Single Sign-On

Einmal anmelden, alles nutzen

Mit einem Single Sign-On (SSO) müssen sich Mitarbeiter nur noch einmal anmelden (primär authentifizieren) und das SSO übernimmt das Anmeldeverfahren bei eingebundenen Applikationen nach hinterlegten Regeln. Dies erspart den Usern nicht nur Tipparbeit, sondern auch die lästige Suche nach Passwörtern. Darüber hinaus lässt sich die Sicherheit durch Verschärfung der Passwortregeln erhöhen und die Anmeldung z.B. mit einer Smartcard oder einem Biometrie-Verfahren kombinieren.

Bei der Gesamt-Abmeldung “Single Log-Out” (SLO) kann sich der Benutzer durch einmaliges “Ausloggen” aus allen genutzten Diensten und Applikationen abmelden. So kann niemand den Account missbrauchen, wenn der Anwender z.B. seinen Arbeitsplatz verlässt.
Mit Ergänzungen wie Passwort-Synchronisation, Web-SSO oder Enterprise-SSO lässt sich das vereinfachte und sichere Anmeldeverfahren auf alle Applikationen ausdehnen.
Das “Simplified Sign-On” ist dagegen ein weniger komfortables und nicht besonders sicheres Verfahren. Es vereinfacht die Anmeldung an mehreren Systemen mit den gleichen Anmeldeinformationen durch den Abgleich der Systeme (Synchronisation von login-name und Passwort untereinander).

Der Nutzen von SSO

- Zugriff auf alle angebundenen Dienste und Anwendungen ohne erneute Anmeldung.
- Zeitersparnis durch Wegfall von Log-In’s (evtl. verbunden mit Suche nach Passwort).
- Weniger Helpdeskanfragen wegen vergessener Passwörter, da sich der Anwender weniger Passwörter merken muss. Und weniger Anfragen bedeuten geringere Auwände.
- Sicherheitssteigerung durch Wegfall der Merkzettel und durch die Ermöglichung strengerer Passwortrichtlinien.
- Besserer Nutzerkomfort und somit höhere Zufriedenheit.

Stolpersteine beim SSO

- Nicht alle SSO Systeme unterstützen den gleichen Umfang an Applikationen und Systemen. Es ist sorgfältig zu prüfen, ob wirklich sämtliche Applikationen (z.B. Unix Applikationen im x-Window, web Applikationen, Applikationen mit kerberos Unterstützung, Apps, etc.) vollständig von allen SSO Funktionen unterstützt werden. Dazu zählen nicht nur der Anmeldevorgang sondern auch der automatische Passwort-Reset und der automatische zyklische Tausch der Passwörter im Hintergrund.
- Oft wird das SSO nur für eine Auswahl an Applikationen umgesetzt, weil sich die Technik-Komplexität der vielfältigen Systeme (AD, LINUX, HOST, SAP, Mobile-Devices, web-Applikationen, gehostete Systeme) und deren Vielzahl kaum beherrschen lässt.
- Die Wenigsten konzipieren das SSO als Zwei-Faktor Authentifizierung zusammen mit Smartcard, Biometrie oder anderen Verfahren. Das ist aber ratsam, da bei SSO das Passwort extrem potent ist (möglicher Komplettzugang!) und ein Ausspähen fatale Folgen hätte.
- Viele übersehen, dass die meisten SSO Produkte keine Managementkomponente besitzten (“Wer darf SSO nutzen?”, “Welche Applikationen darf ein User nutzen?”, etc.), hier hilft eine IdM Provisionierung weiter.
- Oft werden wesentliche Aspekte des Passwortspeichers übersehen: Ist der Passwortspeicher

verschlüsselt? Wo ist er abgelegt? Ist er auch offline verfügbar? Wie wird er synchronisert?
Werden Directories als Repository unterstützt?