ESET SECURE AUTHENTICATION

Ultrasilna autoryzacja użytkowników dla ochrony sieci i danych firmowych

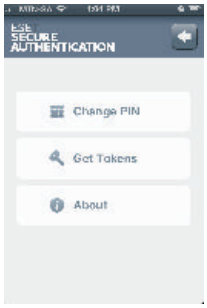
ESET Secure Authentication zapewnia silną autoryzację użytkowników, aby zdalne połączenia z siecią firmową oraz dostęp do danych sensytywnych był bezpieczny i bezproblemowy. Jest to rozwiązanie wykorzystujące dwuskładnikową autoryzację dostępu do firmowego VPN i OWA, z użyciem jednorazowego hasła (OTPs). Zaletą takiego hasła jest jego losowe generowanie, a co za tym idzie brak możliwości odgadnięcia i ponownego wykorzystania.

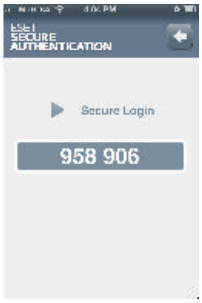
Jak działa ESET Secure Authentication?

Podczas zdalnego łączenia się z siecią firmową przez VPN lub OWA, pracownicy otrzymują jednorazowe hasło na swoją komórkę. Hasło to jest następnie wykorzystane w celu dopełnienia i wzmocnienia standardowych procesów autoryzacji. W rezultacie, dane firmowe są chronione przed intruzami, atakami słownikowymi, próbami kradzieży hasła oraz innymi formami cyberprzestępstwa.

Dwuskładnikowa autoryzacja

W przeciwieństwie do standardowej autoryzacji hasłem, 2FA OTP wykorzystuje dwa elementy. Składa się na nią „coś, co użytkownik zna", np. hasło lub kod PIN i „coś co użytkownik ma", zazwyczaj telefon komórkowy lub token. Wykorzystanie tej kombinacji znacznie zwiększa bezpieczeństwo dostępu do danych.





Architektura ESET Secure Authentication jest zaprojektowana tak, aby wykorzystywać tylko dotychczas istniejącą infrastrukturę firmy. Dodatkowo aplikacja ESET Secure Authentication na telefonach służbowych zawiera aplikację serwerową, która idealnie integruje się ze środowiskiem administratora sieci dla MMC i ADUC .

Aplikacja rozwiązuje problem:

- statycznych haseł, które mogą zostać przechwycone
- tworzenia przez użytkowników haseł łatwych do odgadnięcia, nie będących losową kombinacją znaków
- ponownego wykorzystywania haseł dostępu do zasobów firmowych przy logowania się na prywatnych kontach
- haseł składających się z danych użytkownika, np. imię, data urodzenia
- prostych schematów tworzenia nowych haseł, jak np. „piotr1", „piotr2" itp.

Korzyści dla IT:

- łatwa w instalacji (out-of-the-box)
- dostarczanie jednorazowych haseł poprzez aplikację lub wiadomość SMS
- po instalacji aplikacja działa bez dostępu do Internetu
- kompatybilna z większością urządzeń VPN
- wspiera większość systemów na urządzeniach mobilnych
- wsparcie techniczne w języku polskim

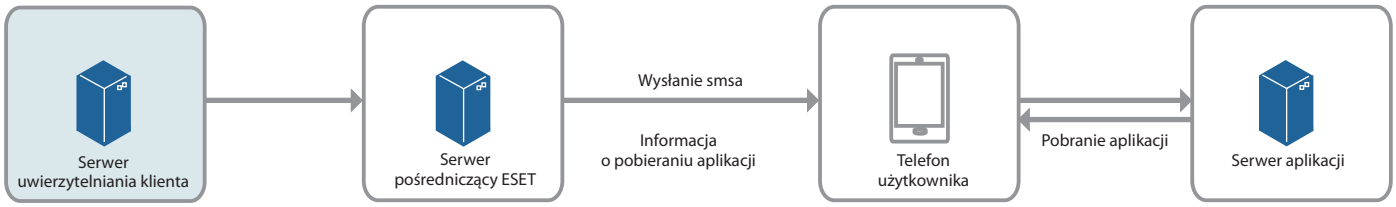
Korzyści dla biznesu:

- pozwala uniknąć włamania, poprzez generowanie unikatowego hasła przy każdej próbie dostępu
- zabezpiecza przed używaniem słabych haseł
- oszczędza koszty – nie wymaga dodatkowego sprzętu
- prosta w instalacji i użytkowaniu
- wsparcie techniczne w języku polskim

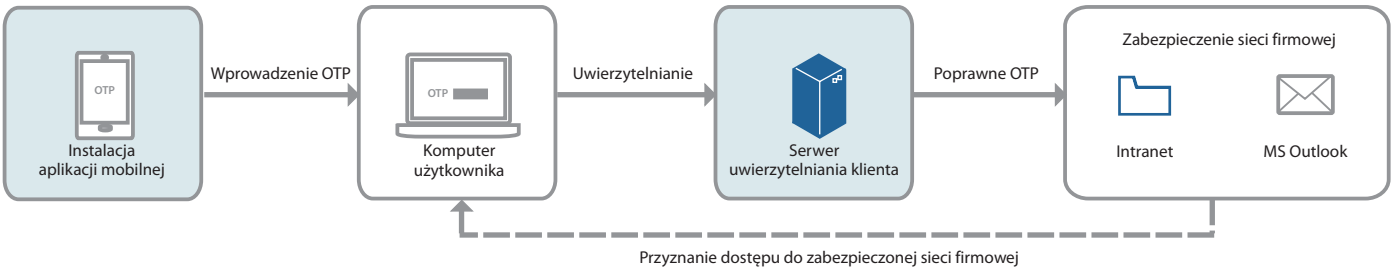
Szczegółowa specyfikacja

Aby zainstalować aplikację ESET Secure Authentication na telefonie komórkowym, jedyne co musisz znać, to numer telefonu pracownika. Aplikacja ESET Secure Authentication wyśle użytkownikowi SMS-a z linkiem aktywacyjnym, którego kliknięcie automatycznie rozpoczyna ściąganie instalatora dla platformy komórkowej. Dostęp do aplikacji jest chroniony kodem PIN, aby zapobiec nieautoryzowanej generacji kodów jednorazowych.

Instalacja i rozpoczęcie korzystania



Komunikacja po stronie klienta



Podsumowanie

Dwuskładnikowa autoryzacja	Dwuskładnikowa autoryzacja z wykorzystaniem jednorazowego hasła dla większego bezpieczeństwa Silniejsza ochrona dla Outlook Web App (OWA), VPN i wszystkich serwisów RADIUS Nie wymaga dodatkowego sprzętu Wygodna do korzystania w telefonie komórkowym
Strona klienta (aplikacja mobilna)	Instalacja jednym kliknięciem, prosty i intuicyjny interfejs Dostarczanie jednorazowych haseł poprzez aplikację lub wiadomość SMS Generowanie hasła niezależnie od połączenia z Internetem Kompatybilna z każdym telefonem komórkowym, posiadającym możliwość wysyłania i odbierania wiadomości SMS Wspiera większość systemów na urządzeniach mobilnych Dostęp do aplikacji chroniony jest kodem PIN, aby zapobiec nadużyciom w przypadku zgubienia lub kradzieży sprzętu
Strona serwera	Łatwe w instalacji (out-of-the-box) Instalator automatycznie rozpoznaje OS i dokonuje wyboru pasujących komponentów
Zdalne zarządzanie	Wspiera MMC Integracja z Active Directory ESET Secure Authentication wzbogacił dodatek ADUC o dodatkowe funkcje, aby ułatwić zarządzanie ustawieniami

WYMAGANIA SYSTEMOWE:
SERWER: Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012 (32-bit & 64-bit)
KLIENT: iOS 4.2 lub wyższy, Android 2.1 lub wyższy, Windows Phone 7 lub nowszy, Windows Mobile 6, BlackBerry 4.3 do 7.1, Symbian J2ME