



Enterprise Single Sign-On

Sicherheit erhöhen, Kosten senken

Studien belegen, dass Benutzer fast immer einfach zu merkende Passwörter verwenden. Diese Passwörter stellen ein hohes Sicherheitsrisiko dar, und das Handling verursacht hohe Kosten. Enterprise Single Sign-On spart Zeit, verbessert die Sicherheit und verringert die Help-Desk-Anfragen. Mit einer einzigen Authentisierung erhält ein Anwender automatisch Zugriff auf mehrere Anwendungen.

Auch unternehmensweit eingeführte Passwort-Restriktionen bieten keine ausreichende Sicherheit. Passwörter bleiben ein Sicherheitsrisiko, weil Benutzer sich schwer zu merkende Passwörter oft notieren (müssen). Diese findet man an Monitore oder Schreibische geheftet wieder. Studien von führenden Analysten gehen davon aus, dass mehr als 60% aller Anrufe im Help Desk auf Passwortprobleme zurückzuführen sind. Ein erheblicher Kostenfaktor, welcher sich mit einem Single Sign-On Service massgeblich reduzieren lässt. Besonders mit Blick auf die Total Cost-of-Ownership ist dieser Punkt nicht zu unterschätzen.

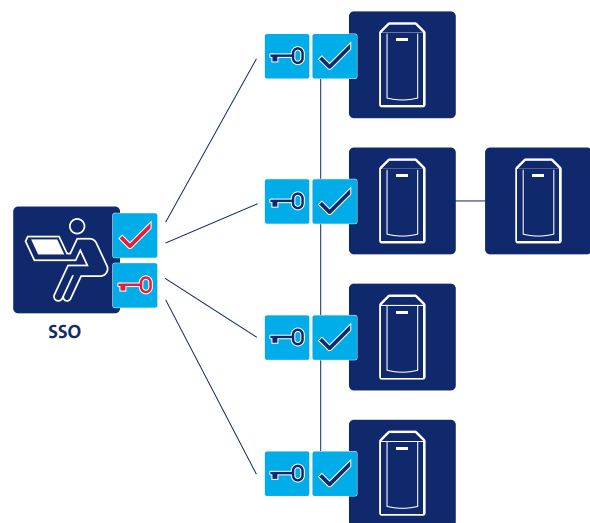
Lösung

In diesem Umfeld gewinnt das Konzept des Single Sign-On (SSO) an Bedeutung. Single Sign-On hilft den Mitarbeitenden unmittelbar: Sie authentisieren sich nur noch einmal und erhalten dann automatisch Zugang zu allen Anwendungen und Systemen, für die sie autorisiert sind. Neben hoher Benutzerakzeptanz steigt auch die Produktivität und Effizienz der Mitarbeitenden. Gleichzeitig nehmen die Help-Desk-Anfragen wegen Passwortproblemen beträchtlich ab. Die damit verbundenen Kosteneinsparungen ermöglichen einen Return on Investment in kurzer Zeit.

Angesichts der Vielfalt an Applikationen erleichtert unser SSO Service einem Benutzer die Anmeldung massiv: Er muss sich gegenüber dem System nur einmal selber authentisieren. Die Anwender müssen sich nicht mehr um das Generieren neuer Passwörter kümmern. Unser SSO automatisiert diese Aufgabe und stellt sicher, dass die vorgegebenen Passwort-Policies der einzelnen Applikationen eingehalten werden. Bei Bedarf generiert SSO für Applikationen im Hintergrund täglich neue starke Passwörter. Die Anwender merken davon nichts

und müssen sich nicht mehr mit dieser lästigen Aufgabe konfrontieren. Damit erreichen Sie ein Höchstmass an Sicherheit im Bereich der Passwörter.

Da die Anwender mit einer einzigen Anmeldung Zugang zu sämtlichen autorisierten Applikationen erhalten, sollte die primäre Authentisierung möglichst mehrere Faktoren beinhalten: Je nach Kundenbedürfnis lassen sich diverse starke Authentisierverfahren integrieren und kombinieren (beispielsweise Biometrie, Smart Cards, OTP etc.).



Einmalige Authentisierung durch User



Automatische Authentisierung durch SSO

Ausprägung

Enterprise Single Sign-On:
Betrieb, Wartung und Support
des Enterprise Single Sign-On Service

Option

Advanced Authentication:
Betrieb, Wartung und Support von
Advanced Authentication (Zusatzmodul
zur Integration von starker Authentisierung)

Ähnliche Services / Komplementäre Services

- Authentication, Authorization and Accounting
- Device Control
- Information Rights Management
- Secure E-Mail
- Workplace Antivirus

Leistungsmerkmale

- Single Sign-On für hunderte von Anwendungen wie Windows-, Web-, Java-Applikationen und Terminal-Emulatoren
- Unterstützung für erweiterte Authentisierung
- Automatisierte Passwortänderungen und -generierung nach klar definierbaren Regelwerken
- Richtlinienbasiertes Sperren von Arbeitsstationen, Schliessen von Anwendungen und Abmelden von Benutzern
- Möglichkeit zur Anbindung von starken Authentisierungsmethoden

Nutzen

- Massiv erhöhte Passwortsicherheit und Risikoreduktion
- Help-Desk-Anrufe wegen Passwortproblemen nehmen markant ab, und die damit verbundenen Kosten sinken signifikant
- Schnellere und einfachere Anmeldungen gewährleisten höhere Produktivität
- Hohe Benutzerakzeptanz und -freundlichkeit
- Gewünschter Sicherheitslevel ist vom Kunden wählbar (herkömmliche und starke Authentisierung)