Systemy autoryzacji dwuskładnikowej -2FA

Właściwa ochrona systemów IT wymaga, aby zabezpieczenia były dostosowane do zmian w sieciach oraz do nowych zagrożeń. Tradycyjne systemy zabezpieczeń, które spełniały wszystkie oczekiwania i zapewniały bezpieczny dostęp kilka lat temu są obecnie nieadekwatne pod względem zapewnianego poziomu ochrony. Standardy bezpieczeństwa obowiązujące jeszcze 3-4 lata temu, w tym autoryzacja bazująca na statycznych hasłach, w dobie zagrożeń takich jak ataki phishingowe, spyware oraz APT (Advanced Persistent Threat) stają się zdecydowanie przestarzałe.

Na szczególne ryzyko narażone są systemy "stykające" się ze światem zewnętrznym - tj. systemy zdalnego dostępu VPN i remote-desktop, poczta elektroniczna typu webmail, systemy wymiany plików, itp.

Przegląd rozwiązań 2FA

Powszechnie uznaje się, że właściwą metodą kontroli dostępu jest autoryzacja użytkowników bazująca na modelu 2FA (Two Factor Authentication), a więc zazwyczaj na czymś, co użytkownik zna (hasło) i na czymś, co posiada (token uwierzytelniający, smartfon, lista haseł jednorazowych, itd.). Z przyczyn praktycznych, najczęściej stosowane są systemy 2FA bazujące na tokenach PKI (z portem USB - przechowujące certyfikat) lub karty inteligentne (SC - Smart Card), tokeny OTP (generujące hasła jednorazowe na wyświetlaczu LCD) oraz tokeny wirtualne w postaci aplikacji na smartfonie.

Tokeny OTP

Autoryzacja OTP (One Time Password) polega na wykorzystaniu sprzętowego lub programowego generatora haseł jednorazowych. Każda operacja wymagająca autoryzacji (np. zestawienie sesji zdalnego dostępu) musi być uwierzytelniona poprzez przepisanie przez użytkownika hasła z wyświetlacza tokena OTP. Swoistą odmianą autoryzacji OTP jest autoryzacja SMS (kod przekazywany SMS-em na telefon użytkownika) oraz rozwiązania bazujące na tokenie realizowanym jako aplikacja na smartfonie. Fizyczne tokeny OTP mogą być zaopatrzone w klawiaturę, która służy do podawania PIN-u a także potrzebna jest przy autoryzacji Ch-Rp (challenge-response). Autoryzacja Ch-Rp stosowana jest zazwyczaj w apliakcjach i polega na dwukrokowej sekwencji uwierzytelnienia: aplikacja wyświetla ciąg znaków zwany "Challenge", który użytkownik przepisuje do tokena, token w odpowiedzi wyświetla ciąg znaków "Response", który użytkownik wprowadza do apliakacji. Ten sposób uwierzytelnienia operacji jest obecnie rekomendowany lub nawet wymagany np. w apliakacjach bankowych przy operacjach takich jak przelewy.

Tokeny PKI/USB oraz karty SM
(Smart Cards)

Autoryzacja bazuje na kluczu prywatnym oraz publicznym certyfikacie przechowywanym na sprzętowym nośniku (tokenie USB lub karcie inteligentnej). Klucz prywatny jest przechowywany w sposób bezpieczny, co oznacza, że jest zabezpieczony hasłem i nie może być skopiowany ze swojego sprzętowego nośnika. Ten rodzaj autoryzacji jest szczególnie wygodny w systemach zdalnego dostępu SSL i IPsec VPN oraz przy logowaniu do lokalnego systemu lub domeny Windows. Tzw. karty inteligenetne są funkcjonalnie równoważne tokenom USB, ich zaletą jest możliwość umieszczenia na nich dodatkowej informacji (danych użytkownika, zdjęcia) oraz zintegrowania ich z radiowym modułem kontroli fizycznego dostępu do pomieszczeń, na przykład zgodnym ze standardem MIFARE.

Systemy chmurowe - SaaS
(Software as a Service)

W modelu tym wdrożenie autoryzacji 2FA bardzo się uprościło - użytkownicy otrzymują tokeny fizyczne lub instalują aplikację na smartfonie, administrator konfiguruje reguły dostępu i przeprowadza integrację systemu autoryzacji z firewallem lub bramką VPN, jednak cały system autoryzacji znajduje się na serwerach chmurowych. Dzięki temu firma posiada kontrolę administracyjną nad dostępem użytkowników, nie ponosi jednak kosztów amortyzacji i eksploatacji serwerów uwierzytelniających.

CC oferuje

W dziedzinie opisywanych rozwiązań autoryzacji oferujemy nie tylko dostawy oprogramowania i tokenów autoryzacyjnych, ale także pełną gamę usług: prowadzimy analizę potrzeb klientów, projektujemy systemy autoryzacji oraz integrujemy je z systemami zdalnego dostępu, infrastrukturą VPN, systemem domenowym, itd. Realizujemy testy oraz diagnostykę istniejącej infrastruktury, wykonujemy częściowe lub pełne migracje rozwiązań sieciowych, wdrażamy i konfigurujemy nowy sprzęt, prowadzimy nadzór oraz utrzymanie w trybie 24x7, a także realizujemy szkolenia warsztatowe. Wszystkie usługi wykonywane są przez naszych pracowników posiadających certyfikaty inżynierów danego producenta - posiadamy i utrzymujemy aktualne certyfikacje wszystkich kluczowych, wymienionych niżej dostawców rozwiązań sieciowych.

Producenci:
Gemalto, HID Global, Vasco, Wheel.

gemalto security to be free · HID · VASCO TRUST FOR THE DIGITAL WORLD · WHEEL SYSTEMS

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: sales@cc.com.pl

Więcej informacji znajdziecie Państwo w Internecie, na stronach:
http://www.cc.com.pl/

Kontakt:
Kontakt ogólny: cc@cc.com.pl
Dział Handlowy: sales@cc.com.pl
Dział Techniczny: tech@cc.com.pl