COGNITUM Software

go:Identity

Die Identity Management Appliance

Out-of-the-Box Benutzerverwaltung - Leicht, sicher und effektiv

Das Problem

Kleine und mittlere Unternehmen stehen vor den ähnlichen Herausforderungen wie große Unternehmen.

Kleine und mittelständische Unternehmen werden aufgrund schmaler IT-Budgets oftmals an der Implementierung von benötigten Identity und Access Management Lösungen gehindert. Dabei werden diese Organisationen vor ähnliche Herausforderungen gestellt wie große Unternehmen.

Ohne eine enge HR-Integration, um Mitarbeiter- und Organisationsdaten zu synchronisieren, und ohne ein automatisiertes Berechtigungsmanagement besteht die Gefahr der Richtlinien- und Vorgabenverletzung.

Die Herausforderung

Anforderungen von Geschäftsführung, Datenschutz und Revision

IT-Prozesse

Wie werden Standardprozesse kostengünstig und ohne hohen Aufwand automatisiert?

- Einstellungen / Wechsel / Ausscheiden von Mitarbeitern
- Self Service / Helpdesk
- Berechtigungen / Passwörter

Sicherheit

- Wie werden Zugriffsberechtigungen auf Notwendigkeit geprüft und die Nachweisbarkeit für die Revision sichergestellt?
- Wer hat welche Zugänge und Rechte? Sind sie notwendig?
- Wer hat diese genehmigt?
- Werden nicht (mehr) benötigte Rechte automatisch entzogen?

Qualität

- Wie kann eine hohe Qualität der Daten und Services sichergestellt werden?
- Wie können fehlerträchtige und zeitaufwändige manuelle Prozessschritte ersetzt werden?
- Wie werden Medienbrüche beseitigt bzw. verhindert?
- Wie wird eine hohe Datenqualität trotz unterschiedlichster Dateneigentümer und Systeme erreicht?

Die Lösung

Eine vollständige, zentralisierte Identity Management Lösung

go:Identity ist eine vollständige, zentralisierte Identity Management Lösung „Out-of-the-Box“ für kleinere und mittlere Unternehmensgrößen. **go:Identity** verwaltet Identitäten, Rollen, Benutzerkonten und deren Berechtigungen in beliebigen Zielsystemen.

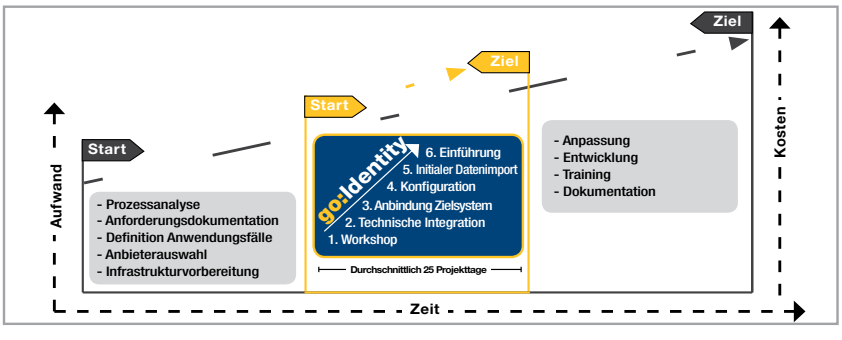
go:Identity ist in wesentlich kürzerer Zeit als andere verfügbare traditionelle Identity und Access Management Lösungen einsatzbereit. Dabei sind diverse Funktionalitäten inklusive z.B. Benutzerprovisionierung und -deprovisionierung, Benutzer Self Serivces und Genehmigungs-Workflows, um nur einige zu nennen.

Die Vorteile

Leicht, sicher und effektiv

Reduzierung des Arbeitsaufwandes

- Automatisierung vieler Aufgaben und manueller Tätigkeiten
- Verbesserung der Sicherheit
- Kontrolle über Zugriffe und Berechtigungen
- Aussagekräftige Daten für Ihre Berichte
- Sicherstellung der Datenintegrität
- Reduzierung der Fehlerquote
- Standardisierung der Datenqualität: Kurze Implementierungsdauer durch Appliance-Ansatz
- **go:Identity** ist eine vorkonfigurierte, standardisierte Lösung.



Hauptfunktionen

Automatisierter HR-Datenimport

HR-Daten sollten vollständig, aktuell und über alle Systeme konsistent sein, um Unternehmensanforderungen zu unterstützen und Sicherheitsrisiken zu minimieren.

go:Identity stellt für den Import von HR-Daten eine Schnittstelle bereit, die automatisiert die regelmäßige Aufbereitung Ihrer Daten durchführt:

- Erstellung von neuen Identitäten
- Generierung von eindeutigen User-IDs und E-Mail-Adressen etc.
- Aktualisierung von bestehenden Identitäten
- Deaktivierung bzw. Löschung von ausgeschiedenen Mitarbeitern, die in den HR-Daten nicht mehr vorhanden oder aktiv sind

Verwaltung von externen Identitäten

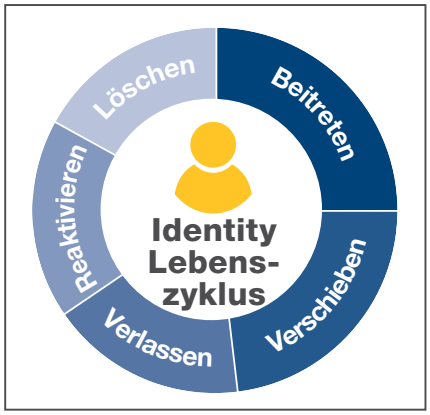
Externe Mitarbeiter, befristete Mitarbeiter oder technische Identitäten für die IT haben oft kein Personalkonto und gelangen daher nicht zwangsläufig über den HR-Datenimport in das System.

go:Identity bietet die Funktionen Anlage, Pflege und Löschung externer Identitäten, um die Sicherheit der Daten zu verbessern und Compliance-Anforderungen gerecht zu werden.

- Die Anlage externer Identitäten wird durch Genehmigungsprozesse abgesichert
- Externe Identitäten erhalten Berechtigungen durch strukturierte Genehmigungsprozesse
- Nicht mehr benötigte Berechtigungen werden am Stichtag automatisch entzogen

Selbstregistrierung von Benutzern

Sollte die Verwaltung von externen Identitäten (bspw. Kunden, Partnern, Interessenten, Studenten etc.) benötigt sein, bietet go:Identity eine optionale Selbstregistrierungsschnittstelle. Damit werden auch Consumer Identity und Access Management (CIAM) Szenarien unterstützt. Kombiniert mit optionalem Web Single Sign-on werden Zugriffe auf Web-Portallösungen und weitere Onlineangebote des Unternehmens kontrolliert.



User Lifecycle Management

go:Identity bietet die Funktion der Automatisierung des kompletten Lebenszyklus von Identitäten. Vom Zeitpunkt des Eintritts eines Mitarbeiters bis zu seinem Verlassen der Firma können Änderungsprozesse automatisiert abgearbeitet werden.

Automatisierte & manuelle Funktionen:

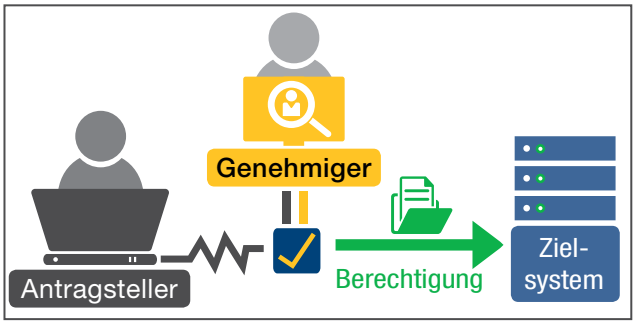
- Erstellen von Identitäten - automatisch aus HR-Daten oder manuell als externe Identitäten
- Ändern von Identitätsdaten - automatisch durch geänderte HR-Daten oder manuell für externe Identitäten
- Deaktivieren von Identitäten samt ihrer Berechtigungen - automatisch am Stichtag
- Löschen von Identitäten - automatisch nach Zeitraum X, wenn gewünscht

Provisionierung von Benutzerkonten und Berechtigungen

Eine manuelle Provisionierung von Berechtigungen in Zielsysteme dauert oft lange, teilweise mehrere Tage. Des Weiteren ist es schwierig nachzuvollziehen, ob die Berechtigungen erteilt bzw. entzogen worden sind.

go:Identity verbindet sich mit einer Vielzahl von gängigen Systemen wie Active Directory, LDAP, Lotus Notes, SAP, Datenbanken, Mainframe u.v.m., um die Erstellung von Benutzerkonten und die Verwaltung von Berechtigungen zu automatisieren:

- Zentrale Verwaltung von Benutzerkonten
- Zentrale Verwaltung von Passwörtern
- Synchronisation von Eigenschaften
- Zentrale Verwaltung von Berechtigungen
- Zentral kontrolliertes Sperren und Löschen von Benutzerkonten



Reporting und Auditing

go:Identity bietet die Datenbasis zur Erstellung eines aussagekräftigen Reportings.

Die Auditdaten in **go:Identity** erlauben einen schnellen Überblick und liefern notwendige Informationen über die Einhaltung von Compliance-Vorgaben. Folgende können beantwortet werden:

- Welche Berechtigungen hat ein Mitarbeiter wann erhalten bzw. verloren?
- Wer hat was wann genehmigt?
- Welche Daten von Identitäten wurden geändert?

Zusätzlich können auch eigene Berichtsvorlagen konfiguriert werden.

Workflowportal für Prozesse und Rezertifizierungen

Die in **go:Identity** vorhandenen Genehmigungsprozesse für Berechtigungen und weitere Funktionsprozesse wie das Pflegen von externen Identitäten und das Einrichten von Vertretungen werden in einem sogenannten Workflowportal zur Verfügung gestellt.

Im Workflowportal wird auch die zyklische Bestätigung Ihrer Mitarbeiter gestartet. Durch diese regelmäßigen Attestierungen wird sichergestellt, dass nur identifizierte und bestätigte Personen Zugang zu Systemen behalten oder entzogen bekommen.

Die Funktionsprozesse im Überblick:

- Genehmigungsprozesse für Rollen
- Bearbeitung von externen Identitäten
- Zyklische Bestätigung von Identitäten, Rollen und Organisationseinheiten innerhalb festgelegter Zeiträume

Richtlinien und Compliance

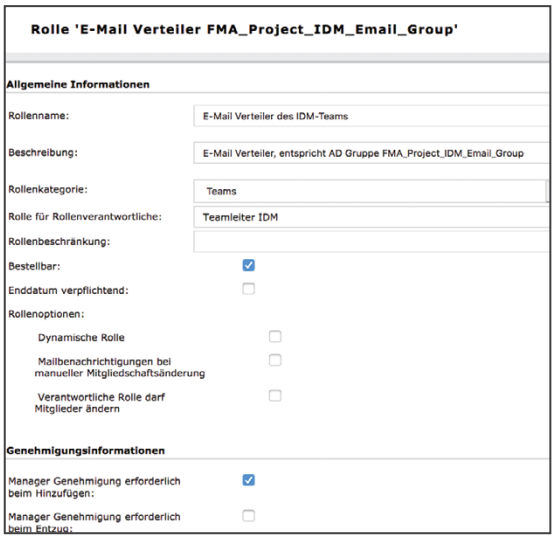
Identitätsdaten werden immer strikter reguliert (bspw. DSGVO, SOX, ISO27001 etc.) und die Notwendigkeit diesen Regularien zu entsprechen wächst. Hinzu kommt, dass Mitarbeiter und Kunden in zunehmendem Maße den sensiblen Umgang mit persönlichen Daten lernen und einfordern.

go:Identity unterstützt die gängigen Regelwerke und wird diese Unterstützung weiter ausbauen.

Admin-Oberfläche für Rollenbearbeitung

Rollen sind in **go:Identity** das zentrale Instrument zur Steuerung und Verteilung von Berechtigungen. Abhängig von der Zielsetzung kann der Administrator verschiedene Rollen über die Admin-Benutzeroberfläche anlegen. Dabei kann die Rolle entweder in einer echten Berechtigung auf einem Zielsystem enden oder zu einer Gruppierung von Identitäten führen. Die Admin-Benutzeroberfläche ermöglicht die Pflege der Rollen und die dynamische Steuerung der Genehmigungsprozesse und Benachrichtigungen pro Rolle:

- Rollenname, Kategorisierung und Beschreibung
- Ist die Rolle bestellbar und ist eine Befristung vorgeschrieben?
- Ist die Genehmigung des Vorgesetzten notwendig?
- Muss eine andere Gruppe von Personen noch zustimmen?
- Wer ist der Rollenverantwortliche? Muss dieser zustimmen?
- Wer soll am Ende eines Genehmigungsprozesses über das Ergebnis benachrichtigt werden?



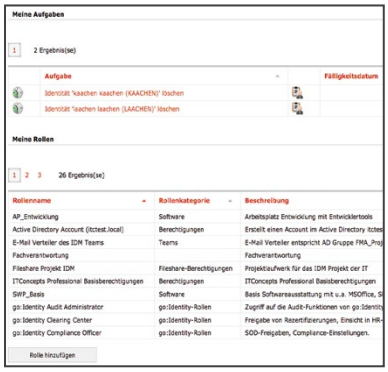
Rollen können zur Verwaltung und Verantwortlichkeit den fachlichen Eigentümern oder Systemverantwortlichen zugeordnet werden. Dadurch wird der Arbeitsaufwand der IT verringert und die Verantwortlichkeit der Zugriffsberechtigungen den Fachbereichen als Dateneigentümern übertragen.

Zentrales Dashboard für die Mitarbeiter

Im Mitarbeiterportal, dem sogenannten Dashboard, können Mitarbeiter eigene Berechtigungen und Rollen einsehen und benötigte weitere Berechtigungen selbst beantragen. Durch diesen „Self Service“ erreichen die Anwender einen hohen Automatisierungsgrad, der IT-Abteilungen enorm entlasten kann. Entscheidungen für die automatisierte Berechtigungserteilung (sogenannte Genehmigungen) werden durch Prozesse in die Fachabteilungen verlagert - genau dorthin, wo sie hingehören. Zusätzlich erhalten die Anwender die Möglichkeit, sich über den Stand von Prozessen zu ihrer Person zu informieren und an Prozessen teilzunehmen.

Weitere Self-Service-Funktionen:

- Änderung und Rücksetzung von Passwörtern
- Telefonbuchfunktion
- Vertretungen pflegen
- Eigene Daten einsehen



Organisationseinheiten und Vorgesetzte

go:Identity bietet ein Modul zum Verwalten von hierarchischen Organisationseinheiten und Verantwortlichen oder Managern. Diese Organisationseinheiten bieten auch die Möglichkeit, Standardberechtigungen zuzuweisen, die innerhalb des Organisationsbaums vererbt werden können.

Technische Details

Unterstützte Sprachen

- Mehrsprachigkeit der Benutzeroberfläche (DE, EN, + weitere Sprachen bei Bedarf)

Anbindung von Zielsystemen

- Anbindungen von Standardsystemen, bspw. Microsoft Active Directory, MS Exchange, MS SharePoint und LDAP sind bereits enthalten
- Weitere Module sind verfügbar für:
  - SaaS, bspw. Microsoft Azure und Office365, SalesForce.com etc.
  - Unternehmensapplikationen, basierend auf SAP, etc.
  - Datenbankapplikationen, bspw. Oracle, MSSQL, MySQL und PostgreSQL
  - Linux und Unix
- Weitere Systeme sind über das flexible Connector Framework integrierbar

Spezifikationen

- Bereitstellung der Lösung als Hardware oder virtuelle Maschine (VM)
- Vorkonfiguriertes System - keine aufwändigen Installationen erforderlich
- Vordefinierte Workflows und Genehmigungsprozesse - Einsatz von praxiserprobten Prozessen von Beginn an, Anpassungen sind möglich
- Integration und Inbetriebnahme in Ihrer Umgebung
- Flexible Bindung - Vertrag jederzeit zum Ende der Laufzeit kündbar

go:Identity

Profitieren Sie von den Vorteilen einer automatisierten Lösung

- ✓ **go:fast** – Verbesserte Produktivität
- ✓ **go:cost-effective** – Kosteneinsparungen
- ✓ **go:secure** – Revisionssicher und transparent
- ✓ **go:easy** – Kontrolle der Berechtigungsvergabe

COGNITUM Software

go:Identity

COGNITUM Software bündelt langjährige Identity und Access Governance Expertise für die Entwicklung von Standardsoftware.

Identity & Access Governance ist eine Kernkomponente im Aufbau einer sicheren IT-Infrastruktur. Mit unserer umfangreichen Praxiserfahrung aus der Beratung, Implementierung und unserem Know-how für Identity und Access Governance Lösungen haben wir unsere Produkte entwickelt, die schnell und kostensparend für jedes Unternehmen – unabhängig von der Branche und Größe – einsetzbar sind. COGNITUM Software gehört zur ITConcepts Unternehmensgruppe, einem weltweit operierenden IT-Dienstleister und Systemintegrator.

COGNITUM Software GmbH
In den Dauen 6, 53117 Bonn, Deutschland • Tel.: +49 228 9087330 • E-Mail: goidentity@cognitum-software.com • Web: cognitum-software.com