COGNITUM Software

go:Identity

Die Identity Management Appliance

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

Das Problem

Eine sichere IT-Infrastruktur ist ohne anwendungsübergreifendes Berechtigungsmanagement nicht möglich

Identity und Access Management (IAM) Lösungen bieten automatisiertes Berechtigungsmanagement und eine enge HR-Integration, um Mitarbeiter- und Organisationsdaten zu synchronisieren.

Unternehmen werden jedoch aufgrund schmaler IT-Budgets und fehlender Zeit oftmals an der Implementierung von IAM-Lösungen gehindert. Damit riskieren sie die Anforderungen von Geschäftsführung, Datenschutz und Revision nicht zu erreichen.

Der Wunsch

Maximale Arbeitserleichterung und Sicherheit innerhalb kurzer Zeit

- Den Aufwand in der Administration von AD, Azure AD, LDAP, SAP, SharePoint, ERP, CRM, etc. verringern
- Regelmäßige Re-Zertifizierungen für die User- und Rollenberechtigungen durchführen (für Wirtschaftsprüfer)
- Anwendungen in die Cloud migrieren (Exchange/Lotus Notes nach Office 365, SharePoint, etc.)
- File-Share-Berechtigungen und VPN-Zugänge einfach verwalten
- Anträge für die IT-Rechtevergabe in ein Self Service Web Frontend mit nachfolgenden Genehmigungsworkflows verlagern
- Die IT-Administration von stupiden und fehleranfälligen Aufgaben entlasten
- Eine einzige Authentifizierung für alle Anwendungen des Users (SSO + Federation)
- Detaillierte Reports über „Wer hat wann, ab wann, bis wann... die Berechtigung gehabt/erteilt/entzogen“
- Verbesserung der IT-Security

Die Lösung

Eine schnell einsatzbereite Identity Management Lösung

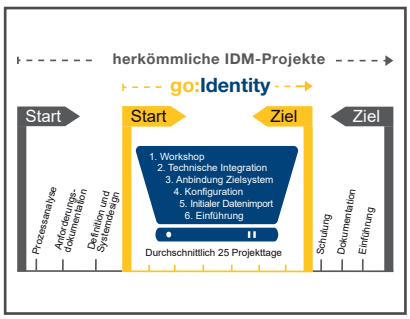
go:Identity ist eine vollständige, zentralisierte Identity Management Lösung „Out-of-the-Box“ für alle Unternehmensgrößen. **go:Identity** verwaltet Identitäten, Rollen, Benutzerkonten und deren Berechtigungen in beliebigen Zielsystemen.

go:Identity ist im Durchschnitt aller Projekte in 25 Projekttagen produktiv. Diverse Funktionalitäten wie z.B. Benutzerprovisionierung und -deprovisionierung, Benutzer-Self-Services und Genehmigungs-Workflows sind bereits integriert.

Die Vorteile

Leicht, sicher und effektiv...

- Automatisierung vieler Aufgaben und manueller Tätigkeiten
- Verbesserung der Sicherheit
- Kontrolle über Zugriffe und Berechtigungen
- Aussagekräftige Daten für Berichte
- Sicherstellung der Datenintegrität
- Reduzierung der Fehlerquote
- Standardisierung der Datenqualität
- Kurze Implementierungszeit durch Appliance-Ansatz



... bei geringem Projekt-Risiko

Durch den „Out-of-the-Box“ Ansatz reduziert sich in unseren Projekten das Projekt-Risiko erheblich. Denn dank der eingebauten „Best-Practice“ haben die Prozesse und Funktionen bereits ihre Tauglichkeit bewiesen.

Hauptfunktionen

User Lifecycle Management

go:**Identity** automatisiert den kompletten Lebenszyklus von Identitäten. Vom Zeitpunkt des Eintritts eines Mitarbeiters bis zu seinem Verlassen des Unternehmens können Änderungsprozesse automatisiert abgearbeitet werden.

Automatisierte & manuelle Funktionen:

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

HR-Daten Einbindung

Daten zu Personen (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 flexible Schnittstellen bereit, die automatisiert die regelmäßige Aufbereitung Ihrer Daten durchführen:

- Erstellung neuer Identitäten
- Generierung eindeutiger User-IDs und E-Mail-Adressen
- Aktualisierung bestehender Identitäten
- Deaktivierung bzw. Löschung ausgeschiedener Mitarbeiter, die in den HR-Daten nicht mehr vorhanden oder aktiv sind

Verwaltung sonstiger Identitäten

Externe und befristete Mitarbeiter oder technische Identitäten für die IT, kurz „externe Identitäten" genannt, haben oft kein Personalkonto. Sie sind häufig nur sehr eingeschränkt unter Kontrolle und in automatisierte Prozesse eingebunden.

Mit go:**Identity** lassen sich externe Identitäten leicht anlegen, pflegen und löschen. Damit wird die Sicherheit der Daten verbessert und Compliance-Anforderungen erfüllt.

- 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

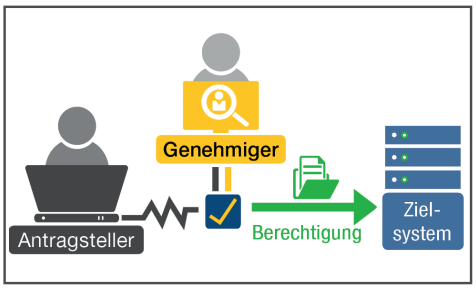
Für die Verwaltung von externen Identitäten wie Kunden, Partnern, Interessenten oder Studenten, bietet go:**Identity** eine optionale Selbstregistrierungsschnittstelle. Damit werden auch Consumer Identity und Access Management (CIAM) Szenarien unterstützt. Kombiniert mit optionalem Web Single Sign-on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

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, Azure AD, LDAP, Exchange, Lotus Notes, SAP, Datenbanken u.v.m., um die Erstellung von Benutzerkonten und die Verwaltung von Berechtigungen zu automatisieren:

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



Anzeige und Analyse von Berechtigungen auf Fileshare Ordner

go:**Identity** zeigt alle Fileshare Berechtigungen einer Identität bzw. alle Zugriffsrechte auf einen bestimmten Fileshare Ordner an. Dazu werden die NTFS-Berechtigungen mit den tatsächlichen Mitgliedschaften in AD-Gruppen in Beziehung gebracht. Es werden so auch ungewollt vergebene Berechtigungen sichtbar.
Alle Informationen an zentraler Stelle: in der zentralen Berechtigung-Sicht Ihrer Identitäten. Gefährliche Ausnahmen können entlarvt und mehr Transparenz und Sicherheit in die Zugriffsverwaltung auf Fileshares gebracht werden.

Reporting und Auditing

go:**Identity** bietet die Datenbasis zur Erstellung eines aussagekräftigen Reportings. Zusätzlich können auch eigene Berichtsvorlagen konfiguriert werden.

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

Folgende Fragen können direkt online beantwortet werden:

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

Workflowportal für Prozesse und Attestierungen

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

Im Workflowportal werden auch die zyklischen Bestätigungen von Mitarbeitern, Berechtigungen und z.B. Organisationseinheiten bearbeitet. Durch diese Attestierungen wird sichergestellt, dass alle Benutzer, vergebenen Berechtigungen und Objekte regelmäßig auf ihre Gültigkeit überprüft werden und ggf. entsprechend behandelt werden.

Die Funktionsprozesse im Überblick:

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

Richtlinien und Compliance

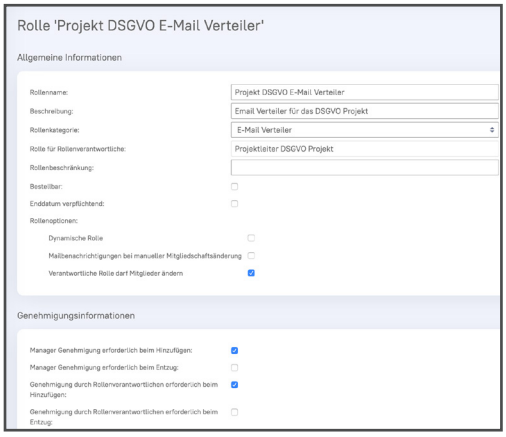
Identitätsdaten werden immer strikter reguliert (bspw. DSGVO, SOX, ISO27001) und die Notwendigkeit diesen Regularien zu entsprechen wächst. Hinzu kommt, dass Mitarbeiter und Kunden in zunehmendem Maße den sensiblen Umgang mit persönlichen Daten lernen und einfordern.

go:Identity unterstützt die gängigen Regelwerke und stellt benötigte Funktionen bereit.

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?

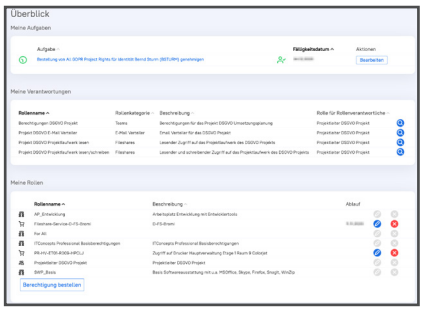


Rollen können zur Verwaltung und Verantwortlichkeit den fachlichen Eigentümern oder Systemverantwortlichen zugeordnet werden. Dadurch werden diese in die Umsetzung eingebunden und der Arbeitsaufwand der IT verringert. Die Verantwortung für die Zugriffsberechtigungen wird den Fachbereichen als Dateneigentümern 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
- Vertretungen pflegen
- Eigene Daten einsehen/bearbeiten



Organisationseinheiten und Vorgesetzte, Projekte, Standorte und mehr

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

Technische Details

Benutzeroberfläche

- Browser-basierte Oberfläche zur einfachen Nutzung von „Überall“
- Mehrsprachigkeit (DE, EN, FR, + weitere Sprachen bei Bedarf)
- Anpassbares Design (zur Adaption an Ihr CI)

Anbindung von Zielsystemen

- Anbindungen von Standardsystemen, z.B. Microsoft Active Directory, Azure AD, Exchange, SharePoint, SAP, LDAP
- Weitere Module sind verfügbar für z.B.:
  - Notes
  - Datenbankapplikationen, bspw. Oracle, MSSQL, MySQL und PostgreSQL
  - Linux und Unix
  - und viele mehr
- Kundenspezifische oder andere Systeme sind über das flexible Connector Framework integrierbar

Spezifikationen

- Bereitstellung der Lösung als 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

Die standardisierte Benutzerverwaltung Out-of-the-Box

- ✓ **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 ist aus der ITConcepts Unternehmensgruppe hervorgegangen, einem weltweit operierendem IT-Dienstleister und Systemintegrator.

COGNITUM Software Team GmbH
Leitschweg 2c, 38448 Wolfsburg, Deutschland • Tel.: +49 5361 8349527 • E-Mail: info@cognitum-software.com • Web: www.cognitum-software.com