egzekwowania standardów bezpieczeństwa, wzrost przyjęcia SaaS doprowadził do korzystania z wielu fragmentarycznych rozwiązań w celu pokrycia rozszerzonych potrzeb zabezpieczania danych i zasobów opartych na chmurze.

Bezpieczny dostęp obejmuje silne uwierzytelnianie poprzez MFA w celu walidacji użytkowników i może również obejmować:

- Narzędzia do zarządzania punktami końcowymi lub zarządzania urządzeniami mobilnymi w celu obrony przed zagrożeniami związanymi z kompromitacją urządzeń
- Portale pojedynczego logowania w celu scentralizowania i uproszczenia procesów logowania dla użytkowników
- Narzędzia do analizy logów w celu identyfikacji i eskalacji potencjalnych zagrożeń bezpieczeństwa
- Wiele pulpitów nawigacyjnych do zarządzania rozproszonymi usługami i pokrywania nieobsługiwanych aplikacji

Wraz z redundantnymi kosztami, które mogą wynikać z tych nakładających się usług, każde dodane narzędzie zwiększa złożoność i szanse na błąd ludzki lub przeoczenie. Znalezienie rozwiązania z kompleksową użytecznością dla bezpiecznego dostępu może zmniejszyć zarówno początkowe, jak i bieżące koszty pracy związane z zarządzaniem.

Szukaj dostawców z prostymi modelami subskrypcji, wycenionymi na użytkownika, z elastycznymi okresami umów.

Autentykatory

Czy musisz kupować sprzętowe urządzenia uwierzytelniające? Fizyczne tokeny dodają koszty inwentaryzacji, zarządzania i wysyłki. w przypadku mobilnych autentykatorów, potwierdź, czy istnieje jakikolwiek koszt za urządzenie dla tokenów programowych, czy też dozwolona jest nieograniczona liczba zarejestrowanych urządzeń dla każdej licencji użytkownika.

Konfiguracja Wysokiej Dostępności

Czy jest to również wliczone w Twoją licencję na oprogramowanie? Konfigurując zduplikowane instancje oprogramowania i łącząc load balancer z główną instancją, możesz potroić koszty oprogramowania. Konfiguracja redundantna lub odzyskiwania po awarii może również znacznie zwiększyć koszty, a niektórzy dostawcy pobierają dodatkowe opłaty licencyjne za ciągłość działania.

Opłaty za Wdrożenie

Wdrożenie i Konfiguracja

Dowiedz się, czy możesz wdrożyć rozwiązanie, korzystając z własnych zasobów, czy też będzie to wymagało wsparcia i czasu profesjonalnych usług w celu zainstalowania, przetestowania i rozwiązania problemów ze wszystkimi niezbędnymi integracjami.

Rejestracja Użytkownika Końcowego

Oszacuj, ile czasu zajmie każdemu użytkownikowi rejestracja i czy wymaga to dodatkowego szkolenia administracyjnego i czasu pomocy technicznej. Omów z dostawcą typowy czas wdrożenia oczekiwany w Twoim przypadku użycia i zasięgnij opinii od podobnych organizacji, aby zweryfikować, jak to się zgadza z ich doświadczeniem. Szukaj intuicyjnego doświadczenia użytkownika końcowego i prostego procesu rejestracji które nie wymaga obszernego szkolenia. Rozwiązania oparte na tokenach są często droższe w dystrybucji i zarządzaniu niż w zakupie.

Wsparcie Administratora

Aby ułatwić pracę administratorom, szukaj gotowych integracji dla głównych aplikacji, aby skrócić czas i zasoby potrzebne do wdrożenia. Potwierdź również dostępność integracji ogólnego przeznaczenia dla najpopularniejszych protokołów uwierzytelniania, aby pokryć przypadki brzegowe, wraz z API do uproszczenia integracji dla aplikacji internetowych. Zobacz, czy możesz ustawić program pilotażowy do testowania i zbierania opinii użytkowników – proste integracje nie powinny trwać dłużej niż 15 minut.

Koszty Bieżące

Poprawki Bezpieczeństwa, Utrzymanie i Aktualizacje

Roczna opłata za utrzymanie może zwiększyć koszty oprogramowania i sprzętu, ponieważ klienci muszą płacić za bieżące aktualizacje, poprawki i wsparcie. Często to klient jest odpowiedzialny za wyszukiwanie nowych poprawek od dostawcy i ich stosowanie, co wymaga czasu i zasobów.

Szukaj dostawcy, który automatycznie aktualizuje oprogramowanie w przypadku nowych naruszeń bezpieczeństwa i innych krytycznych aktualizacji, oszczędzając koszty zatrudnienia zespołu. Wybierz dostawcę, który często aktualizuje i najlepiej wprowadza automatyczne aktualizacje bez żadnej pomocy ze strony Twojego zespołu.

Utrzymanie administracji

Rozważ koszty zatrudnienia pełnoetatowego personelu do utrzymania Twojego rozwiązania MFA. Czy Twój dostawca utrzymuje rozwiązanie wewnętrznie, czy to Ty musisz zatrudnić ekspertów do zarządzania nim?

Oszacuj, ile czasu zajmuje wykonanie rutynowych zadań administracyjnych. Czy łatwo jest dodawać nowych użytkowników, cofać poświadczenia lub wymieniać tokeny? Rutynowe zadania, takie jak zarządzanie użytkownikami, powinny być proste. Zarejestruj się na okres próbny i przetestuj go przed wdrożeniem dla wszystkich użytkowników.

Wsparcie i Pomoc Techniczna

Gartner szacuje, że zapytania o resetowanie haseł stanowią od 30% do 50% wszystkich połączeń z pomocą techniczną. a według Forrester, od 25% do 40% wszystkich połączeń z pomocą techniczną wynika z problemów z hasłami lub resetowania. Forrester ustalił również, że duże organizacje wydają do 1 miliona dolarów rocznie na personel i infrastrukturę tylko na obsługę resetowania haseł, przy średnim koszcie pracy dla pojedynczego resetowania hasła wynoszącym 70 dolarów.

Jeśli rozwiązanie wymaga obszernego wsparcia ze strony Twojego zespołu IT lub infrastruktury, czy zostaniesz obciążony kosztami czasu spędzonego na wspieraniu Twojego rozwiązania MFA w siedzibie firmy? Oszacuj ten koszt i uwzględnij go w swoim budżecie.

Nowoczesne Rozwiązania – brak kosztów ukrytych

- Wysoka wartość, koszty początkowe
- Prosty model subskrypcji
- Darmowa aplikacja mobilna do uwierzytelniania
- Brak opłat za dodawanie nowych aplikacji lub urządzeń
- Brak kosztów utrzymania centrum danych/serwerów
- Automatyczne aktualizacje bezpieczeństwa i aplikacji
- Panel administracyjny w zestawie
- Portal samoobsługowy dla użytkowników w zestawie
- Zasady i kontrole dostępu użytkowników, urządzeń i aplikacji
- Oceny stanu i postawy urządzenia
- Kontekst urządzenia z rozwiązań bezpieczeństwa innych firm
- Uwierzytelnianie bezhasłowe
- Analiza zachowań użytkowników
- Pojedyncze logowanie (SSO) i wsparcie chmury

Tradycyjne Rozwiązania – wiele ukrytych kosztów

- Potencjalnie niskie koszty początkowe, niewielka wartość
- Dodatkowy koszt za dodawanie nowych aplikacji lub użytkowników — oprogramowanie/sprzęt administracyjny
- Autentykatory — tokeny, USB itp.
- Utrzymanie centrum danych i serwerów
- Konfiguracja wysokiej dostępności
- Wsparcie administracyjne
- Poprawki, konserwacja i aktualizacje
- Wsparcie pomocy technicznej

Czas do Wartości

Czas do wartości, czyli czas do bezpieczeństwa, odnosi się do czasu poświęconego na wdrożenie, uruchomienie i adaptację rozwiązania. Określ, ile czasu zajmuje, zanim Twoja firma zacznie czerpać korzyści z bezpieczeństwa rozwiązania uwierzytelniania wieloskładnikowego. Jest to szczególnie ważne po niedawnym naruszeniu lub incydencie bezpieczeństwa.

Proof of Concept - pilotaż

Uruchomienie programu pilotażowego MFA pozwala przetestować rozwiązanie na małej grupie użytkowników, dając możliwość zebrania cennych informacji zwrotnych na temat tego, co działa, a co nie, przed wdrożeniem go w całej organizacji.

Wdrożenie

Przejdź przez prawdopodobne scenariusze implementacji, aby oszacować czas i koszty związane z udostępnianiem bazy użytkowników. Usługi oparte na chmurze zapewniają najszybsze czasy wdrożenia, ponieważ nie wymagają instalacji sprzętu ani oprogramowania, podczas gdy rozwiązania lokalne zazwyczaj wymagają więcej czasu i zasobów, aby je uruchomić.

Większość specjalistów ds. bezpieczeństwa nie ma czasu na pisanie własnego kodu integracyjnego. Wybierz dostawcę, który dostarcza gotowe integracje dla wszystkich głównych aplikacji chmurowych, VPN-ów, systemów Unix i rozwiązań dostępu zdalnego Microsoft. Będziesz także chciał poszukać dostawcy, który umożliwia automatyzację funkcjonalności i eksportowanie logów w czasie rzeczywistym.

Ponadto, aby zaoszczędzić czas na integracji pojedynczego logowania, sprawdź, czy Twoje rozwiązanie MFA obsługuje standard uwierzytelniania SAML (Security Assertion Markup Language), który deleguje uwierzytelnianie od dostawcy usług lub aplikacji do dostawcy tożsamości.

Wdrażanie i Szkolenie Użytkowników

Proces rejestracji u dostawcy jest często głównym pochłaniaczem czasu dla administratorów IT. Upewnij się, że przechodzisz przez cały proces, aby zidentyfikować wszelkie potencjalne problemy.

W przypadku przedsiębiorstw, masowa rejestracja może być bardziej efektywnym czasowo sposobem na zapisanie dużej liczby użytkowników.

Aby wspierać Twoje aplikacje chmurowe, upewnij się, że Twoje rozwiązanie MFA pozwala szybko udostępniać MFA dla nowych użytkowników dla aplikacji chmurowych, używając istniejących poświadczeń lokalnych i prostej synchronizacji z dostawcą tożsamości (IdP).

Sprawdź, czy rozwiązanie wymaga sprzętu lub oprogramowania dla każdego użytkownika, lub czasochłonnego szkolenia użytkowników. Wdrożenie tokenów może wymagać dedykowanego zasobu, ale łatwa samoobsługa eliminuje potrzebę ręcznego udostępniania tokenów.

Dzięki mobilnemu rozwiązaniu opartemu na chmurze, użytkownicy mogą szybko pobrać aplikację na swoje urządzenia. Rozwiązanie, które pozwala użytkownikom pobierać, rejestrować i zarządzać własnymi urządzeniami uwierzytelniającymi za pomocą tylko przeglądarki internetowej, może również zaoszczędzić czas zespołu wdrożeniowego.

Wymagane Zasoby

Rozważ czas, personel i inne zasoby wymagane do integracji aplikacji, zarządzania użytkownikami i urządzeniami oraz utrzymania/monitorowania rozwiązania. Zapytaj swojego dostawcę, co pokrywa i gdzie musisz uzupełnić luki.

Wsparcie Aplikacji

Niektóre rozwiązania MFA wymagają więcej czasu i personelu do integracji z Twoimi aplikacjami, zarówno lokalnymi, jak i chmurowymi. Sprawdź, czy dostarczają obszerną dokumentację, a także API i SDK, abyś mógł łatwo wdrożyć rozwiązanie w każdej aplikacji, na której polega Twoja organizacja.

Zarządzanie Użytkownikami i Urządzeniami

Jak każde dobre narzędzie bezpieczeństwa, Twoje rozwiązanie MFA powinno dawać administratorom moc potrzebną do wspierania użytkowników i urządzeń z minimalnym trudem.

Szukaj rozwiązania z scentralizowanym panelem administracyjnym dla skonsolidowanego widoku Twoich wdrożeń dwuskładnikowych i umożliwiającego administratorom:

- Łatwe generowanie kodów awaryjnych dla użytkowników, którzy zapomnieli lub zgubili telefony.
- Dodawanie i cofanie poświadczeń w miarę potrzeb, bez konieczności udostępniania i zarządzania fizycznymi tokenami.

Zapytaj swojego dostawcę, czy oferuje portal samoobsługowy, który pozwala użytkownikom zarządzać własnymi kontami, dodawać lub usuwać urządzenia i wykonywać inne proste zadania.

Utrzymanie

Upewnij się, że Twoje rozwiązanie wymaga minimalnej bieżącej konserwacji i zarządzania, co przekłada się na niższe koszty operacyjne. Rozwiązania hostowane w chmurze są wygodne, ponieważ dostawca zajmuje się infrastrukturą, aktualizacjami i konserwacją.

Czy możesz wykorzystać swój istniejący personel do wdrożenia i utrzymania tego rozwiązania, czy będziesz musiał zatrudnić więcej personelu lub wykonawców do wykonania tej pracy? Zapytaj swojego dostawcę, czy monitorowanie lub logowanie jest wliczone w rozwiązanie.

Rozwiązanie, które wymaga wielu dodatkowych zasobów do adaptacji i skalowania, może nie być warte kosztów i czasu. Oceń, czy Twoje rozwiązanie pozwala łatwo dodawać nowe aplikacje lub zmieniać polityki bezpieczeństwa w miarę ewolucji potrzeb Twojej firmy.