User Identity Management – sicher und komfortabel

Mit FortiAuthenticator bietet Fortinet eine zentrale Instanz für «User Identity Management». Die als Hardware- und Software-Appliance verfügbare Lösung unterstützt RADIUS, LDAP, 802.1X Wireless Authentication, Certificate Management, Fortinet Single Sign On (SSO) und 2-Faktor-Authentifizierung.

Traditionelle Authentifizierungs- und Autorisierungsmechanismen basieren in der Regel auf der Verwendung von User-Name und Passwort – angesichts des laschen Umgangs mit den persönlichen «Credentials» ein höchst unsicheres Verfahren. Selbst die Verwendung komplexer Passwörter löst das Problem nicht nachhaltig. Sie lassen sich schwer merken, weshalb viele User dieselben Zugangsdaten auf unterschiedlichen Plattformen und Applikationen verwenden. Wird eines dieser Systeme gehackt, sind Angriffe auf die verbleibenden Anwendungen ein Leichtes.

FortiAuthenticator erweitert das Security-Produkte-Portfolio von Fortinet mit einem zentralen «User Identity Management» sowie mit «User Access Control»-Funktionen.

Um eine sichere User-Authentifizierung (Überprüfung der Echtheit der berechtigten Person) und User-Autorisierung (Freigabe von Anwendungen gemäss individuell vergebenen Rechten) zu gewährleisten, sind intelligentere Login-Verfahren notwendig («Strong Authentication»). Dazu stellt Fortinet mit FortiAuthenticator eine wegweisende Plattform zur Verfügung. FortiAuthenticator ist eine zentrale Instanz für jegliche User-Authentication- und -Authorization-Funktionen von FortiGate Firewalls. Dazu gehören beispielsweise IPSEC/SSL-VPN, Administratoren-Zugänge, Captive Portal, Firewall Authentication inkl. Single Sign On (SSO). FortiAuthenticator unterstützt auch Drittsysteme. Diese können über RADIUS oder LDAP angebunden werden. Zudem unterstützt die Lösung Funktionen wie 2-Faktor-Authentifizierung, Identitätsverifikation und 802.1X Wireless Authentication. Dank der Unterstützung von LDAP und RADIUS, der nahtlosen AD-(Active-Directory-) Einbindung sowie der Integration von «Fortinet Single Sign On» in Active Directory stehen umfangreiche Funktionen zur Zugriffskontrolle der Anwender zur Verfügung.

FortiAuthenticator-Highlights – ein Auszug

- Starke Authentifizierung und Autorisierung mittels 2-Faktor-Authentifizierung
- RADIUS- und LDAP-Server
- AD-Synchronisation (LDAP)
- Integration in existierende AD-Infrastrukturen ermöglicht Nutzung identitätsbasierter Regelwerke (Zugriff in Abhängigkeit von Gruppenzugehörigkeiten)
- Integrierte CA (Certificate Authority)
- Unterstützt Hardware- und Software-Token (FortiToken) sowie SMS- und E-Mail-Token
- Fortinet Single Sign On (FSSO) zur Reduktion der Anzahl erforderlicher Logins
- Aufbau von sicheren Wireless-LANs (WPA Enterprise/802.1X)
- Komfortables Gäste-Management mit Funktionen wie zeitlimitierte Zugriffe und Multi-Site-Unterstützung
- Self-Service-Portal
- Erhältlich als Hardware-Appliance oder VM-Lösung
- Einfache Verwaltung über Web-Interface

2-Faktor-Authentifizierung mit unterschiedlichen Token

FortiAuthenticator ermöglicht eine wahlweise Unterstützung von Hardware-, Mobile-, SMS- und E-Mail-OTP-Token, die zeitbasierende Einmalpasswörter (OTP) generieren. Da für die Anmeldung eine Kombination aus Wissen (Zugangsdaten) und Besitz (Token) erforderlich ist, verhindern OTPs den unerlaubten Zugriff auf Netzwerk und Applikationen durch Dritte. Zudem bilden sie aufgrund des nur kurzzeitig gültigen Zugangscodes einen wirksamen Schutz gegen Keylogger und ähnliche Attacken.

FortiToken Mobile

«FortiToken Mobile», eine App-basierende Client-Software von Fortinet, macht Smartphones und Tablets (iOS, Android) zum mobilen OTP-Token bzw. zum persönlichen Authentifizierungs-Device. Die Open-Authentication-(OATH-) konforme Lösung weist gegenüber herkömmlichen Hardware-Token markante Vorteile auf. Dazu gehören das einfache Rollout und die komfortable Aktivierung von Token bzw. Lizenz ebenso wie die Tatsache, dass keine zusätzliche Hardware notwendig ist.

BOLL
IT Security Distribution

BOLL ENGINEERING AG

Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch, www.boll.ch