Gesicherter Zugriff auf Daten und Applikationen

Die «Multi Factor Authentication»-Gesamtlösung von VASCO ermöglicht, den Zugriff auf Daten und Applikationen wirksam zu schützen und zugriffsberechtigte Personen bei deren Anmeldung sicher zu authentisieren. Das «Package» beinhaltet den Authentifizierungsserver IDENTIKEY sowie OTP-Token DIGIPASS.

VASCO unterstützt unterschiedliche Hardware-, Mobile- und SMS-Token, die zeitbasierte Einmalpasswörter (OTP) generieren.

Für den geschützten (Remote-)Zugriff auf Unternehmensdaten und Applikationen reichen einfache Authentifizierungs- und Autorisierungsverfahren (User-Name/Passwort) nicht aus. Gefragt sind vielmehr sogenannte «Strong Authentication»-Verfahren (Zwei-Faktoren-Authentisierung), bei denen die nutzerspezifischen Credentials mit einer zusätzlichen Log-in-Komponente – einem One Time Password (OTP) – ergänzt werden.

Dynamische, zeitbasierte Einmalpasswörter werden auf Knopfdruck durch einen OTP-Token generiert. Sie kommen beispielsweise für den sicheren Zugang ins Firmennetzwerk beziehungsweise für die Freigabe von Anwendungen und Daten gemäss individuell vergebenen Rechten (User-Autorisierung) zum Tragen. Ferner ermöglichen sie die Absicherung von Transaktionen und Datentransfers. OTP-Lösungen dienen zudem der sicheren Überprüfung der Echtheit der berechtigten Person (User-Authentifizierung) und unterstützen somit das Bestreben, unerlaubte Zugriffe durch Dritte zu verhindern.

VASCO unterstützt alle denkbaren Arten von OTP-Token – so auch eine SMS-basierte Variante. Dabei wird das One-Time-Passwort nicht durch einen physischen Token vor Ort, sondern durch einen zentralen Authentisierungsserver generiert und via SMS-Gateway an den jeweiligen User übermittelt. Mit «Digipass for Mobile» stellt VASCO zudem eine app-basierte Authentifizierungslösung zur Verfügung.

Nahtlose Integration

Die enterprisetaugliche Authentifizierungslösung von VASCO lässt sich einfach und schnell in bestehende Umgebungen und Applikationen einbinden. Dazu stellt der Authentifizierungsserver «IDENTIKEY» komfortable «Plug and play»-Funktionalitäten zur Verfügung und unterstützt sowohl Radius- als auch Web- und SOAP-Schnittstellen. Ob als Virtual- oder Hardware-Appliance – beide Varianten ermöglichen ein zentralisiertes, komfortables User-Management. So steht dem Administrator eine einheitliche Konsole für Funktionen wie Benutzerverwaltung, Token-Management, Auditing und Reports zur Verfügung.

Komplettlösung für die starke Authentisierung

Die leistungsfähige «Strong Authentication»-Gesamtlösung von VASCO verknüpft «User Identity Management» und «User Access Control»-Funktionen zu einem wirksamen Ganzen und adressiert Anwendungsbereiche wie Windows-Logon, Remote-Zugriffe via VPN, sichere Einbindung mobiler Devices, Absicherung von Webanwendungen und Schutz von Cloud-Services. Sie besteht aus der Server-Software IDENTIKEY sowie aus den Client-Komponenten DIGIPASS.

IDENTIKEY

- Authentifizierungsserver für die Netzwerk- und Anwendungssicherheit mit Einmal-Passwörtern und digitaler Signatur
- Skalierbar – geeignet für Kleinstanwendungen bis hin zu Grossinstallationen
- Unterstützung unterschiedlichster Plattformen (Windows- und Linux-Server, virtualisierte Umgebungen)
- Nahtlose AD-(Active-Directory-) Einbindung sowie LDAP- und RADIUS-Unterstützung
- Inkl. Funktionen wie Primary-Backup und Replica-Server, Webfilter, Windows Desktop- und Netzwerk-Logon, SOAP, SBR etc.
- Mandantenfähig

DIGIPASS

- Hardware-, Mobile- und auf SMS-basierende Token
- Unterstützte Authentifizierungstechnologien: One-Time-Passwörter (OTP), starke statische Passwörter (SSP) – gespeichert auf Digipass Smart Card oder Digipass Token
- Public Key Infrastructure (PKI) für Signaturen und Verschlüsselung

BOLL
IT Security Distribution

BOLL ENGINEERING AG

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