

RSA® Authentication Manager Express

Mechanizm silnego uwierzytelniania za przystępną cenę wprost od lidera tej branży

W skrócie

- Sprawdzona technologia uwierzytelniania wieloskładnikowego
- Optymalizacja z uwzględnieniem ograniczonych zasobów firm (do 2500 użytkowników)
- Płynne przejście od zabezpieczenia hasłami do mechanizmu silnego uwierzytelniania
- Możliwość dynamicznego dopasowywania uwierzytelniania do profilu użytkownika i poziomu ryzyka związanego z próbą uwierzytelnienia
- Łatwe wdrożenie i użytkowanie w każdym środowisku: rozwiązanie od razu po zainstalowaniu obsługuje najbardziej znane systemy SSL VPN i aplikacje WWW

Pracownik współczesnej firmy musi być coraz bardziej mobilny, a sama firma musi ściśle przestrzegać przepisów oraz chronić poufne informacje i własność intelektualną przed wyrafinowanymi atakami. Słabe zabezpieczenia oparte tylko na hasłach nie wystarczają do odstraszenia cyberprzestępców świetnie znających się na technologiach i nie zapobiegają przedostaniu się materiałów firmy w niepowołane ręce. Coraz więcej firm przenosi informacje do systemów dostępnych online i zapewnia zdalny dostęp do zasobów danych przez systemy SSL VPN i aplikacje WWW. W tej sytuacji silne uwierzytelnianie staje się koniecznością.

Wybierając spośród dostępnych mechanizmów silnego uwierzytelniania, firma powinna postawić na rozwiązanie zapewniające bezpieczeństwo, ale równocześnie nie utrudniające pracy użytkownikom ani nie obciążające budżetu lub zasobów informatycznych.

Silne uwierzytelnianie za przystępną cenę

RSA Authentication Manager Express to rozwiązanie do silnego uwierzytelniania wieloskładnikowego, skutecznie zabezpieczające, wygodne w obsłudze i nienadwyżające budżetu firmy. Rozwiązanie RSA Authentication Manager Express zabezpiecza silniej i skuteczniej niż hasła, otwierając pole do wdrożenia zdalnego i całodobowego dostępu do informacji firmy dla telepracowników, partnerów, wykonawców i klientów. Silne uwierzytelnianie jest oparte na sprawdzonych technologiach i można je dopasować do ograniczonych zasobów firmy, założeń tolerancji ryzyka oraz profili użytkowników.

Płynne przejście od haseł do uwierzytelniania wieloskładnikowego

RSA Authentication Manager Express to rozwiązanie do płynnego i silnego uwierzytelniania, stopniowane w zależności od ryzyka (risk-based authentication). W sposób niezakłócający pracy chroni materiały dostępne przez Internet (sieci VPN i aplikacje WWW) przed nieuprawnionym dostępem. Użytkownicy nadal mogą stosować zwykłe nazwy i hasła, ale mechanizm RSA Risk Engine uwzględnia podczas uwierzytelniania także liczne inne czynniki, zaliczające się do następujących trzech kategorii:

- coś, co użytkownik wie: na przykład nazwa użytkownika i hasło;
- coś, co użytkownik ma: na przykład laptop lub komputer stacjonarny;
- coś, co użytkownik robi: na przykład czynności niedawno wykonywane na koncie.

Mechanizm RSA Risk Engine określa poziom wiarygodności użytkownika na podstawie podobieństwa tych czynników do wcześniej zarejestrowanych zdarzeń związanych z uwierzytelnianiem. Kiedy obliczony poziom wiarygodności jest równy lub wyższy od poziomu określonego przez firmę, użytkownik zostaje uwierzytelniony. W typowej sytuacji użytkownik nie ma świadomości działania mechanizmu wieloskładnikowego — po prostu podaje hasło.

Jeśli podczas próby uwierzytelnienia pewne cechy odbiegają od tych zarejestrowanych przy wcześniejszych przypadkach uwierzytelniania — na przykład podczas próby połączenia z nowego urządzenia — użytkownik musi przedstawić

dotatkowy dowód tożsamości. Może być na przykład konieczne podanie znanej użytkownikowi odpowiedzi na pewne pytanie albo przedstawienie kodu autoryzacyjnego przesłanego przez SMS lub e-mail.

Prosta instalacja, wdrożenie i oddanie do dyspozycji użytkownikom

RSA Authentication Manager Express zapewnia najszybsze i najbezpieczniejsze wdrożenie mechanizmu uwierzytelniania wieloskładnikowego. Rozwiązanie to jest dostarczane w postaci fabrycznie przygotowanej do wdrożenia i użytkowania, na bazie bezpiecznej i wygodnej w obsłudze platformy sprzętowej (Appliance). Zarządzanie odbywa się za pomocą intuicyjnej konsoli dostępnej przez przeglądarkę, a rozwiązanie jest fabrycznie zintegrowane z systemami SSL VPN i serwerami WWW, co zostało potwierdzone stosownymi certyfikatami. Instalacja i integracja rozwiązania RSA Authentication Manager Express z dotychczasowym środowiskiem firmy przebiega bardzo płynnie.

Wdrożenie rozwiązania RSA Authentication Manager Express opartego na poziomie ryzyka sprowadza się do wskazania serwerowi istniejącej populacji użytkowników w usłudze Microsoft Active Directory i wybrania minimalnego poziomu pewności wymaganego do uwierzytelnienia. Mechanizm RSA Risk Engine rozpoczyna monitorowanie przypadków uwierzytelniania i gromadzenie związanych z tym informacji. W ten sposób buduje profile użytkowników na potrzeby szacowania ryzyka i porównywania podczas późniejszego uwierzytelniania — wszystko to w sposób niewidoczny dla użytkowników. Po zgromadzeniu ilości informacji wystarczającej do utworzenia profilu użytkownika mechanizm ten automatycznie aktywuje nowe reguły i rozpoczyna uwierzytelnianie z uwzględnieniem wielu czynników. Z perspektywy użytkownika przejście na uwierzytelnianie wieloskładnikowe jest płynne — nadal wymaga się po prostu podania hasła. W instalacji z mechanizmem RSA Authentication Manager Express hasła dają lepsze zabezpieczenie, a użytkownik nie musi uczyć się nowych czynności ani pamiętać wielu informacji wymaganych do poświadczenia tożsamości.

Uczący się, sprawdzony mechanizm Risk Engine

Ten sam mechanizm RSA Risk Engine, który użyto w rozwiązaniu RSA Authentication Manager Express jest stosowany do zabezpieczenia rachunków ponad 250 milionów klientów bankowości online na całym świecie. Jest sprawdzony i bezpieczny. Pozwala skutecznie potwierdzić tożsamość bez utrudniania pracy użytkownikom i wymagania dodatkowych czynności uwierzytelniających. Mechanizm RSA Risk Engine nie bazuje na regułach statycznych, lecz uwzględnia kombinacje różnych czynników: danych urządzenia oraz sposobu postępowania użytkownika. Gromadzi informacje o urządzeniach, osobach i całej populacji użytkowników, dynamicznie analizuje te dane i dostosowuje model ryzyka. Użytkownicy, w których przypadku ustalono niski poziom ryzyka, są uwierzytelniani bez dodatkowych zabiegów. Użytkownicy o podwyższonym poziomie ryzyka muszą podać dodatkowe informacje. W rozwiązaniu RSA Authentication Manager Express administrator ma możliwość określenia —

odpowiednio do reguł zarządzania ryzykiem w firmie — w jaki sposób i kiedy użytkownicy muszą podawać dodatkowe dane.

Analizowanie urządzeń

Mechanizm analizowania urządzeń zastosowany w rozwiązaniu RSA Authentication Manager Express w niewidoczny sposób analizuje dane komputera stacjonarnego lub laptopa użytkownika. Procedura ta jest wykonywana dynamicznie i przy każdej próbie uwierzytelnienia. Uwzględniane są dziesiątki parametrów charakterystycznych dla danego urządzenia. Na podstawie tych informacji mechanizm RSA Risk Engine może określić, czy dane urządzenie było wcześniej używane przez tę osobę i czy może zostać uznane za wiarygodne. Jeśli tak, użytkownik zostaje uwierzytelniony po podaniu hasła. Natomiast jeśli urządzenie nie jest rozpoznawane, użytkownik musi przedstawić dodatkowy dowód tożsamości. Dzięki funkcji analizowania urządzeń komputer użytkownika staje się wiarygodnym dodatkowym czynnikiem uwierzytelniania — eliminuje konieczność przedstawiania statycznych poświadczeń i instalowania dodatkowego oprogramowania.

Analiza behawioralna

Analiza behawioralna polega na ocenianiu wzorców zachowań użytkowników, przypadków uwierzytelniania i uzyskiwania dostępu do konta oraz innych czynników składających się na ocenę poziomu ryzyka podczas każdej próby uwierzytelnienia. Ryzyko behawioralne oblicza się przez porównanie bieżącego żądania uwierzytelnienia z historią uwierzytelniania danego użytkownika, znanymi zachowaniami innych użytkowników populacji oraz sygnaturami behawioralnymi typowymi dla prób uzyskania nieuprawnionego dostępu. Kiedy ryzyko jest niskie, zachowania użytkownika stanowią kolejny czynnik uwierzytelniający, który potwierdza tożsamość posiadacza konta w sposób niezauważalny dla tej osoby.

Funkcje i elementy rozwiązania RSA Authentication Manager Express są wzajemnie powiązane i działają w połączeniu. Tworzą jeden wieloskładnikowy mechanizm uwierzytelniania, zapewniający jednocześnie wyjątkowe bezpieczeństwo, wygodę i niski koszt, których wymagają firmy. RSA Authentication Manager Express to jeden z produktów związanych z uwierzytelnianiem oferowanych przez firmę RSA — lidera na rynku rozwiązań uwierzytelniających. Pozwala wdrożyć uwierzytelnianie wieloskładnikowe w sposób bezpieczny dla infrastruktury.



www.rsa.com

©2010 EMC Corporation. Wszelkie prawa zastrzeżone. EMC, EMC, RSA oraz logo RSA to zastrzeżone znaki towarowe lub znaki towarowe firmy EMC Corporation w Stanach Zjednoczonych i/lub innych krajach. Wszelkie inne wymienione produkty i usługi stanowią znaki towarowe odpowiednich podmiotów.

AMX_DS_1210