NMX *flow*
smart. reliable. adaptive.

Von dezentraler Verwaltung zur *zentralen Identitätsplattform*

Wie ein Unternehmen durch NMX*flow* alle Benutzerverwaltungs-Prozesse automatisieren kann

Ausgangslage

Ein Unternehmen nutzt eine zentrale HR-Stammdatenverwaltung, in welcher alle Identitäten erstellt und gepflegt werden.

Die Herausforderung: Die IT-Infrastruktur ist hybrid aufgebaut. Lokales Active Directory, Entra ID und hybride Accounts müssen verwaltet werden, während Datenablagen und Exchange-Umgebungen sowohl vor Ort als auch in Microsoft 365 laufen. Dazu kommt Tresorit für den sicheren Datenaustausch mit externen Partnern.

Bei dieser Vielzahl an Systemen müssen alle Accounts, Rollen und Berechtigungen, die von den HR-Stammdaten abgeleitet werden, über die verschiedenen Umgebungen hinweg konsistent gehalten werden – eine komplexe Aufgabe ohne zentrale Orchestrierung.

Zielsetzung

NMX*flow* für zentrales Identity und Access Management

Die klare Vision: Eine digitale Identität als Single Source of Truth, die im HR-System erstellt, bewirtschaftet und beim Austritt vollständig entfernt wird – mit allen verknüpften Accounts und Rollen in sämtlichen angeschlossenen Systemen.

Konkret sollte NMX*flow* folgende Ziele ermöglichen:

Eine zentrale digitale Identität

Im HR-System erstellt (join), bewirtschaftet (move) und deaktiviert oder gelöscht (leave). Alle benötigten Accounts und Rollen für die Authentifizierung und Autorisierung in den verschiedenen Systemen – ob vor Ort oder in der Cloud – sollen immer mit dieser Identität verknüpft sein.

Governance sicherstellen

Namenskonventionen und Sicherheitsrichtlinien sollen für alle Rollen konsequent umgesetzt werden.

Komplette Digitalisierung der Account-Workflows

Inklusive sicherer Bereitstellung von initialen Anmeldedaten.

Microsoft Teams vollständig automatisieren

Automatisierte Erstellung, Verwaltung und Archivierung von Teams basierend auf Departementen und Abteilungen, plus Self-Service Portal für projektbasierte Teams mit Start- und Enddatum.

Bestehende Accounts verknüpfen

Die bereits vorhandenen Accounts in den verschiedenen Systemen sollen initial mit den korrekten Identitäts-Records verbunden werden.

Microsoft Self-Service integrieren

Access Packages und Self Service Password Reset nahtlos einbinden.

Bidirektionale Synchronisation

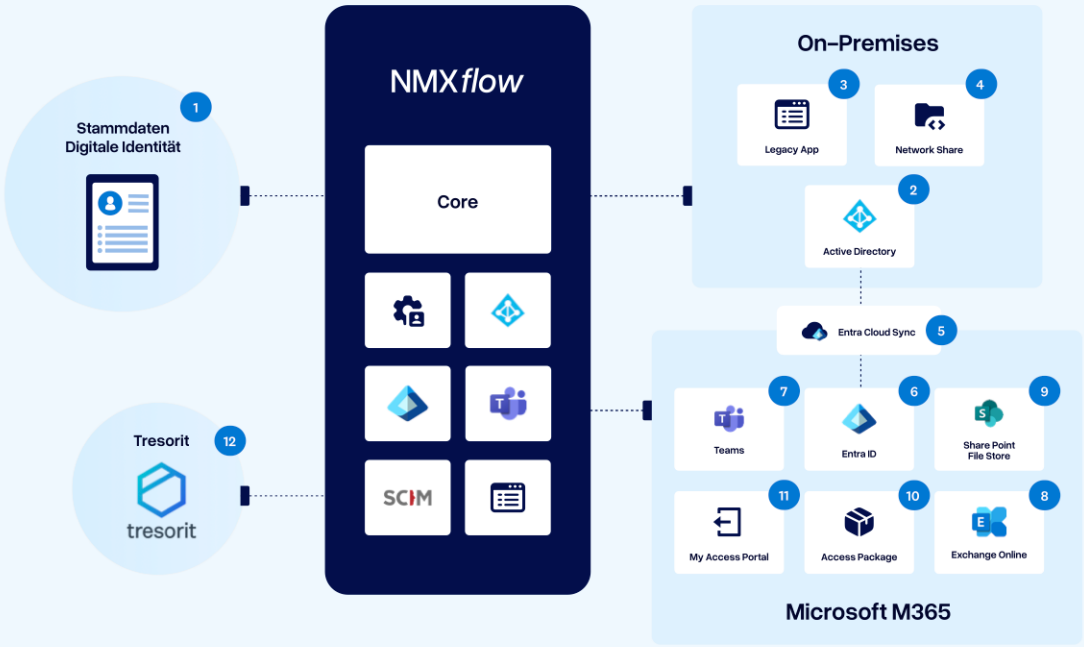
Attribute aus den Systemen sollen zurück in die HR-Stammdaten geschrieben werden können.

Umsetzung

NMX*flow* als zentrale Synchronisationsdrehscheibe

NMX*flow* wird als zentrale Synchronisationsdrehscheibe implementiert und orchestriert nun sämtliche Identity- und Access-Management-Prozesse:

- **Matchingtabelle und Konfiguration:**
  Zunächst wird eine Matchingtabelle erstellt, die definiert, welche Attribute aus den HR-Stammdaten in welches Attribut beim jeweiligen Objekt im entsprechenden Zielsystem übertragen werden. Diese Zuordnungen werden anschliessend in den jeweiligen Sync-Modulen konfiguriert.
- **Anbindung der HR-Stammdatenverwaltung:**
  Die HR-Stammdatenverwaltung oder die Stammdatenverwaltung aus dem Schulinformationssystem wird mittels REST-API and NMX*flow* angebunden.
- **Anbindung der Zielsysteme:**
  Die verschiedenen Zielsysteme werden je nach System über REST-API, SCIM, kundenspezifische Schnittstellen oder andere Technologien angebunden.
- **Access Packages für Self-Service:**
  Diverse Access Packages werden erstellt und konfiguriert. Mit diesen können berechtigte Entra Accounts sich selbständig weitere Rollen und Ressourcenzugriffe zuweisen — wahlweise ohne oder mit zusätzlichen Admin-Genehmigungen. Die Zuweisung der Access Packages erfolgt über Entra ID-Gruppen, die durch NMX*flow* bewirtschaftet werden.



1. **Stammdaten:** Alle für die Ziel-System relevanten Attribute müssen bei der «Digital Identity» (Stammdaten) erstellt und gepflegt werden.

2. **AD Accounts & Gruppen:** Erstellen, bearbeiten oder entfernen von AD-Accounts, Gruppen und Gruppenmitgliedschaften.

3. **On-Premises Ressourcen:** Basierend auf AD-Gruppenmitgliedschaften kann der Zugriff auf AD-integrierte Ressourcen wie z.B. ein Netzwerk-Share gesteuert werden.

4. **Optional: Accounts & Gruppen für eine Applikation:** Erstellen, bearbeiten oder entfernen von Accounts, Gruppen und Gruppenmitgliedschaften in einer on-Premises Applikation/System mit einer eigenen Benutzerdatenbank.

5. **Microsoft Entra Cloud Sync:** Der Service synchronisiert Accounts inkl. dem dazugehörigen Password-Hash, Gruppen und deren Mitgliedschaften vom AD in das Entra ID. Aus dem Entra ID kann der Password-Hash und Entra ID Security Gruppen in das AD synchronisiert werden.

6. **Entra ID Accounts & Gruppen:** Erstellen, bearbeiten oder entfernen von Entra ID Accounts, Gruppen und Gruppenmitgliedschaften.

7. **Microsoft Teams:** Automatische Erstellung von MS Teams und Kanälen inkl. den dazugehörigen Owners und Members.

8. **Teams Self-Service Portal:** Teams Self-Service Portal für die Erstellung von einzelnen Teams/Channels inkl. Governance (Naming, Lifecycle, etc.)

9. **M365 Ressourcen:** Basierend auf Entra ID Gruppenmitgliedschaften kann der Zugriff auf M365 Ressourcen wie z.B. die Datenablage in einer SharePoint Site gesteuert werden.

10. **Microsoft Access Packages:** Im Kunden M365 Tenant werden die benötigten Access Packages erstellt und für eine oder mehrere Entra ID Gruppen freigegeben. Diese Gruppenmitgliedschaften werden via NMX*flow* verwaltet.
Die Access Packages verweisen dann auf die Ressourcen (Cloud und onPrem) auf welche der Benutzer Zugriff erhalten soll.

11. **User MS Portal «myaccess»:** Der Benutzer sieht seine verfügbaren Access Packages via myaccess.microsoft.com und kann sich diese entsprechend zuweisen bzw. anfordern (Approval notwendig).

12. **Tresorit:** Erstellen, bearbeiten oder entfernen von berechtigten Entra ID Accounts in die Tresorit Benutzerdatenbank für den Zugriff auf Tresorit Services (Datenablagen, Passwort Tresor, etc.)

Das Ergebnis

Zentrale Identitätsverwaltung mit kompletten Lifecycles
Durch NMX*flow* als zentrale Synchronisationsdrehscheibe werden nun alle digitalen Identitäten vom HR-System aus gesteuert. Der komplette Lifecycle – vom Eintritt über Änderungen bis zum Austritt – wird automatisch in alle angebundenen Systeme übertragen.

Konsistente Governance über alle Systeme
Die Matchingtabelle stellt sicher, dass Namenskonventionen und Sicherheitsrichtlinien einheitlich in allen Zielsystemen umgesetzt werden. Jede Identität ist mit allen benötigten Accounts und Rollen verknüpft.

Automatisierte Workflows und Self-Service
Account-Erstellung, Microsoft Teams-Verwaltung und die Bereitstellung von Zugriffsrechten laufen nun vollautomatisch ab. Über Access Packages können berechtigte Mitarbeitende sich selbständig weitere Rollen und Ressourcen zuweisen.

Nahtlose Integration in die hybride Infrastruktur
Alle Systeme – ob vor Ort oder in der Cloud – sind über REST-API, SCIM und weitere Schnittstellen angebunden und werden kontinuierlich synchronisiert. Die bidirektionale Synchronisation ermöglicht zudem das Zurückschreiben von Attributen in die HR-Stammdaten.

Jetzt anfragen

info@nmxflow.ch
+41 62 558 48 88
www.nmxflow.ch

Created by Netree AG