Hybrid Identity Services.

Viele Cloud- und Applikationsanbieter verwalten die Benutzerkonten selbst. Für Unternehmen bringt das wesentliche Nachteile. Jeder User benötigt ein eigenes Passwort für den jeweiligen Dienst. Das Unternehmen kann nicht effizient kontrollieren, welche Mitarbeiter welche Dienste nutzen. Hybrid Identity setzt hier an und trennt die User-Verwaltung von der Applikation.

Mehr Sicherheit in der Dienste-Verwaltung

Was ist Hybrid Identity?

Hybrid Identity verlagert die Kontenverwaltung zurück ins Unternehmen. Hybrid Identity Services basieren auf zwei Lösungsansätzen, die die Komplexität von Anmeldeoptionen vereinfachen:

- **Sicherer Fernzugriff**
- **Single-Sign On für Cloud- und Web-Applikationen**

Die Applikation wird dabei strikt von der der Anmeldeverwaltung und den Anmeldedaten getrennt, sodass die Verwaltung der Benutzer sicher im Unternehmen bleibt. Die Applikation wird extern als Web-Applikation oder Cloud Service betrieben.

Sie profitieren von einer zentralen Anmeldeverwaltung für alle im Betrieb verwendeten Applikationen. Datenmissbrauch, Shadow IT durch die Verwendung unbekannter Dienste sowie der Verwaltungsaufwand bei internen Veränderungen oder dem Verlassen des Unternehmens durch den Mitarbeiter, können sicher und effizient vermieden werden.

Wie funktioniert Hybrid Identity?

Hybrid Identity besteht aus zwei getrennten Ebenen. Ebene 1 ist das Unternehmen, das die Benutzerkonten verwaltet. Ebene 2 ist der Anbieter der Applikation, der die Anmeldungen aus dem Netzwerk des Unternehmens akzeptiert.

Beide Ebenen tauschen für den Anmeldeprozess und die Zugriffssteuerung Security Tokens aus. Bei der Anmeldung erhält der Benutzer einen Token, der seine Identität bestätigt und weitere Informationen enthält, beispielsweise Gruppenmitgliedschaften oder Abteilungszugehörigkeiten. Diese Informationen werden dementsprechend ausschließlich aus dem Unternehmen über einen sicheren Kanal abgefragt und an den Anbieter verschlüsselt weitergegeben.

Single Sign On

Hybrid Identity Services beinhalten die Einrichtung von Single Sign On mit ADFS und AD Connect:

- Die Synchronisierung von lokalen AD-Informationen mit Azure AD (in der Cloud) mithilfe von AAD Connect, einschließlich Benutzer, deren Kennwörter, Gruppen- und Verteilerlistenzugehörigkeit
- Verwaltung der Zugriffe zu Anwendungen, Diensten und Daten mithilfe von statischen und dynamischen (auf Kriterien basierten) Self-Service-Gruppen.
- Wahlweise ausfallsicher, durch Implementation einer HA-Lösung.
- Zusätzliche Verbesserung der Verfügbarkeit durch teilweises Auslagern der Dienste in die Cloud
- Die Lösung kann auch vollständig in der Cloud betrieben werden (auf Basis IaaS).

Ihr Nutzen

- User können mit einem einzigen Anmeldekonto auf verschiedene Dienste zugreifen
- Die Benutzer müssen sich nicht mehrere Kontendaten merken
- Single Sign On für unterstützte Applikationen
- Fern- und Anwendungszugriff werden sicherer
- Verbesserte Benutzerproduktivität
- Kein Datenverlust beim Austritt eines Mitarbeiters
- Automatische Skalierbarkeit als IaaS in der Cloud
- 7x24x365 Betrieb Out-of-the-Box
- Ausfallsicher und immer verfügbar

Sie möchten mehr über unsere Lösungen erfahren? Dann wenden Sie sich bitte an:

microsoft@acp.at