Markus Steiner setzt sich seit über 15 Jahren mit dem Thema IAM auseinander. Als Senior IAM Architekt und berät er Firmen, Verwaltungen und Schulen bei der Umsetzung von IAM Projekten.

Systemintegration mit IAM Lösung midPoint zu SWITCH, AHVN13/ZAS & Co.

midPoint ist zurzeit das umfassendste Open Source Identity und Access Management System (IAM). Es bietet eine ausgereifte Compliance & Governance konforme Identitäts- und Berechtigungsverwaltung. Der Beitrag zeigt anhand von Beispielen unterschiedliche Systemintegrationen auf.

Identity und Access Management Systeme wie midPoint automatisieren die Verwaltung von digitalen Identitäten sowie die dazugehörigen Accounts und deren Berechtigungen in den Zielsystemen.

IAM System der Oberklasse

midPoint der Firma Evolveum agiert dabei wie ein Datenhub, der kontinuierlich Quellsysteme liest wie z.B. Mitarbeiterdaten aus einem HR-System. Sobald sich Informationen ändern, werden diese basierend auf definierten Policies (Regeln) verarbeitet und in die Zielsysteme propagiert. So können z.B. AD Accounts und/oder AD-Gruppenzugehörigkeiten in Zielsystemen automatisiert verwaltet werden. Zu diesem Zweck liest midPoint auch kontinuierlich die Benutzerkonten und deren Berechtigungen in den Zielsystemen. Einerseits wird somit geprüft, ob die erforderlichen Berechtigungen (Soll-Zustand) einer Identität tatsächlich vorhanden sind. Andererseits, ob die Identität nicht über zu viele Berechtigungen verfügt, weil z.B. ein Administrator einem Benutzeraccount im Zielsystem erweiterte Berechtigungen zugewiesen hat. Somit ist midPoint in der Lage, zu jedem Zeitpunkt die tatsächlich vergebenen Benutzerberechtigungen wiederzugeben und basierend auf definierten Policies bei Abweichungen reagieren zu können.

> Erwähnenswert ist, dass sich auch die EU-Kommission für midPoint entschieden hat und somit ein weiterer starker Treiber für die Weiterentwicklungen ist.

Neben weiteren IAM Funktionalitäten wie Genehmigungs- und Überprüfungsprozessen von Benutzerberechtigungen erfüllt midPoint alle wesentlichen Compliance-Anforderungen hinsichtlich Prozessvorgaben, Transparenz und Nachvollziehbarkeit.

Schlüsselfaktor Systemintegration

Der Integration der Zielsysteme kommt eine zentrale Bedeutung bei, da erst dadurch das Potential eines IAMs ausgeschöpft wird. midPoint bietet deshalb eine Vielzahl von Out-of-the-box Konnektoren an wie DatabaseTable/JDBC, CSV, LDAP, AD, UNIX/Linux, GoogleApps, SCIM, Webservice (REST). Eine Vielzahl dieser Konnektoren wird von Evolveum entwickelt und unterhalten. Andere hingegen werden von der «Community» oder weiteren Firmen bereitgestellt.

IAM Integration in der öffentlichen Verwaltung und im Bildungswesen

Im Umfeld der öffentlichen Verwaltung ist somit ein automatisierter Abgleich der AHVN13 mit dem ZAS gegeben, um eine effiziente Verwaltung von Identitäten bzw. Benutzer zu ermöglichen. Im Bereich der Hochschulen spielt die bestehende Integration zu SWITCH eine analog wichtige Bedeutung. Daneben bringt auch die Systemintegration zu Polyright riesige Vorteile in den Bereichen Studentenkarte, Zutrittskontrolle und bargeldloses Bezahlen. Hier leistet die Firma ITConcepts einen wichtigen Beitrag, indem sie den SWITCH- und den Polyright-Konnektor unterhält.

Laufende Weiterentwicklung

Die Liste der Konnektoren und verfügbaren Systemintegrationen ist laufend am Wachsen. So verfolgt ITConcepts mit Interesse das Pilotprojekt edulog, das ein Pendant zu SWITCH im Bereich der kantonalen Schulen ist.
Ein weiterer Konnektor, der laufend an Bedeutung gewinnt, ist der Microsoft Graph API Connector. Dieser ermöglicht die erweiterte Systemintegration zu Azure und Office365, womit die Benutzerberechtigungsverwaltung z.B. für Exchange und Microsoft Teams über midPoint möglich wird. Hier ist ITConcepts daran, diesen laufend weiterzuentwickeln.
Erwähnenswert ist, dass sich auch die EU-Kommission für midPoint entschieden hat und somit ein weiterer starker Treiber für die Weiterentwicklung ist.

Authentifizierung, SSO und MFA

Bei der Entwicklung von midPoint wurde der Fokus bewusst auf das Management von Identitäten und Zugangsberechtigung (Authorization) gelegt. Für die Abdeckung der Anforderungen hinsichtlich Authentification, Single-Sign-On und Multi-Factor-Authentification können weitere Produkte nach Wahl eingesetzt werden, sofern diese die gängigen Protokolle unterstützen.
Abschliessend lässt sich sagen, dass midPoint auch hinsichtlich Systemintegration mit den kommerziellen Produkten problemlos mithalten kann und weiterhin eine rasante Entwicklung durchläuft.