Identity Processes:

Identity Management

Prozessorientiert einführen

Whitepaper

Oktober 2008

Inhalt

Abbildungen

1. Management Summary

Unternehmen sind darauf angewiesen, alle an den Geschäftsprozessen beteiligten Mitarbeitern zweifelsfrei zu identifizieren und mit den notwendigen Zugangsrechten in den jeweiligen IT Systemen auszustatten. Die Unternehmen müssen steuern auf welche Unternehmensressourcen welche Personen mit welchen Rechten und zu welchem Zeitpunkt zugreifen dürfen. Diese Aufgaben sind keineswegs trivial. Mitarbeiter und externe Geschäftspartner genießen unterschiedliche Privilegien auf gespeicherte Daten und Anwendungen. Privilegien, die bedingt durch Wachstum oder Umorganisation Ihres Unternehmens, ständigen Änderungen ausgesetzt sind. Mit zunehmender Mitarbeiteranzahl steigt auch die Komplexität der Benutzerverwaltung. Selbst kleinere Unternehmen ab einigen Hundert Mitarbeitern benötigen deshalb ein schnelles und sicheres Identity Management, um Zugriffsrechte zuverlässig zu erteilen und zu verwalten. Für große Unternehmen ist ein solches Werkzeug unerlässlich.

Doch Zugangsrechte müssen nicht nur richtig vergeben werden, sie müssen auch jederzeit sofort entziehbar sein, sei es aufgrund eines organisatorischen Wechsels oder des Austritts eines Mitarbeiters. Daher ist eine Betrachtung der Berechtigungsvergabe immer im Kontext der Vergabe- und Entziehungsprozesse notwendig. Zudem leitet sich die Berechtigung eines jeden Nutzers in den meisten Fällen aus dessen betrieblicher Funktion, seinem Arbeitsplatz, ab.

So können die meisten Zugangsrechte aus der Kombination organisatorische Zuordnung und Fachrolle (z. B. „Vertrieb Inland“ und „Vertriebsleiter“) vergeben werden. Lediglich einige wenige Berechtigungen wie Fileshares und E-Mail-Account werden abhängig von der Person vergeben.

In einer heterogenen Systemlandschaft sind in der Regel die Informationen der Identitäten durch die lokalen Benutzerverwaltungen in jedem der Systeme verteilt abgespeichert. Können Sie die Fragen:

- „Welcher Mitarbeiter hat in welchen Systemen welche Zugangsrechte?“,
- „Seit wann hat der Mitarbeiter diese Zugangsrechte?“,
- „Wer hat ihm diese Zugangsrechte zugewiesen?“,
- „Wie lange dauert die Vergabe der Zugangsrechte?“ und
- „Welche Kosten entstehen dadurch?“

beantworten? Sie könnten es, nachdem sie eine Identity Managementlösung eingeführt haben. Ohne eine solche Lösung sind die Informationen nur mit viel Mühe durchzuführen und verursachen, bedingt durch sehr viel manuelle Arbeit, noch erhebliche Kosten.

Auch die nachweisbare Einhaltung gesetzlicher Vorschriften ist unter diesen Bedingungen eine komplexe Aufgabe. Sollen die Compliance Anforderungen permanent und unternehmensweit

durchsetzbar sein, müssen alle Benutzerverwaltungen in den einzelnen Systemen im Unternehmen konsistent gehalten werden. Des Weiteren müssen die Zugangsrechte der Identitäten für alle Systeme plattformunabhängig und zentral aktualisierbar sein. Dies ist nur mit einem umfassenden Identity Management System möglich, das Zugriffe sicher kontrolliert und Zugangsrechte automatisiert vergibt.

IBSolution unterstützt Sie bei der Einführung solch einer IdM Lösung und bündelt sein Beratungs-Know-How unter dem Begriff **Identity Processes (IdP)**. Unsere Kunden erhalten in Form von 3 Pakten zu fixen Preisen die folgenden Lösungen:

- Zentrale und systemübergreifende Benutzerverwaltung
- Regeln von Zugangsrechten jedes einzelnen Benutzers auf der Grundlage von Rollen innerhalb der Organisation
- Leistungsstarke Datensynchronisierungs- und Self-Service-Schnittstellen
- Protokollierung-, Auditing-, Monitoring- sowie Reporting-Funktionalitäten
- Erstellen von unternehmensspezifischen Identity Lifecycle Prozesse
- Integration in die bestehende IT-Systemlandschaft

Das IdP-Team der IBSolution GmbH ist Ihr strategischer Partner bei der Implementierung dieses leistungsfähigen und effizienten Werkzeuges und unterstützt Sie dabei gerne, damit Ihr Unternehmen zukünftig sämtliche Anforderungen in Bezug auf Identity Management erfüllen kann.

Weitere Informationen und einen Überblick über die verschiedenen Komponenten, den Aufbau und die Vorteile des Lösungsansatzes finden Sie in den folgenden Kapiteln.

2. Die Welt ohne IdM

Unternehmen betreiben heute eine Vielzahl von IT-Systemen. So hat selbst ein mittelständisches Unternehmen, das ausschließlich SAP-Systeme im ERP Umfeld einsetzt, mehr als 3 SAP Systeme zu verwalten, die die unterschiedlichsten Anforderungen abdecken. Bei Großkonzernen kann die Systemanzahl aber auch mehr als 100 Systeme betragen. Dazu kommen unzählige Datenbankanwendungen, Mailprogramme und Zugriffe auf externe Ressourcen, die ebenfalls verwaltet werden müssen. Die Umsetzung der Identity Management Maßnahmen ist aufgrund der unterschiedlichen Systeme für eine effiziente und stringente Administration die größte Herausforderung. Jedes der Systeme verwaltet selbstständig seine Benutzerkonten, um so den Mitarbeitern Zugriffsrechte auf Datenbanken, Verzeichnisdienste und Anwendungen zu gewähren. Somit müssen die Benutzer in mehreren Systemen administriert werden. In jedem dieser Systeme legen Administratoren Benutzerkonten an, weisen Gruppen Rechte zu und pflegen Gruppenmitgliedschaften. Aber nicht nur die Administration dieser Konten kostet die Unternehmen viel Zeit und Geld, auch die Kontrolle der jeweils vergebenen Rechte ist sehr kostspielig. So erwarten die Wirtschaftsprüfer jedes Jahr einen Nachweis, dass in den Finanzsystemen alle User mit den „richtigen“ Rechten ausgestattet waren. Nur so kann aus Sicht des Gesetzgebers wirtschaftlicher Missbrauch vermieden werden.

Die hohe Anzahl und die fehlende Integration der Systeme untereinander führen zu einer dezentralen und manuellen Benutzerverwaltung. Bei der Neuanlage von Mitarbeitern muss der IT-Administrator diese Accountdaten in jedem System immer wieder neu eingeben. Bei einer Änderung oder Löschung (oder bei so einfachen Dingen wie Heirat) sind erneut alle Systeme einzeln durchzuarbeiten. Auch durch die nicht zeitnahe Einführung neuer Sicherheitseinstellungen können hohe Aufwände entstehen, in dem jeder User einzeln angepasst werden muss. Weiterhin wird durch das Einholen von Genehmigungen und der Rücksprachen mit den Vorgesetzten, um die Zugangsrechte einzurichten, sehr viel Zeit benötigt. Dieser Administrationsmarathon wird mit jedem neu angeschafften System umfangreicher und komplexer. Je mehr Systeme es gibt, desto größer sind auch der Aufwand der Datenpflege und die dadurch entstehende Gefahr von fehlenden oder fehlerhaften Eingaben, die wiederum zu inkonsistenten Daten führen können.

Dies hat zur Folge, dass die Datenqualität sinkt und letzten endlich auch die Sicherheit darunter leidet. Der Zeitaufwand zum Anlegen eines neuen Users beträgt laut der Anwenderstudie „Identity Management 2006/2007“ des Fraunhofer-Instituts für Informations- und Datenverarbeitung (IITB) durchschnittlich 3,55 Stunden bei Unternehmen ohne Identity Management (IdM). Nach Angaben von Oracle benötigt ein Mitarbeiter gewöhnlich 16 Minuten pro Tag mit dem Einloggen über verschiedene Passwörter. Des Weiteren ist bei 45 Prozent aller Helpdesk Anrufe der Grund ein Passwort-Reset, Experten schätzen, dass jede dieser Anfragen das Unternehmen zwischen 25 und 40 Euro kostet.

Dies führt zu einer Steigerung der IT-Kosten und kann dennoch einen sicheren Systembetrieb nicht gewährleisten.

Viele Unternehmen verfügen heute noch immer nicht über standardisierte Prozesse zur Beantragung bzw. den Entzug von Zugangsrechten, was sich als weiteres Problem darstellt. Zugangsrechte werden oft auf Zuruf gewährt. Was dazu führt, dass Benutzer nicht in allen Anwendungen gleich Zugriff erhalten. Es werden zu viele oder zu wenige Zugriffsrechte vergeben. Die verzögerte Bereitstellung von Zugriffsrechten führt zu einer eingeschränkten Produktivität des Mitarbeiters. Darüber hinaus werden Organisationsmöglichkeiten verschiedenster Rechte meist so vielfältig abgebildet wie die Unternehmensstruktur selbst. Ein regelrechter „Wildwuchs“ entsteht durch fehlende Standards in der IT-Welt und vor allem durch fehlende Standards in den Unternehmen.

Werden Berechtigungsvergaben nicht dokumentiert, gibt es keine Transparenz und Nachvollziehbarkeit, um festzustellen, wer wann wem welche Zugangsrechte erteilt hat. Oftmals sind es die Auszubildenden des Unternehmens die im Zuge ihrer Ausbildung eine Abteilung nach der anderen durchlaufen und immer wieder neue Zugangsrechte zugewiesen bekommen, aber es gibt niemanden der ihnen diese wieder entzieht. Aufgrund eines nicht vorhandenen Reportings, ist auch die Anzahl an Benutzerleichen, die Lizenzkosten verursachen, schwer nachzuprüfen.

Die vielen Benutzerzugänge nehmen nicht nur sehr viel Zeit der IT-Abteilung und der Mitarbeiter in Anspruch, sondern stellen zu dem ein hohes Sicherheitsrisiko für das Unternehmen dar. Mitarbeiter müssen sich innerhalb ihrer täglichen Arbeit eine Vielzahl an Benutzernamen und Passwörtern merken und neigen daher oft dazu sich diese zu notieren. Nach einer Befragung von Ernst & Young sehen Unternehmen neben Computerviren die größte Bedrohung in den eigenen Mitarbeitern. 43% von insgesamt 543 befragten Führungskräfte gaben an, dass ausgeschiedene Mitarbeiter in ihrem Unternehmen weiterhin Zugang zu vertraulichen Informationen hatten, weil ihnen die Zugriffsrechte nicht schnell genug oder versehentlich gar nicht entzogen worden waren. Durch diese unzureichenden Sicherheitsmaßnahmen kann sowohl Datenmissbrauch als auch –diebstahl einen immensen Schaden anrichten. Laut einem Identity Management Experten[1] sind 57% der unberechtigten Zugriffe auf Mitarbeiter und 21% auf ehemalige Mitarbeiter zurückzuführen.

Dass die Erwartungen an Unternehmen in Bezug auf Sicherheit und Datenschutz immer weiter steigen, zeigen nicht nur die in den beiden Studien festgestellten Missstände. Die Vielzahl von verabschiedeten, nationalen und internationalen Gesetzen und Richtlinien in den letzten Jahren stellen zusätzliche Anforderungen dar, die erfüllt werden müssen. Einer der Gründe hierfür ist, dass inzwischen auch das Management für die Einhaltung der immer strenger werdenden gesetzlichen

[1] Michael Richter ist Autor des Buches „Identity Management – Integration der Benutzerverwaltung in einer heterogenen Systemlandschaft“.

Regelungen und Bestimmungen zum Schutz der Privatsphäre sowie Nachvollziehbarkeit der Datenmanipulation und der Bedrohung durch Identitätendiebstahl, haftbar gemacht werden kann. Diese Forderungen und festgelegten Regelungen veranlassen Unternehmen dazu, die Sicherheit ihrer Systeme ständig zu verbessern. Das Risikomanagement beinhaltet auch immer das IT-Risiko-Management. Daher muss die Vergabe und Änderung von Zugriffsrechten revisionssicher dokumentiert sein und der Risikoanalyse zur Verfügung stehen.

Die genannten Missstände gilt es durch die Einführung eines Identity Management Systems zu beseitigen. Es bietet richtliniengesteuerte Komponenten zur Automatisierung von routinemäßigen Sicherheits- und Ressourcenmanagementaufgaben. Durch die Automatisierung und Richtlinienintegration lassen sich Ihre geschäftlichen Richtlinien zuverlässig und konsistent durchsetzen.

3. Identity Management

Identity Management befasst sich mit der zentralen und automatisierten Benutzer- und Berechtigungsverwaltung von Identitäten (Attribute einzelner Mitarbeiter wie Personalnummer, Vorname, Nachname, etc.) über ihren Lebenszyklus hinweg. Weiterhin unterstützt ein Identity Management System das Unternehmen u. a. bei der automatischen Verknüpfung von User-IDs, Zugangsrechten, IT-Ressourcen und ist die ausführende Instanz bei der Umsetzung und Sicherstellung der entsprechenden Regelwerke. Darüber hinaus stellt es für ausgewählte Benutzer Self-Services bereit. Das Ziel liegt damit in der generellen Optimierung des im Folgenden genauer betrachtenden Identity Lifecycles hinsichtlich Produktivität, Qualität, Sicherheit und Nachvollziehbarkeit in einer komplexer werdenden IT-Infrastruktur.

Identity Lifecycle

Der Lebenszyklus einer Identität eines Mitarbeiters setzt sich aus mehreren Phasen zusammen. Zu Beginn des Lebenszyklus, in der Phase der Erstellung, wird die digitale Identität definiert. Dazu wird der Nutzer identifiziert und registriert. Die Art der Identifizierung und Registrierung hängt vom Einsatzzweck und Grad der Verbindlichkeiten ab, die mit der digitalen Identität verbunden sein soll. Dies wird beim Eintritt eines neuen Mitarbeiters in das Unternehmen festgelegt. Anschließend wird die digitale Identität im System angelegt.

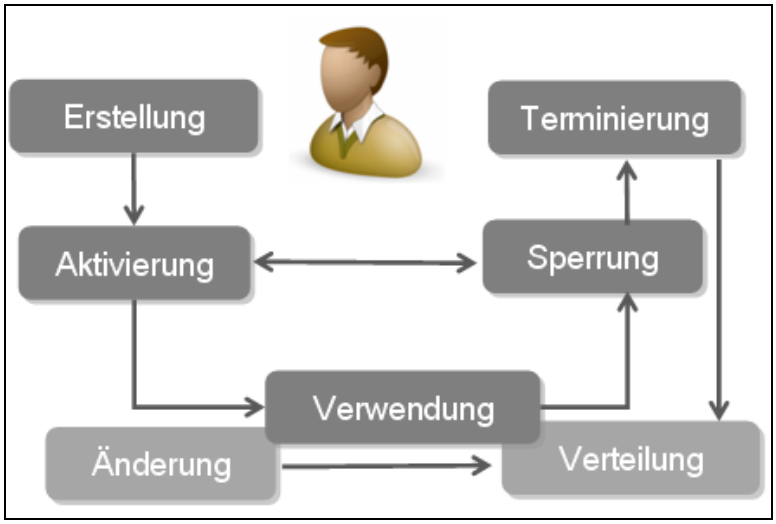

Abbildung 1: Identity Lifecycle

Bis zur eigentlichen Vergabe an den Mitarbeiter bleibt die Identität noch inaktiv. Der Mitarbeiter erhält am Tag des Eintritts in das Unternehmen seine Nutzerkennung und es werden Authentifizierungsmerkmale festgelegt. Ebenfalls werden die neuen User in der Nacht vor dem Eintritt in den Systemen automatisch angelegt und freigeschaltet. Dies kann erstmalig zum Zeitpunkt des Arbeitsbeginns oder nach einer Beurlaubung geschehen. Während der Lebensdauer der Identität

finden Änderungen an den Attributen statt. Diese können technische Gründe haben, indem ein Update eines bestehenden Systems durchgeführt wird und sich daraufhin die spezifischen Attribute ändern oder durch die Einführung eines ganz neuen Systems im Unternehmen. Betriebswirtschaftliche Gründe können sein, dass bspw. ein Abteilungswechsel oder eine Beförderung des Mitarbeiters vollzogen wurde und somit Zugangsrechte entzogen und Neue zugeteilt werden. Nachdem die Identität aktualisiert wurde, kann wieder eine automatische Verteilung der Daten erfolgen.

Im Falle des Verlustes oder Verdachts auf Missbrauch der Identität wird ein Verfahren benötigt, um den Zugang zu sperren. Auch eine Beurlaubung, Krankheit oder zeitlich begrenzte Versetzung kann eine solche Sperrung erforderlich machen. In bestimmten Fällen ist auch das Reaktivieren der digitalen Identität sinnvoll (z. B. bei der Rückkehr des Mitarbeiters in seine ursprüngliche Funktion). Die letzte Phase einer Identität in ihrem Lebenszyklus ist die Terminierung. Dies ist dann der Fall, wenn die Geschäftsbeziehung zwischen Unternehmen und Mitarbeiter endet. Häufig wird die Sperrung der irreversiblen Terminierung vorgezogen, um den Zugang zu historischen Daten zu bewahren.

4. Gesetzliche Anforderungen

Compliance bedeutet die Einhaltung und Umsetzung von gesetzlichen Bestimmungen und Regularien. An diese gesetzlichen Richtlinien, Vorschriften und Verhaltensregeln ist jedes Unternehmen gebunden. Es ist definiert, wie der Umgang mit elektronischen Daten stattfinden muss, wer Zugriff darauf hat und wie die Archivierung durchgeführt wird. Zusätzlich gelten für bestimmte Wirtschaftsbereiche spezielle Regelungen. In allen Firmen müssen definierte Prozesse vorhanden sein, in denen genau festgelegt ist, wer was machen darf.

Im Rahmen von Compliance gibt es fünf Regelungen, die einer genaueren Betrachtung bedürfen:

- Sarbanes-Oxley Act
- Euro-SOX / BASEL II
- European Data Protection Directive
- ISO-Norm 27001
- HIPAA

Sarbanes-Oxley Act

Das US-Gesetz Sarbanes–Oxley Act gilt für alle in- und ausländischen Firmen, die an der US-Börse notiert sind und beschäftigt sich mit der Finanzberichterstattung. Diese verlangt eine ausführliche Dokumentation der Geschäftsprozesse. Indirekte Forderungen an die IT bzw. ein IdM-System lassen sich aus dem Gesetz direkt ableiten. Demzufolge müssen Unternehmen adäquate Kontrollstrukturen für das Finanzreporting einführen, betreiben und sich jährlich einem Audit unterziehen. Innerhalb des Gesetzes wird auf generelle IT-Kontrollen verwiesen, die unter anderem den Schutz von Daten, Prozessen und Applikationen sowie den Zugriff darauf definieren. Um die Vorgaben erfüllen zu können, müssen unternehmensweite Richtlinien aufgestellt werden. Die Unternehmensführung trägt bei der Umsetzung der Forderungen volle Verantwortung und wird bei Nichterfüllung mit einer Haftstrafe von bis zu 10 Jahren und einer Geldstrafe von bis zu 15 Millionen US$ bestraft.

Euro-SOX / BASEL II

Für alle europäischen Mitgliedsstaaten ist seit Juni 2008 die Richtlinie Euro-SOX, mit ähnlichem Inhalt wie SOX, ins nationale Recht umgesetzt worden.

Ein Gesetz, das im Zusammenhang mit Identity Management ebenfalls eine wichtige Rolle spielt, ist Basel II, welches die Gesamtheit der Eigenkapitalvorschriften bezeichnet. Kernpunkt des Gesetzes ist die Bewertung eines operativen Risikos und fordert daher ein aktives IT-Risiko-Management, das sich

mit allen Aspekten der IT-Sicherheit im Unternehmen befasst. Aus Sicht des Identity Managements geht es um die Schwerpunkte Datenschutz, unberechtigten Zugriff inner- und außerhalb des Unternehmens sowie der Rechtetrennung.

European Data Protection Directive

Für Unternehmen und Organisationen innerhalb der EU gilt gleichfalls wie Euro-SOX, die European Data Protection Directive. Diese Datenschutzrichtlinie dient dem Zweck, verschiedene Gesetze zu harmonisieren. Dabei werden weitreichende Verpflichtungen im Zusammenhang mit der Ansammlung, Ablage und dem Gebrauch von personenbezogenen Daten von Mitarbeitern (wie bspw. die persönliche Adresse) und Kunden geregelt. Erhebliche Auswirkungen auf das IdM haben dabei die Forderungen zur Auskunftspflicht und angemessenen technischen Schutz der Daten.

ISO-Norm 27001

Die Bewertung der Sicherheit von IT-Umgebungen regelt die ISO-Norm 27001. Sie beschreibt die Grundsatzanforderungen an das IT-Sicherheitsmanagement und befasst sich mit der Einrichtung und Aufrechterhaltung eines Informationssicherheitsmanagementsystems. Neben der Informationstechnik werden insbesondere die relevanten Geschäftsprozesse betrachtet. Dadurch ist nicht mehr die Technik der Treiber für die Prozesse der IT-Sicherheit, sondern das Management. Für die auf allen Ebenen entstehenden IT-Risiken werden angemessene und priorisierte Maßnahmen zur Verfügung gestellt.

HIPAA

Ist Ihr Unternehmen im Gesundheitswesen tätig, kommt das Gesetz Health Insurance Portability and Accountability Act, kurz HIPAA, zum tragen. HIPAA regelt den Umgang von geschützten Patienteninformationen. Unter anderem enthält es auch Regelungen zum Datenschutz und zur Datensicherheit. Es legt fest, dass die Nutzer der medizinischen DV-Systeme und deren Zugriffsrechte nach eindeutigen Regeln verwaltet und im System gepflegt werden. Der Zugriff auf Ressourcen, die Patienteninformationen enthalten, ist auf die zu berechtigten Personen zu beschränken. Mit der Einführung der Gesundheitskarte, die sämtliche Daten über den Gesundheitszustand ihres Besitzers speichert, gewinnt dieses Gesetz zunehmend an Bedeutung.

Weitere Aspekte der Compliance

Unternehmen, die bei mehrfach geänderten Accounts den Überblick verlieren, bekommen bei Überprüfungen und erst recht im Schadensfall erhebliche Schwierigkeiten. Ganz gleich welche Vorschriften Sie einhalten müssen: wenn Sie nicht über geeignete Verfahren und entsprechende Berichterstellungsfunktionen verfügen, stehen die Chancen nicht sehr hoch, dass Sie interne und externe Audits ohne Beanstandung bestehen. Wie die oben genannten Gesetze und Vorschriften

zeigen, sind bei der Erteilung von Zugangsrechte hohe Sicherheitsstandards einzuhalten. Dazu gehört nicht nur, dass der jeweilige Vorgesetzte und nicht der Administrator entscheidet, auf was der Einzelne zugreifen kann und auf was nicht.

Außerdem muss diese Entscheidung protokolliert werden, damit im Schadensfall sichtbar ist, wer wann welche Zugangsrechte von wem und für welche Dauer bekam. Kommen durch den unbefugten Zugriff nämlich Dritte zu Schaden, ist das Unternehmen nur dann nicht regresspflichtig, wenn es nachweisen kann, nicht fahrlässig mit der Accountvergabe umgegangen zu sein.

Mit dem SAP NetWeaver IdM erhalten Sie die Tools, die Sie brauchen, um die richtigen Verfahren zu implementieren und deren Effizienz und durchgängige Einhaltung unter Beweis zu stellen. Die Software unterstützt Unternehmen und Organisationen bei der Erfüllung dieser gesetzlichen und unternehmensinternen Anforderungen. Individuell konfigurierbare Reporting-Funktionen dokumentieren die vorhandenen Kontrollmechanismen und überprüfen, ob die aktuellen Zugangsrechte der Benutzer mit den vorgegebenen Regelungen übereinstimmen. So haben nur autorisierte Benutzer Zugang zu den IT-Systemen und –Ressourcen.

5. Einordnung und Abgrenzung Identity Management

Im Folgenden möchten wir Ihnen die Architektur sowie bestehenden Komponenten eines Identity Management Systems vorstellen.

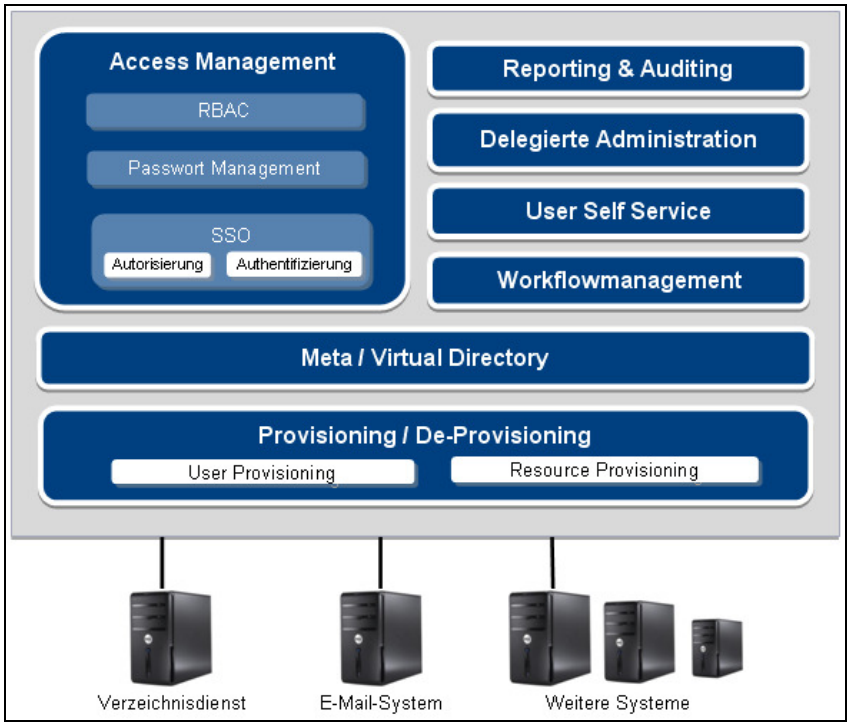

Abbildung 2: Architektur eines IdM-Systems

Die Basis eines jeden IdM-Systems bildet in der Regel ein Metadirectory, dargestellt in der Abbildung 3, welches zentral die Identitätsdaten der Mitarbeiter speichert. Die Provisioning-Komponente ist zuständig für die automatisierte Verwaltung, Verteilung und Synchronisation der Daten mit den Clientsystemen. Dies kann im Unternehmen die Bereitstellung von Benutzerkonten für die Mitarbeiter, verschiedene Arten von Ressourcen oder Zugriffsrechten sein.

Innerhalb des Provisioning wird unterschieden zwischen dem User- und dem Resource-Provisioning. Im Zusammenhang mit dem Identity Management spricht man beim automatischen Erzeugen von Benutzerkonten in den unterschiedlichen Systemen von User- oder Employee-Provisioning.

Die regel- oder rollenbasierte, zentrale Vergabe von Zugangsrechten wird als Resource-Provisioning bezeichnet. Das regelbasierte Resource-Provisioning sieht vor, dass die Steuerung der Berechtigungsvergabe der Benutzerkonten wahlweise über Gruppenmitgliedschaften oder unternehmensweite Rollenmodelle durchgeführt wird. Über die Rolle - die systemübergreifende Zugangsrechte enthält - wird definiert, zu welchen Gruppen der Mitarbeiter aufgrund seiner Funktion

hinzugefügt werden muss. Die Vergabe der Rollen findet im Metadirectory des IdM-Systems statt. Der Mitarbeiter erhält über eine Rolle die entsprechende Gruppenmitgliedschaft im IT-System.

Mit Hilfe des Resource-Provisioning ist es somit möglich, Zugangsrechte zentral zu steuern und die Vergabe der Zugangsrechte auf IT-Ressourcen systemübergreifend zu realisieren.

Das De-Provisioning ist die Umkehrfunktion und kommt beim Verlassen des Unternehmens zum Einsatz. Um Sicherheitslücken zu schließen, müssen dem Mitarbeiter sämtliche Rechte zentral im IdM-System entzogen werden. Die Sperrung des Benutzerkontos über das IdM-System führt nach der Synchronisation dazu, dass die Zugriffsrechte in allen angebundenen Systemen entzogen werden und sich der Mitarbeiter auch nicht mehr per VPN in das Firmennetzwerk einwählen kann, um interne Daten abzurufen. Weiterhin wird das De-Provisioning benötigt, wenn ein Mitarbeiter einen internen Stellenwechsel vornimmt. Steigt er in der Organisationshierarchie auf oder wechselt womöglich in eine andere Abteilung, so werden neue Zugangsrechte und Zugriffsrechte zugeteilt. Im gleichen Zuge müssen ihm die alten Rechte entzogen werden. Neben der Steigerung des Sicherheitsniveaus verfolgt das De-Provisioning darüber hinaus auch wirtschaftliche Interessen. Jedes eingesparte Benutzerkonto reduziert den Administrationsaufwand und spart in vielen Systemen und Anwendungen Lizenzkosten ein.

Unternehmen haben mittlerweile erkannt, dass es ökonomische und organisatorische Gründe gibt, Teile der traditionellen, zentralisierten Administration, verwaltet von Systemadministratoren, durch ein benutzerverantwortliches Administrationsmodell zu ersetzen. Im Rahmen der Self-Services des Identity Managements kann der Mitarbeiter vorgegebene administrative Tätigkeiten an den personenbezogenen Daten seines Benutzerkontos durchführen, ohne dass ein Administrator in den Vorgang eingreifen muss. Somit wird der Service-Desk Ihres Unternehmens entlastet.

Im Zuge der Beantragung von Zugangsrechten wird Gebrauch von den beiden Komponenten „Delegierte Administration“ sowie des Workflowmanagements gemacht. Die delegierte Administration ist der Mittelweg zwischen der benutzerverantwortlichen und der zentralisierten Administration. In diesem Modell wird die Verantwortlichkeit der Administration innerhalb des Lebenszyklus der Identitätsdaten auf dezentralisierte Administrationsgruppen aufgeteilt. Der Umfang der Delegierung wird dabei nach der Organisationsstruktur und Administrationsrollen festgelegt.

Um innerhalb des IdM-Systems Zugriffe und Aktionen der Mitarbeiter revisionssicher dokumentieren zu können, wird eine Reporting- und Auditing-Komponente bereitgestellt. Somit lässt sich genau feststellen, wann welche Änderungen im Metadirectory vorgenommen wurden. Diese Funktionalität gibt systemübergreifend Auskunft, wer wann wem welche Zugangsrechte gegeben hat, wann welche Benutzer über welche Berechtigungszugriffe verfügen und sie ihnen wieder entzogen wurden. Somit

werden die Zugangsrechte in einer heterogenen Systemlandschaft transparent und die Sicherheit erhöht.

6. SAP NetWeaver Identity Management im Detail

Wie in den vorangegangenen Kapiteln erwähnt, ist es für Unternehmen eine sehr große Unterstützung, wenn digitale Identitäten mit einem Werkzeug verwaltet werden. Mithilfe des nachfolgend vorgestellten SAP NW Identity Management (IdM) ist es möglich, digitale Identitäten effizient und sicher über Systemgrenzen hinweg zu verwalten und sich so den zuvor genannten Problemen erfolgreich zu stellen. Das IdM dient als zentrale Stelle für ein unternehmensweites Benutzermanagement, indem die Informationen aus den verschiedenen Clientsystemen sowie den angeschlossenen Verzeichnisdiensten ausgelesen und im eigenen Metadirectory, dem sog. Identity Store, gespeichert werden. Die Berechtigungsstruktur der heterogenen Systemlandschaft Ihres Unternehmens wird dadurch transparent und ist leichter zu überprüfen und zu administrieren. Dadurch ist Ihr Unternehmen zu jedem Zeitpunkt in der Lage Auskunft zu geben, wer wann im Besitz von welchen Zugriffsrechten war und kann somit die gesetzlichen Anforderungen erfüllen.

Dass SAP NetWeaver Identity Management dient als zentrale Stelle für unternehmensweites Benutzermanagement. Dabei unterstützt es die effiziente und sichere Verwaltung digitaler Identitäten in heterogenen Systemlandschaften. Es bietet eine tiefe Integration mit anderen SAP NetWeaver Plattform Komponenten und Anwendungsmodulen. Gleichzeitig ergänzt es die bereits bestehenden SAP NetWeaver Security Frameworks. Es können sowohl SAP als auch Non-SAP Systeme angesprochen und definierte Prozesse bei der Verwaltung der Benutzer abgebildet werden.

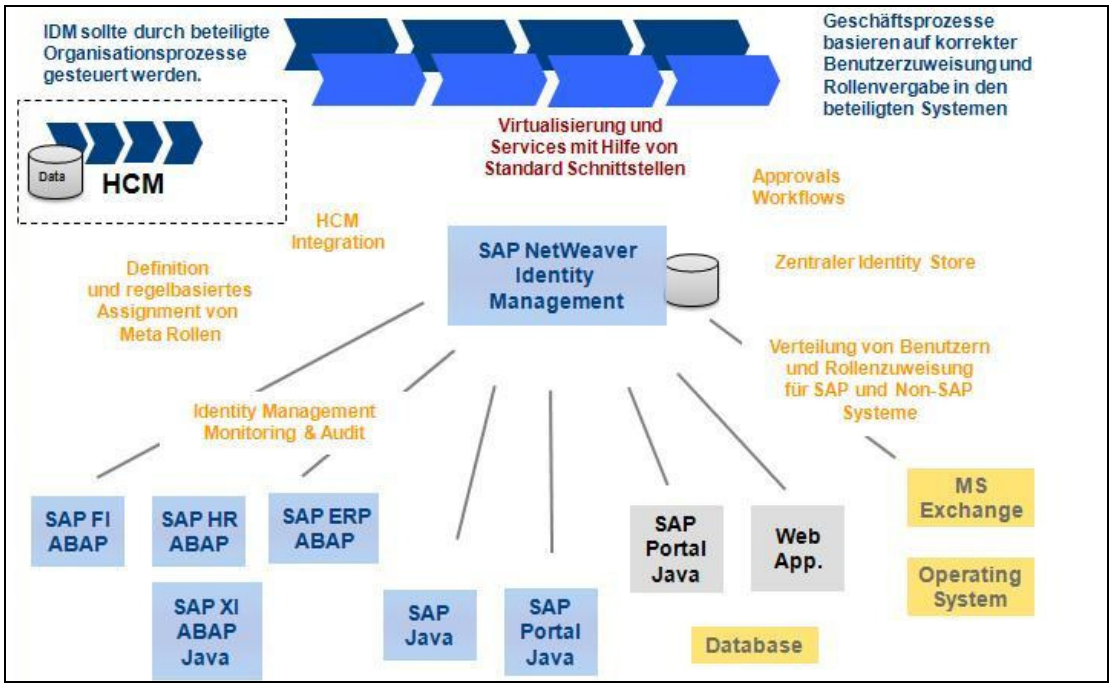

Abbildung 3: SAP NW IdM

SAP NW IdM bietet ein plattformübergreifendes Provisioning unternehmensweiter IT-Systeme und -Dienste. Um diesen Prozess umzusetzen, verwaltet es die Benutzer, die Zielsysteme und unterschiedliche Arten von Privilegien: Rollen, Zugangsrechte und Gruppen. Auf der Basis von Rollen, Regeln oder Policies werden den Benutzern sämtliche Privilegien in einem Schritt zugewiesen. Die Zielsetzung des Provisioning ist es, dass Änderungen genau einmal durchgeführt werden müssen und dann auf alle anderen Systeme der mehr oder minder heterogenen IT-Infrastruktur des Unternehmens und gegebenenfalls sogar über die Unternehmensgrenzen hinaus umgesetzt werden.

Komponenten

SAP NW IdM besteht im Wesentlichen aus zwei Komponenten, dem Identity Center (IC) sowie dem Virtual Directory Server (VDS). Zentraler Bestandteil des Identity Centers ist der Identity Store, in dem alle Identitäten in einem flexibel erweiterbaren Datenmodell organisiert werden können. Es ist möglich mehrere Identity Stores innerhalb eines IC anzulegen, um so auch Konzernstrukturen zu verwalten. Über den Virtual Directory Server wird sowohl der standardisierte Zugriff (per LDAP, SPML, etc.) auf die Inhalte des Identity Stores ermöglicht als auch der virtualisierte Zugriff auf in der Umgebung verteilte Datenquellen.

Basierend auf einer relationalen Datenbank (wahlweise kann hier der MS SQL Server oder eine Oracle Datenbank eingesetzt werden) bietet das Identity Center die Möglichkeit mehrere der erwähnten Identity Stores als zentrale Einheit(en) und als Datenbasis zu erstellen und zu verwalten.

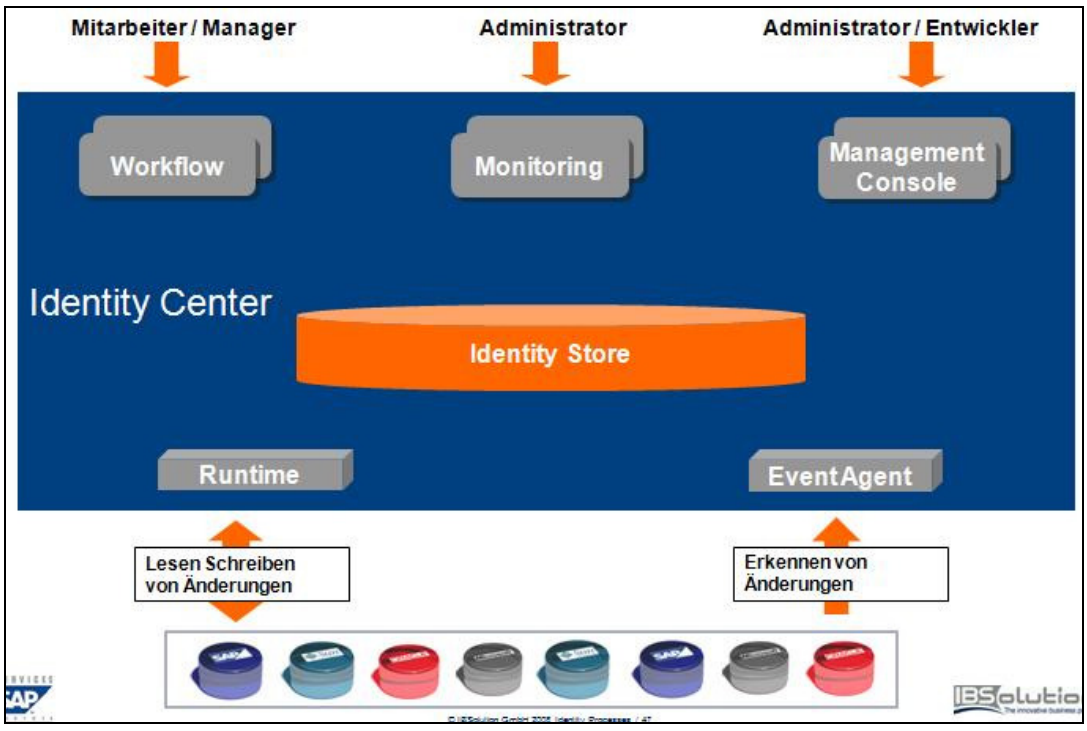

Abbildung 4: SAP NW IdM Identity Center - Architektur und Komponenten

Neben den Identity Stores dient die Definition sog. Repositories der Anbindung verschiedener Fremdsysteme. Diese Repositories können zum einen Quell- oder auch Zielsysteme für die Synchronisation der Daten mit dem Identity Store und/oder angebundene Systeme für eine automatisierte Berechtigungsverwaltung, sein.

In das SAP NetWeaver Identity Management sind Workflow-Funktionalitäten für Administratoren, Mitarbeiter und Manager integriert. Das Front-End ist eine Web-Applikation, die sich in das SAP NW Portal integriert. Hier können sich Benutzer anmelden, definierte Aufgaben sowie Genehmigungen einsehen und durchführen. Die Verwaltung der Workflows findet auf Identity Store Ebene und komplett im Identity Center statt. Die IBSolution liefert mit EPE zusätzliche Funktionen aus, die das Anlegen von dezentralen Workflows erlaubt.

Identity Center (IC)

Das Identity Center ist das Entwicklungswerkzeug des SAP NW IdM. Hierin wird der Identity Store angelegt, mit Daten befüllt und wieder ausgelesen. Quell- und Zielsysteme werden über die Repositories angelegt. Das Datenmodell des Identity Stores wird über bereits vordefinierte und eigens erstellte Objektklassen definiert. Weiterhin können Attribute und Beziehungen zwischen den Objektklassen erstellt werden. Das IdM System wird durch das Anlegen von Jobs und Passes konfiguriert. Diese können durch das Job-Log und System-Log überwacht werden.

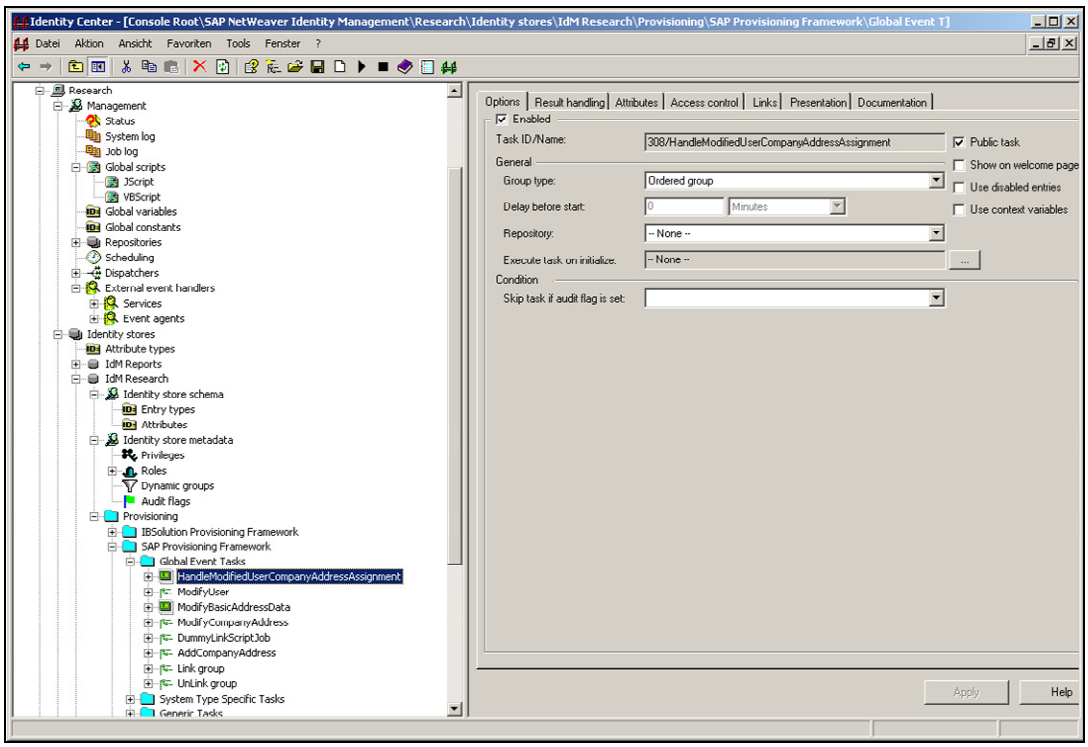

Abbildung 5: Identity Center

Zusätzlich benötigte Logik kann innerhalb von Visual Basic und Java Skripten implementiert werden. Die Ausführung der Jobs wird über die Dispatcher geregelt, die ebenfalls im Identity Center erstellt werden.

Workflow und Monitoring

Damit die Verwaltung von Identitäten und deren Zugangsrechten auf den Zielsystemen in kontrolliertem Rahmen geschieht, entwickelte die IBSolution das Add-on EPE, aktuell in der Version 3.0. Dieses gestattet es, unternehmensspezifische Genehmigungsprozesse umzusetzen. Die genauen Funktionen von EPE werden in Kapitel 7 erläutert.

Reporting

Eine wichtige Funktion im Umgang mit personenbezogenen Daten ist das Protokollieren von Datenzugriffen und –änderungen. In nahezu jeder Unternehmensrevision werden die Zugangsrechte, deren Verwaltung und deren Historie auf den jeweiligen Zielsystemen untersucht und abgeprüft. Dabei spielt es eine entscheidende Rolle, in welchem Maße diese Protokolldaten vorhanden und umfassend genug sind. Viele Sicherheitslücken und eine Reihe von fehlerhaften Zugangsrechten können durch aufbereitete Protokoll-Audits festgestellt und behoben werden.

SAP NW IdM als zentrales Instrument für die Verwaltung personenbezogener Daten kontrolliert und protokolliert automatisch alle Daten- und Berechtigungsänderungen von digitalen Identitäten sowohl auf dem SAP NW IdM System selbst als auch auf den jeweils angeschlossenen Zielsystemen.

Dabei werden die Reports nicht nur aktuell angezeigt, sondern auch archiviert und man kann jederzeit nachsehen wie der Zustand vor 1 Tag, 1 Woche oder 1 Jahr war. Die Reports können in verschiedenen Formaten wahlweise automatisiert oder manuell ausgegeben werden.

Virtual Directory Server

Der Virtual Directory Server (VDS) stellt die Daten aus dem Identity Store in unterschiedlichen Standardformaten wie LDAP, SPML oder DSML dar. Dadurch kann das IdM viel flexibler gegenüber angeschlossenen Systemen auftreten, als dies klassische Metadirectories können. Des Weiteren können andere Datenquellen virtuell angebunden werden. Die Daten und Attribute sind physikalisch in den Quellsystemen, werden nicht importiert aber so dargestellt als wären sie im Identity Store abgelegt. Dadurch kann man mehrere Attribute eines Users aus verschiedenen Quellen gemeinsam darstellen. Abbildung 7 zeigt beispielhaft Möglichkeiten über die vorhandenen Standardprotokolle eine Vielzahl von Systemen anzubinden.

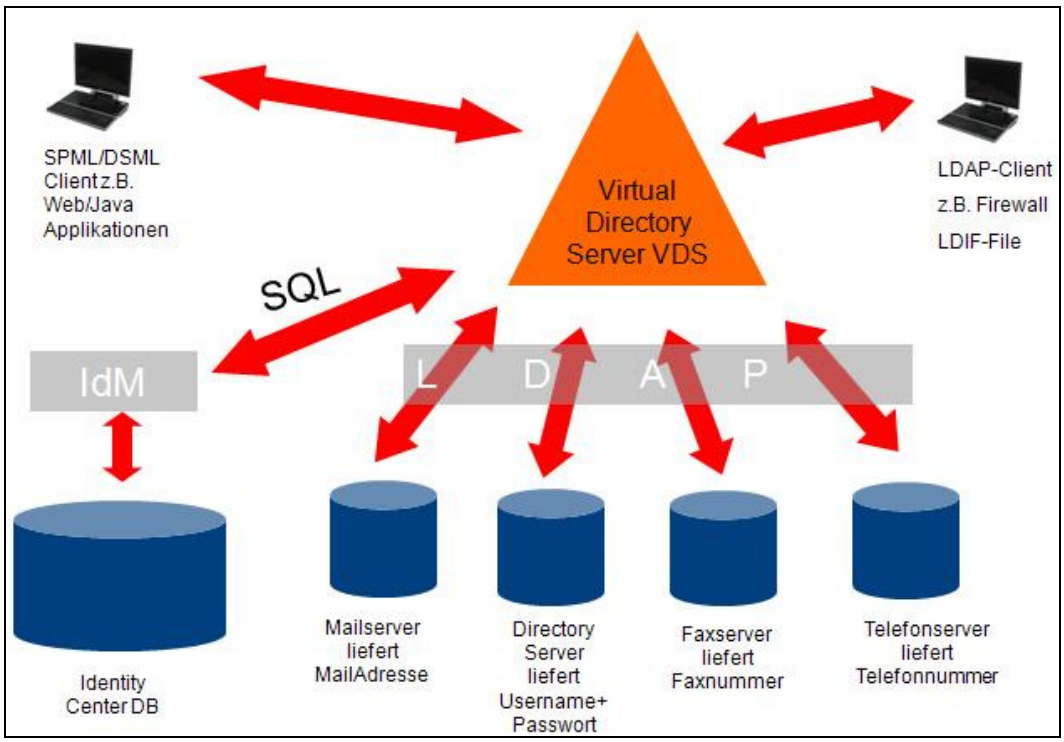

Abbildung 6: Virtual Directory Server

Synchronisation und Datenhoheit

Das Datenmodell des Identity Stores setzt sich aus einer Vielzahl von Objektklassen, die in Relation zueinanderstehen, zusammen. Durch Definition von weiteren Objektklassen bzw. dem Hinzufügen von Attributen zu den bereits existierenden Objektklassen ist das Datenmodell flexibel erweiterbar. Damit bietet das Identity Center die Grundlage für eine saubere und konsolidierte Datenbasis mit allen für die Verwaltung der Identitäten relevanten Informationen. Die zuvor genannten Event Agents spüren Änderungen sowohl in den Clientsystemen als auch im IdM-Werkzeug auf, leiten automatisch gesteuert die Synchronisation ein und gewährleisten somit die Konsistenz der Daten.

Es können eine Vielzahl unterschiedlicher Datenquellen angebunden werden. Abbildung 8 zeigt beispielhaft die Synchronisation von Daten aus unterschiedlichen Clientsystemen. Ein zentraler Punkt bei der Synchronisation ist die Festlegung der führenden Systeme und die Datenhoheit für die im Identity Store verwalteten Attribute.

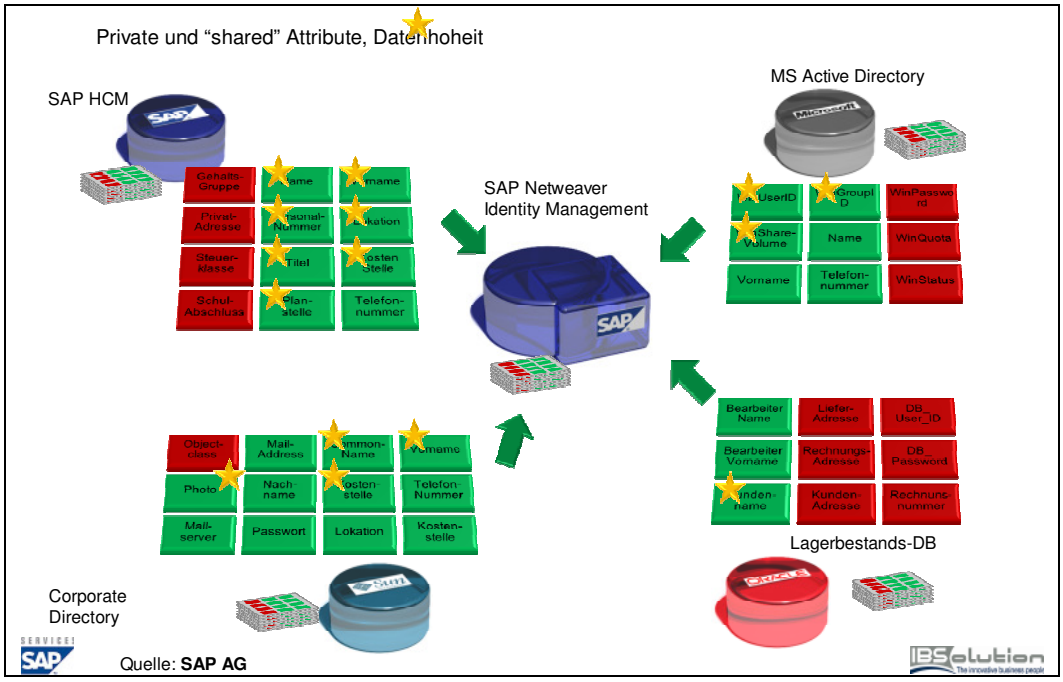

Abbildung 7: Synchronisation von Daten aus unterschiedlichen Quellen

Konnektoren

Die im Identity Store vorhandenen Identitäten werden über eine Vielzahl von Konnektoren synchronisiert bzw. in der Umgebung verteilt. Die in Ihrer Firma vorhandenen SAP-Systeme, ein Active Directory und LDAP-Directory können hierdurch angebunden und generische Fileschnittstellen bereitgestellt werden. Weitere Adapter können bei Bedarf unter Nutzung der entsprechenden APIs entwickelt werden. Abbildung 9 zeigt die aktuell verfügbaren Konnektoren.

Als Special Expertise Partner im SAP MDM und IdM entwickelte die IBSolution GmbH als erste Firma weltweit einen Konnektor für die Anbindung des SAP MDM an das SAP IdM und erweiterte somit das Portfolio der Standardkonnektoren. Hierdurch ist es möglich technische Rollen aus dem SAP MDM auszulesen, Fachrollen im IdM anzulegen und Benutzern zuzuweisen. Des Weiteren können Benutzer ins SAP MDM (de)provisioniert und geändert werden.

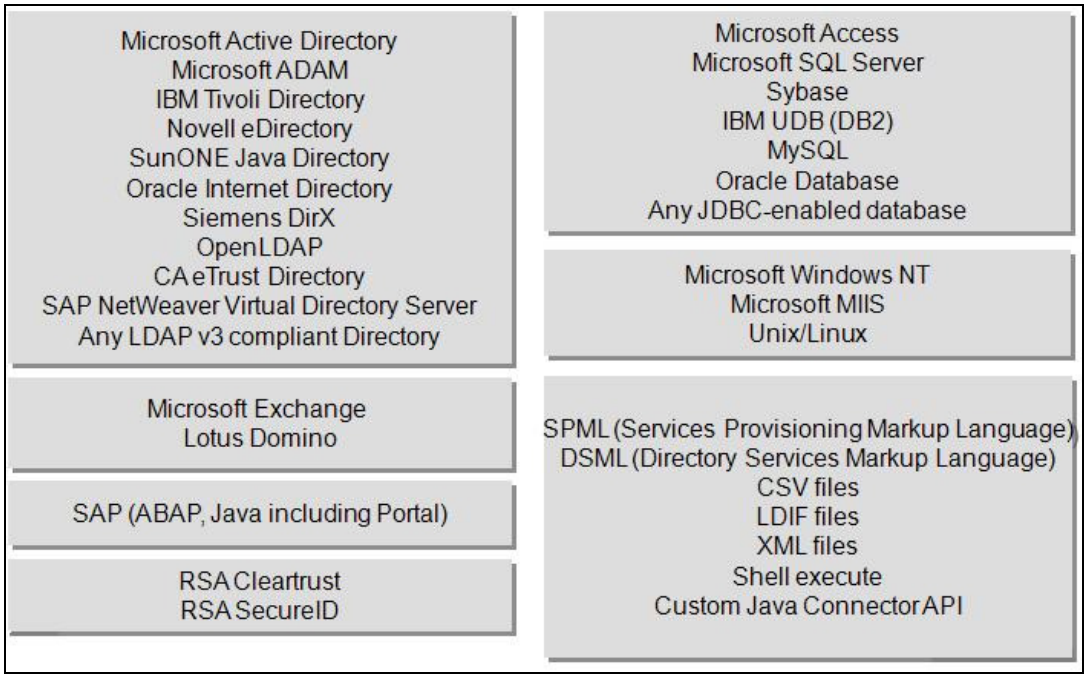

Abbildung 8: Verfügbare Konnektoren

7. Add-on Employee Productivity Excellence 3.0

Das von der IBSolution GmbH entwickelte Add-on „Employee Productivity Excellence“, kurz EPE, wurde in den letzten Monaten komplett überarbeitet. Die aktuelle Version besteht aus verschiedenen Java Technologien und weist ein breites Funktionsspektrum auf, das über die Möglichkeiten von SAP NW IdM hinausgeht. Ein Beispiel dafür sind die flexiblen Möglichkeiten auf Basis der Workflow Komponente. Eines der Herzstücke von EPE ist eine zentrale Aufgabenliste, in der die Anwender offene Aufgaben und Benachrichtigungen von Prozessen sehen und bearbeiten können. Über die Verbindung zu einem SMTP-Server können automatisch Email Notifikationen bei der Zuweisung von Aufgaben versendet werden.

Weiterhin enthält das Add-on ein flexibles Autorisierungskonzept, welches mit Hilfe von Benutzergruppen Rechte innerhalb der Anwendung vergibt und dabei neben internen Mitarbeitern auch externe Personen (wie Kunden oder Lieferanten) berücksichtigt und einbinden kann.

Zu erwähnen ist ebenfalls das Fachrollenkonzept. Mit diesem können einem Mitarbeiter mehrere sogenannte Fachbenutzer zugewiesen werden. Diesen Fachbenutzern lassen sich beliebige Fachrollen sowie technische Rollen zuweisen. Fachrollen setzten sich dabei wiederum aus Fachrollen und technischen Rollen der jeweiligen Systeme zusammen. Die für den Zugriff letztendlich benötigten technischen Benutzer werden automatisch und für den Anwender transparent vergeben.

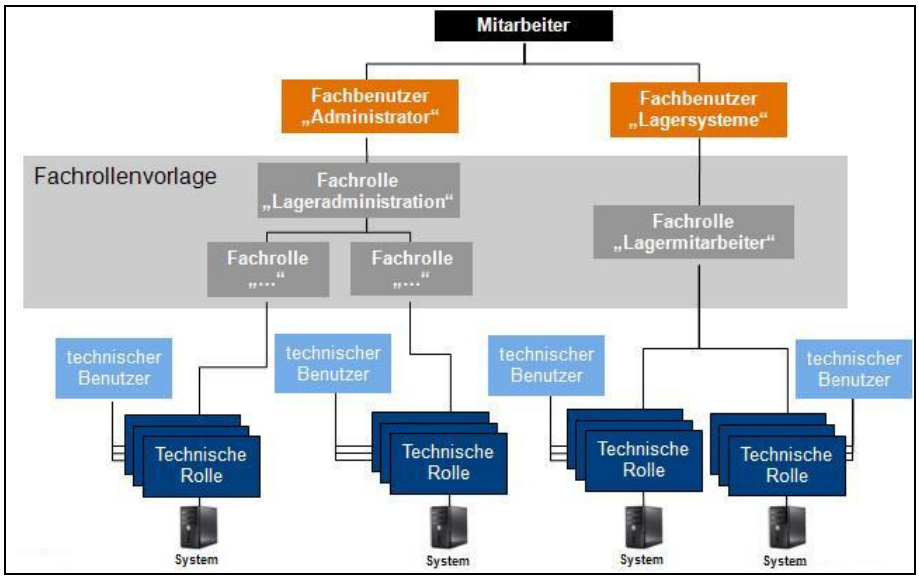

Abbildung 9: EPE - Fachrollenkonzept

EPE ist in der Lage den Identity Management Lifecycle vom Eintritt bis zum Austritt des Mitarbeiters zu unterstützen. Finden Änderungen im SAP HCM statt, werden diese automatisch an EPE übermittelt

und führen dort zum Start der jeweiligen Prozesse. Diese bereits vordefinierten Prozesse können innerhalb eines Kundenprojektes genau auf Ihr Unternehmen abgestimmt werden.

Damit die Verwaltung von digitalen Identitäten im kontrollierten Rahmen geschieht und jederzeit flexibel angepasst oder erweitert werden kann, verfügt EPE über das Workflow Construction Kit (WCK) - zu sehen in Abbildung 11. Mithilfe des WCK können jederzeit vorhandene, definierte Prozesse bearbeitet und neue Prozesse definiert werden.

Das WCK ermöglicht dabei auf einer fachlichen Ebene die Definition von Prozessen zur Verwaltung von Benutzern und Rollen. Über einen Wizard definiert der Anwender Schritt für Schritt, welchen Prozesstyp er bearbeiten möchte, welche Personen oder Gruppen darin involviert sind, mit welchen Daten gearbeitet werden soll und welche Personen(kreise) bei potenziellen Genehmigungen zuständig sind. Nach Bearbeitung des Prozesses kann der Anwender „per Knopfdruck“, d.h. ohne Programmier- und Konfigurationskenntnisse, einen Self-Service daraus generieren. Je nach Bauart des Prozesses werden dabei Employee-Self-Services (ESS) oder Manager-Self-Services (MSS) erstellt.

Bei den ESS kann der Anwender für sich selbst etwa Benutzer und Rollen beantragen. Die MSS dienen der Delegierung von Aufgaben. Ein Mitarbeiter kann somit Zugangsrechte oder Datenänderungen für bzw. bei anderen Mitarbeitern vornehmen. Das Sperren eines Mitarbeiteraccounts ist dabei ebenso möglich.

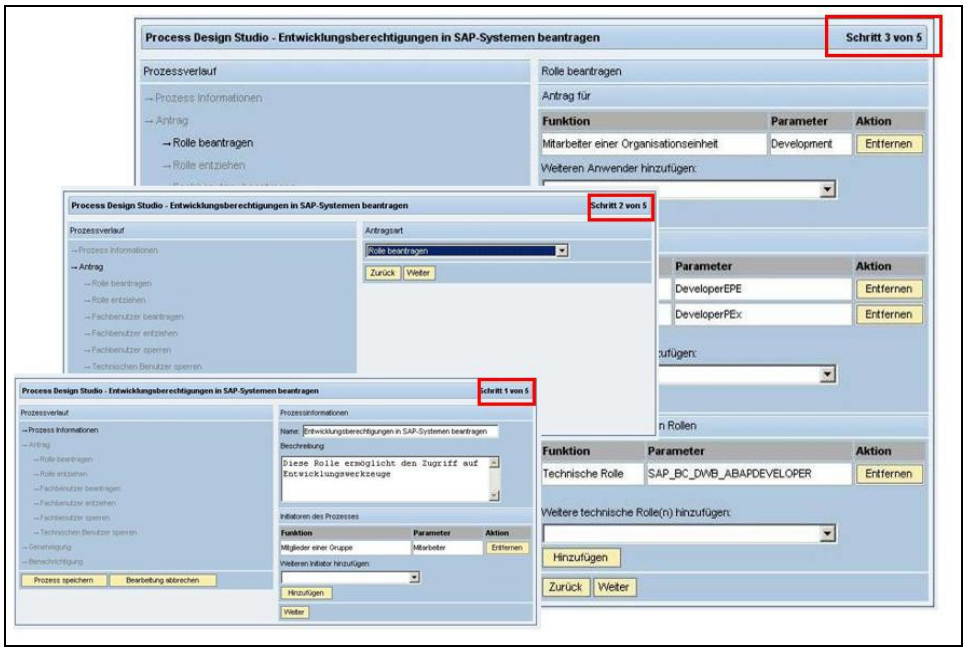

Abbildung 10: Workflow Construction Kit

Die Basis für den Ablauf von Prozessen innerhalb EPE ist die Organisationsstruktur Ihres Unternehmens. Für eine erweiterte Integration der Verwaltung von digitalen Identitäten bietet EPE die Möglichkeit, neben der hierarchischen Strukturierung von Fachrollen und damit Vererbung von Rechten und Rollen, diese mit Organisationsstrukturen des Unternehmens zu verknüpfen.

Möglich wird dies über den sogenannten Business Role Explorer. Den Business Role Explorer gibt es in zwei Ausführungen. Der Standard Business Role Explorer erlaub dem Anwender neue Fachrollen zu erstellen und diese zu editieren. Die aus dem SAP NW IdM replizierten technischen Rollen können hierbei vorhandenen Fachrollen systemübergreifend zugewiesen werden.

Bei der Rollenvergabe prüfen Regelwerke ungültige Kombinationen von Rollen, sodass bspw. ein Mitarbeiter nicht gleichzeitig im Besitz der Rollen Ein- und Verkäufer ist.

Im Advanced Business Role Explorer können vorhandene Fachrollen den Organisationseinheiten aus dem SAP HCM zugewiesen werden. Sämtliche Berechtigungsanfragen und -vergaben werden über eine interne Historisierung gespeichert, um die Nachvollziehbarkeit gewährleisten zu können.

Über einen Provisioning Scheduler wird letztendlich der Synchronisierungsablauf zwischen EPE und dem SAP NW IdM definiert und gesteuert. Neben der Anbindung des SAP NW IdM über einen speziell entwickelten und konfigurierbaren Konnektor, unterstützt EPE grundsätzlich auch die projektspezifische Anbindung von LDAP- und SPML-fähigen Clients, die nicht an das SAP NW IdM angeschlossen werden sollen.

EPE 3.0 ist in das SAP NW Portal integriert und ist somit auch UWL konform. Die vollständige Anpassung auf Ihre Umgebung wird im Rahmen eines Projektes umgesetzt.

Beispiel Prozesse

Das SAP NW IdM System unterstützt mit dem Add-on EPE die Definition von fachlich orientierten Workflows und Genehmigungsprozessen. Diese können flexibel im Workflow Construction Kit modelliert werden und stehen zur Ausführung im browserbasierten Workflow UI zur Verfügung.

Ziel ist es, die vorhandenen organisatorischen Prozesse in Ihrem Unternehmen durch das Identity Management System in technische Prozesse umzuwandeln. Spezielle Mechanismen sorgen dafür, alle Zugänge und Zugangsrechte auf einmaligen Befehl hin automatisch zeitgesteuert freizuschalten bzw. wieder zu sperren und eine unbefugte Nutzung von Zugangsrechte zu vermeiden. Anhand von typischen Beispielprozessen des Identity Lifecycles möchten wir Ihnen den Leistungsumfang dieses Werkzeuges im Folgenden näher bringen.

Beispiel Prozess: Mitarbeiterein- und austritt

Die Datenerfassung eines neuen Mitarbeiters erfolgt in der Regel über die Personalabteilung. Handelt es sich um einen internen Mitarbeiter, werden die Daten typischerweise im HR-System gespeichert. Die Verwaltung von Externen oder Business Partnern kann aber durchaus auch in einem anderen System erfolgen und werden projektspezifisch integriert.

Durch einen individuell anpassbaren Automatismus werden die Daten nach Erfassung im HR-System bereits vor dem Eintritt des Mitarbeiters in das EPE übertragen, was zum Start eines vorkonfigurierten Prozesses führt. In diesem können dem Mitarbeiter zuvor konfigurierte Standard(Fach-)Rollen für bspw. die Nutzung von Internet und Email zugewiesen werden. Die Zugangsrechte können durch Hinzufügen von weiteren Rollen (bei entsprechender Genehmigung der Führungskraft) erweitert werden. Rechtzeitig zum Eintrittsdatum werden die entsprechenden Rechte vergeben. Somit entsteht keine Verzögerung und der Mitarbeiter kann vom ersten Tag an voll produktiv arbeiten.

Verlassen Mitarbeiter das Unternehmen, egal ob sie in Mutterschaftsurlaub gehen oder das Unternehmen wechseln, sollten ihre Accounts gesperrt oder ganz gelöscht werden. Dies führt zum einen zu einer Steigerung der Unternehmenssicherheit und zum anderen zu einer Reduktion der Lizenzkosten. Gekündigte Mitarbeiter können somit weder firmeninterne Daten herunterladen noch gefälschte Dokumente oder Viren hochladen. Externe Mitarbeiter, die nicht dem Unternehmen angehören und daher nicht in der Personalverwaltung erfasst sind, stellen ein zusätzliches Sicherheitsrisiko dar. Verlässt bspw. der Mitarbeiter eines Lieferanten, der vorher Zugriff auf bestimmte Daten des Kunden hatte, seine Firma, wird die Benutzerverwaltung des zu beliefernden Unternehmens in den wenigsten Fällen von der Personalverwaltung über die Auflösung des Vertragsverhältnisses informiert. Dadurch entstehen Benutzerleichen im System, die einen potenziellen Gefahrenherd darstellen.

Die implementierten Regelwerke erstellen bei Eintritt, automatisiert für den neuen Mitarbeiter die Accounts auf den benötigten Zielsystemen und sperren bzw. löschen diese wieder bei Austritt. Neben der zeitlichen Einsparung durch die Reduktion des Administrationsaufwands wird die IT-Abteilung entlastet und das Sicherheitsrisiko gesenkt, was die zuvor genannte Studie des Fraunhofer Institutes bestätigt. Eine Einführung von SAP NW IdM mit EPE bedeutet also eine deutliche Einsparung beim Zeitaufwand bei gleichzeitig gestiegener Sicherheit und Qualität der Benutzerverwaltung.

Beispiel Prozess: Organisatorischer Wechsel

Nach zwei bis drei Jahren steigt ein Mitarbeiter, bedingt durch das Wachstum Ihres Unternehmens, zum Teamleiter auf und benötigt entsprechend weitere Zugriffsrechte oder es findet ein Abteilungswechsel des Mitarbeiters statt. Für diese Fälle kann das zentrale IdM-System die neuen (Fach-)Rollen schnell und korrekt entweder automatisch oder über einen definierten

Genehmigungsprozess zuweisen und auf den Clientsystemen die Benutzerkonten eigenständig erzeugen. Somit ist gewährleistet, dass die neuen Zugangsrechte sofort zur Verfügung stehen und der Mitarbeiter in seiner Tätigkeit nicht eingeschränkt wird. Die alten Zugangsrechte können entweder sofort entzogen werden, was meist aber nur in der Theorie möglich ist oder nach einer gewissen Zeit. Nicht nur die Zugangsrechte können sich bei einem Abteilungswechsel ändern: Ist dieser bspw. standortübergreifend, korrigiert das IdM-System automatisch die Firmenadresse des entsprechenden Mitarbeiters.

Beispiel Prozess: Zeitlich begrenzte Rollenbeantragung

In vielen Unternehmen gibt es neben dem Tagesgeschäft noch laufende Projekte. Diese sind meist zeitlich begrenzt und viele verschiedene Mitarbeiter aus unterschiedlichen Bereichen nehmen zeitweise entsprechende Funktionen wahr, für welche entsprechende Zugangsrechte in den Systemen notwendig sind.

Benötigt nun ein Mitarbeiter bestimmte Zugangsrechte für die Dauer eines Projektes, ist es möglich, die Rollen- bzw. Rechtevergabe zeitlich zu begrenzen.

Je nach Ihrem Wunsch lassen sich Prozesse als Employee-Self-Services oder Manager-Self-Services anbieten und geben Ihnen die Möglichkeit zu entscheiden, wer wann welche Rechte für welchen Zeitraum beantragen bzw. letztendlich auch bekommen soll.

Möglichkeiten und Ausblicke

Zu den genannten Möglichkeiten bietet IdP grundsätzlich die Möglichkeit, kundenspezifische Anforderungen mit einzubinden. Zudem wird der Umfang der Prozesse und Prozessarten permanent weiterentwickelt.

So sind Prozesse möglich, bei denen die Mitarbeiter selbstständig bspw. ihre Kommunikationsdaten ändern oder ausgewählte Zugangsrechte anfordern ohne dass die IT-Abteilung am Prozess beteiligt ist. Auch Zeiterfassungskorrekturen, Urlaubsanträge oder Verbesserungsvorschläge lassen sich einrichten. Die Führungskraft wird über eine Email Notification über den Berechtigungsantrag informiert und kann diesen wahlweise ablehnen oder genehmigen. Neben den Self-Services bietet lassen sich grundsätzlich auch Delegated-Services umsetzen, mit deren Hilfe eine Abteilungssekretärin in der Lage ist, z.B. die Telefonnummer aller Mitarbeiter der jeweiligen Abteilung zu ändern.

Durch die Bereitstellung etwa eines Passwort-Self-Services werden Ihre Mitarbeiter weniger abgelenkt, konzentrieren sich auf ihre Arbeit und sind effizienter. Die Mitarbeiter ändern Passwörter und verwalten ihre Identität gemäß der unternehmensweiten Passwortregelungen und den Geschäftsrichtlinien selbst, wodurch Ihr Helpdesk entlastet wird. In Kombination mit einem Single

Sign-On System müssen sich ihre Mitarbeiter nur noch ein Benutzername und Passwort merken, welches dann wesentlich komplexer aufgebaut sein kann. Die Zeitersparnis beim Einlogen sowie die sinkende Anruferzahl beim Helpdesk verschafft ihrem Unternehmen eine höhere Produktivität und senkt wiederum die Kosten.

Die aufgezeigten Beispielprozesse verdeutlichen den großen Mehrwert von SAP NW IdM in Kombination mit EPE für die verschiedenen Mitarbeiter, was sich letzt-endlich bei den Prozesskosten positiv bemerkbar macht. Die täglichen Routineaufgaben können automatisiert werden und Unstimmigkeiten beim Abgleich von Benutzerdaten in unterschiedlichen Anwendungen und Systemen sind wesentlich leichter aufzudecken. Aufgaben innerhalb der Genehmigungsprozesse kann, von der Administratoren weg, hin zu den Fachabteilungen verlagert werden. Die Administratoren haben dadurch Zeit für andere Tätigkeiten, was letztendlich zur Einsparung von Personal und IT-Kosten führt. Der Wegfall manuell durchzuführender Aufgaben führt somit zu direkten Kosteneinsparungen aufgrund der Verringerung des zeitlichen Aufwandes für die Ausstattung von Benutzern mit der richtigen Ausrüstung und den richtigen Zugriffsrechten. Wenn Zugriffsrechte gemäß geschäftlichen Richtlinien erteilt werden, entsteht daraus der zusätzliche Vorteil, dass die Governance nicht mehr durch Softwarefunktionen limitiert wird. Abteilungen legen somit die geschäftlichen Richtlinien für die Mitarbeiter anhand der Unternehmensziele fest.

Dass EPE in Verbindung mit SAP NW IdM unterstützt Sie nicht nur bei der Einhaltung der Unternehmensrichtlinien sondern verhindert, dass jemand bspw. gleich-zeitig als Einkäufer und Lieferant aufgeführt wird. Wer das Recht hat, die Zahlung einer Rechnung zu veranlassen und gleichzeitig Stellvertreter seines Chefs ist, kann zu einem günstigen Zeitpunkt das Vieraugenprinzip austricksen. Sobald der Chef im Urlaub oder krank ist, kann der Mitarbeiter über das System die Zahlungsanweisung einmal in seiner Angestelltenfunktion freigeben und gleich danach in seiner Stellvertreterfunktion. Einem herkömmlichen IT-System würde diese Unstimmigkeit nicht auffallen. Eine intelligente Benutzerverwaltung, wie sie im EPE möglich ist, prüft unter Einbeziehung gesetzlicher und unternehmensinterner Vorschriften, fortlaufend ob beantragte und automatisch zugewiesene Zugangsrechte, auch wirklich zulässig sind und schlägt gegebenenfalls Alarm. Nicht nur Administratoren werden unterstützt, ihr Führungspersonal kann durch die Delegated Services, Aufgaben an seine Mitarbeiter abgeben und sich somit wichtigeren Tätigkeiten widmen.

8. Abgrenzung SAP NW IdM zu anderen Begriffen

Im Folgenden soll das SAP NW IdM zum

- Single Sign-On,
- dem SAP GRC und
- der Zentralenbenutzerverwaltung (ZBV) der SAP

abgegrenzt werden.

Single Sign-On

Das Single Sign-On (SSO) ermöglicht dem Mitarbeiter Zugriff auf alle berechtigten Systeme mit nur einer Authentifizierung. Als Authentifizierung wird die Überprüfung der Mitarbeiteridentitäten gegenüber den IT-Systemen bezeichnet. Ist diese erfolgreich im Vergleich zu den Autorisierungsinformationen, wird der Zugriff auf das System gewährt. Im SSO-System wird ein Benutzerkonto mit entsprechendem Passwort des Mitarbeiters angelegt. Meldet sich nun der Mitarbeiter im SSO-System an, werden die Login-Informationen durch das System an die daran angeschlossenen Applikationen übermittelt. Dieses Verfahren kombiniert Sicherheit mit Komfort für den Mitarbeiter. In Bezug auf das SAP NW IdM ist SSO ein Add-on, welches über Drittanbieter, entweder clientbasiert oder servergestützt eingesetzt werden kann.

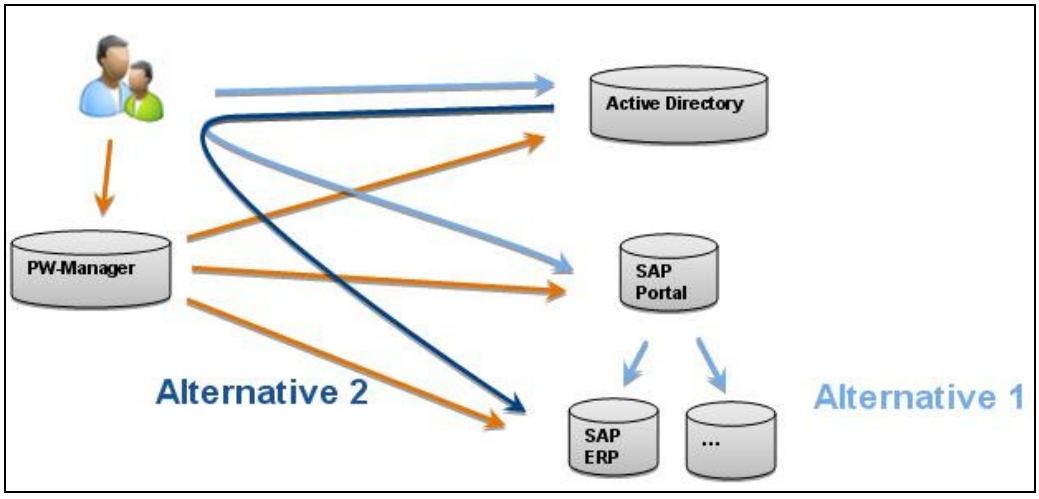

Abbildung 11: Single Sign-On

Abbildung 12 zeigt mögliche Alternativen in einer IT-Umgebung mit MS Active Directory und einem SAP NW Portal. In Alternative 1 authentifiziert sich der Benutzer gegen das AD, dieses übernimmt die Anmeldung am SAP NW Portal. Das Portal wiederum übernimmt die Anmeldung an den Systemen, die an es angebunden sind (Logon Ticket mit SAP). Alternative 2 stellt eine weitere Möglichkeit der

Nutzung von SSO dar. Hierbei übernimmt das AD die komplette Anmeldung für sämtliche Systeme innerhalb der IT-Landschaft (ebenfalls mit Kerberos).

Abgrenzung zu SAP GRC / Virsa

SAP Governance, Risk und Compliance (GRC), welches als technologische Grundlage die NetWeaver Plattform hat, wird von Unternehmen in den Bereichen der nachhaltigen Unternehmensführung, des Risikomanagements und bei der Einhaltung gesetzlicher Auflagen eingesetzt. Dabei werden Risikobewertungen und Sicherheitskontrollen mit den Geschäftsprozessen des Unternehmens verknüpft. Die wesentlichen Funktionen von SAP GRC sind die Speicherung und Verwaltung von GRC-relevanten Informationen wie Unternehmensregeln, interne Bestimmungen und branchenspezifische Vorschriften (Außenhandel, Umwelt-, Gesundheits- und Arbeitsschutz).

SAP IdM und SAP GRC ergänzen sich gut, da die GRC Lösung es ermöglicht, die Rollen und Berechtigungen in einem SAP ERP System auf mögliche Gefährdungsrisiken zu durchsuchen. Dies kann ein IdM normalerweise nicht leisten.

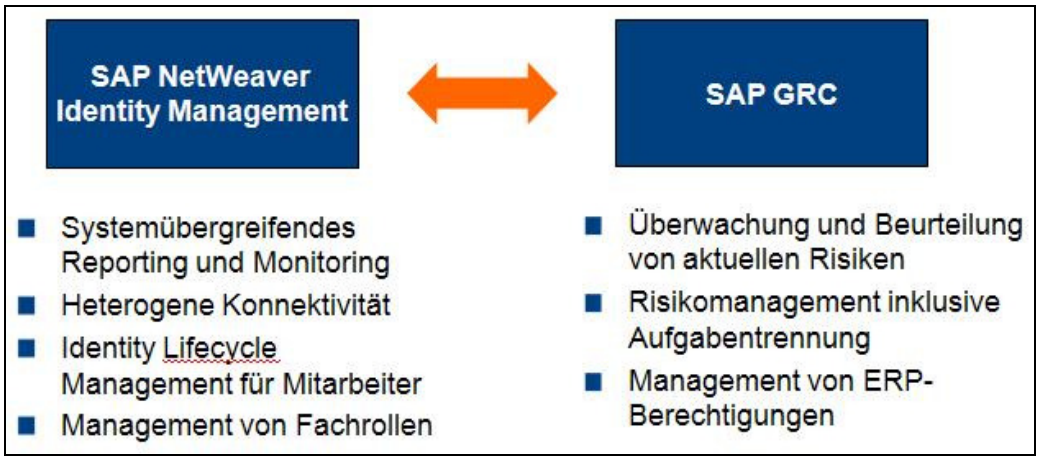

Abbildung 12: Abgrenzung SAP GRC

Durch die Integration von SAP NW IdM in SAP GRC lässt sich bis auf Transaktionsebene ein Compliant Identity Management erreichen.

Abgrenzung zur zentralen Benutzerverwaltung (ZBV)

Die Zentrale Benutzerverwaltung (ZBV) der SAP, in der aktuellen Version NetWeaver 7.1, ist in ihrem Funktionsumfang beschränkt. Es können nur SAP Web AS Systeme verwaltet werden, wobei es für die Vergabe der Zugangsrechte keinen Standardworkflow gibt.

Die Vorgesetztenfindung erfolgt bei der Berechtigungsgenehmigung daher manuell. Im Gegensatz zum SAP NW IdM beschränkt sich die Sicht innerhalb der ZBV auf die Benutzer. Im Standard nicht

enthaltene Attribute sind hierbei nur sehr schwer abbildbar. Ein weiterer Nachteil der ZBV ist, dass sich die verschiedenen technischen Rollen nicht in Fachrollen zusammenfassen lassen. Lediglich die Unterscheidung in Einzel- und Sammelrollen ist möglich.

9. Identity Process: Der Beratungsansatz der IBSolution

Identity Process kurz IdP ist die strategische Methode der IBSolution, um Identity Management Projekte schneller und kostengünstiger zu implementieren. Neben dem deutschlandweit exzellenten Know-how im SAP NW IdM Tool, hat unsere Entwicklungsabteilung mit dem Add-on EPE 3.0, ein Workflow-Tool und Fachrollenwerkzeug geschaffen, mit dem Sie individuell Ihre Prozesse abbilden können. Zusätzlich bietet die IBSolution für das Provisioning Framework vordefinierten Content. Diese Voraussetzungen zusammen mit unseren vordefinierten Paketen, die sowohl Prozesse als auch Konnektoren beinhalten, bilden ein Stufenmodell, das eine schrittweise Implementierung ermöglicht.

IdP Pakete

Um möglichst alle Kundenbedürfnisse abdecken zu können, bietet die IBSolution verschiedene IdP Pakete zu einem festen Preis an. Ziel ist es, bereits mit dem IdP Start Paket dem Kunden eine voll funktionsfähige IdM Infrastruktur zu implementieren, welche dann über Plus und Advanced erweitert werden kann. Abbildung 14 stellt die vier wesentlichen Pakete dar.

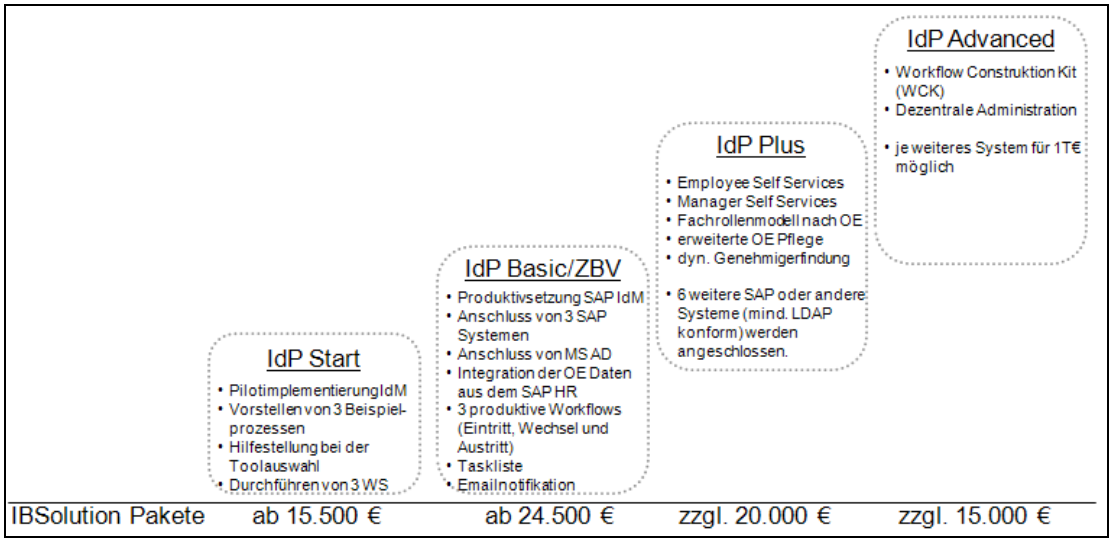

Abbildung 13: IdP Pakete

IdP Start Paket

Das IdP Start Paket bietet Ihnen eine lauffähige und vorkonfigurierte Testinstallation des SAP NW IdM inklusive dem Add-on EPE 3.0. Dieses Paket erlaubt Ihnen die Analyse der SAP IdM Lösung, ohne viel Geld auszugeben und liefert Ihnen im Anschluss eine aussagefähige Projektkalkulation mit Machbarkeitsempfehlung. Aus dem Organisationsmanagement Ihres vorhandenen SAP HCM Systems werden ausgewählte Daten in das SAP NW IdM übernommen. Die automatisierte Provisionierung basiert dabei auf der Zugehörigkeit zu einer Organisationseinheit, einer Planstelle

oder einer bestimmten Ausprägung zusätzlich übernommener Merkmale. Der Workflow wird für drei Beispielprozesse mit ausgewählten Employee- und Manager-Self-Services konfiguriert. Weiterhin erfolgt ein exemplarischer Anschluss der Systemtypen SAP Web AS ABAP / SAP Web AS Java oder MS Active Directory.

IdP Basic/ZBV Paket

Dieses Paket enthält die Installation des SAP NW IdM inklusive dem Add-on EPE 3.0 in einer 2-stufigen Landschaft sowie der Durchführung eines 1-tägigen Workshops, in dem Ihre relevante SAP Systemlandschaft analysiert und gemeinsam mit Ihnen ein Migrationsplan für die aktuellen Systeme erstellt wird. Im Anschluss daran erfolgt die Übernahme der SAP-Berechtigungen (Rollen und Profile). Der Identity Lifecycle wird durch die Implementierung von drei produktiven Workflows (Eintritt, Wechsel und Austritt des Mitarbeiters) vollständig abgebildet. Weiterhin beinhaltet dieses Paket die Anbindung von max. drei SAP Web AS ABAP Systemen sowie des MS Active Directories. Nach Fertigstellung des Projektes erfolgt eine 1-tägige Administratorschulung zur Vermittlung der Projektkenntnisse. Als Dokumentation bekommt der Kunde ein Troubleshooting Guide sowie ein Cookbook zum selbstständigen Anschluss weiterer SAP Web AS ABAP Systeme.

IdP Plus Paket

Sind Ihre Anforderungen durch das IdP Start Paket noch nicht vollständig abgedeckt? Das IdP Plus Paket bietet weitere verschiedene Employee-Self-Services zur Fachrollenpflege und zum Beantragen von Zugangsrechten. In diesem Paket ist das Fachrollenmodell von den HCM-Organisationseinheiten abgeleitet. Zusätzlich können weitere SAP- oder Non-SAP-Systeme (mindestens LDAP-konform) an das SAP NW IdM angebunden werden.

IdP Advanced Paket

Das IdP Advanced Paket beinhaltet das vollfunktionsfähige Workflow Construction Kit (WCK), das das dezentrale Anlegen von Workflows ermöglicht und so die Basis für die delegierte Adminstration ist. Damit können Sie Ihre eigenen Identity Prozesse modellieren. Zusätzlich können Verantwortliche für die Genehmigung definiert werden. Die Workflowschritte basieren hierbei auf dem Organisationsmodell oder anderen Richtlinien.

10. Referenzen

Die Firma BLANCO wurde 1925 gegründet und gehört heute zur E.G.O.-Gruppe. Sie produziert und vermarktet innovative Qualitätsprodukte und –systeme in den Bereichen Küchentechnik, Catering Systeme, Medical Care und Industrial Components. Mit den insgesamt 1300 Mitarbeiter an fünf Produktionsstandorten erwirtschaftete die BLANCO GMBH + CO KG 2007 einen Umsatz von 271 Millionen Euro.

Die IBSolution GmbH implementierte bei BLANCO eines der ersten SAP NW IdM Projekte in Deutschland. Hierbei wurden Identity Management Prozesse zur Verwaltung digitaler Identitäten eingeführt. Ziel des Projektes war es, eine systemübergreifende, zentrale und automatisierte Benutzer- und Berechtigungsverwaltung zu implementieren. Das SAP NW IdM wurde hierbei in die bestehende heterogene IT-Infrastruktur integriert. Es wurde ein zentrales Metadirectory für die Identitätsdaten erstellt. Die SAP- und Non-SAP-Systeme wurden unter Einsatz von Standardkonnektoren sowie SAP NW PI zur Übernahme der Identitäten aus dem SAP HCM und SAP ERP (Geschäftspartner) angebunden. Die Umsetzung einer Migrationsstrategie der alten Benutzerbestände auf die neuen Anforderungen, um die Benutzer-IDs in den verwalteten Systemen zu vereinheitlichen, zählte ebenfalls zum Projektumfang.

11. IBSolution GmbH

IBSolution ist 2003 in Heilbronn als Start-up mit sechs Mitarbeitern angetreten. Heute gehören wir zu den führenden Beratungshäusern rund um SAP NetWeaver und sind mit über 160 Mitarbeitern an den Standorten Berlin, Dortmund, Heilbronn, München sowie in der Schweiz vertreten.

Wir verstehen uns als Bindeglied zwischen den betriebswirtschaftlichen Herausforderungen des Kunden und der Kompetenz der Softwarehersteller. Als Full-Service-Dienstleister beraten wir Sie umfassend in allen Bereichen von SAP NetWeaver. Wir unterstützen mit vorhandenen Komplettlösungen und eigenen Produkten, um Ihre Anforderungen so flexibel wie möglich umzusetzen.

Dabei verfolgen wir ein klares Ziel: Die Steigerung Ihrer Leistungsfähigkeit. Wir sind einer der ersten Special Expertise Partner für SAP NetWeaver Identity Management. Bereits heute schon, nach so kurzer Einführungszeit dieser Software, können wir ein erfolgreich durchgeführtes Projekt bei einem größeren Unternehmen vorweißen. Zusammen mit dem Kunden wird hierzu in Kürze eine Success Story herausgebracht.

Neben regelmäßigen Veröffentlichungen von Blogs und Webinaren (anzusehen unter www.ibsolution.de), beraten die Solution Architekten und Consultants unseres IdP-Teams, Entwickler und Berater weltweit im SDN-Forum, in dem wir auch die Top-Ten Liste anführen. Durch unseren engen Kontakt zum SAP IdM Entwicklungsteam und Produktmanagement tragen wir zur ständigen Verbesserung des Produktes bei. Deutschlandweit vertrauen Unternehmen jeder Größenordnung und aus zahlreichen Branchen auf unser Know-how. Man schätzt uns als vertrauensvollen Partner, der viel Wert auf den Gesamtüberblick der SAP-Welt legt.

Unsere Projekte sind überschaubar, kalkulierbar – und bringen Ihr Unternehmen nach vorn. Nutzen Sie die Möglichkeit mit unseren Festpreispaketen eine lauffähige und vorkonfigurierte Installation des neuen Werkzeuges SAP NetWeaver Identity Management 7.0 in Ihrer eigenen Umgebung aufzubauen.. Weitere Informationen finden Sie auf unserer Webseite www.ibsolution.de.

12. Impressum

IBSolution GmbH
Edisonstr. 21
74076 Heilbronn
Tel. 07131 / 64974-0
Fax. 07131 / 64974-7042
www.ibsolution.de