

manage **it**

[[IT - S t r a t e g i e n u n d L ö s u n g e n]]

Prozesse müssen (auch) gelebt werden

Business Process Management

Koexistenz statt Konkurrenz

Trends in der Telekommunikation

CIO, ihr Beitrag bitte

Business Technology Optimization

Frage: Wie stehen die Geschäfte?

Antwort: Business Performance Management

Der CIO als Spar-Weltmeister

IT-Kosten

Nutzen Sie unser Angebot für
Sonderdrucke oder E-Publishing-Dateien
von Artikeln dieser Ausgabe

Tel.: +49 8092 87543

LDAP, Metadirectory und Identity-Management

Bitte nur einmal einloggen

Mal angenommen, Sie würden sich morgens an den Rechner setzen, Sie loggen sich ein und benötigen für den Rest des Tages keinen weiteren Beweis, dass Sie und nicht Ihr Arbeitskollege vor der Tastatur sitzt. Sie müssten nicht immer wieder ein anderes Passwort für Ihren Zugriff auf die Mail, die Gehaltslisten bei der Personalabteilung, den Car-Konfigurator für den Dienstwagen oder die Architektur-Dokumentation für Ihr Projekt angeben. Haben Sie sich schon mal überlegt, wie viele Passwörter Sie gemäß der Sicherheits-Richtlinien Ihres Unternehmens durchschnittlich alle vier Wochen ändern müssten?

Und wie kryptisch diese eigentlich sein müssen?

Das Thema Authentifizierung ist in jedem Unternehmen mehr oder weniger ein Damoklesschwert. Viele Mitarbeiter werden verpflichtet, für die unterschiedlichsten Freigaben eine Vielzahl von Zugangskennungen zu verwalten, seien es Passwörter, Zertifikate, Passphrasen usw. Nicht jede Zugriffskontrolle ist so sicher, wie sich die Unternehmensleitung das gerne wünschen würde. Nach einem Urlaub sind viele Mitarbeiter erst einmal damit beschäftigt, sich an all die Kennungen zu erinnern, die sie für ihre Arbeit benötigen. Und manche haben dann »Erinnerungs-Stützen« in Form von Zetteln, die sie im besten Fall im eigenen Geldbeutel transportieren oder aber sie kleben sie unter die Tastatur.

Sag mir deinen Namen... User-Datenmanagement ist in Unternehmen wichtiger denn je. Immer mehr Applikationen werden verwendet, diese Anwendungen benötigen die Informationen, wer mit ihnen arbeiten darf und wer nicht. Damit hält jede eine eigene Datenbank von Benutzerdaten vor, die gewartet und aktualisiert werden möchte.

Der Ansatz in Form eines zentralisierten Directorys löst das Problem der

Benutzerdatenverteilung. So wird nicht mehr jede Applikation mit ihrem eigenen Datenstamm versehen, sondern »fragt« den Directory-Server nach den User-Daten. Beispiel: Ein Nutzer, der im Internet nach Informationen für seine Arbeit recherchiert, möchte über

Nutzen Sie unser
Angebot für
Sonderdrucke oder
E-Publishing-Dateien
von Artikeln aus

manage it
[IT-Strategien und Lösungen]

Tel.: +49 8092 87543

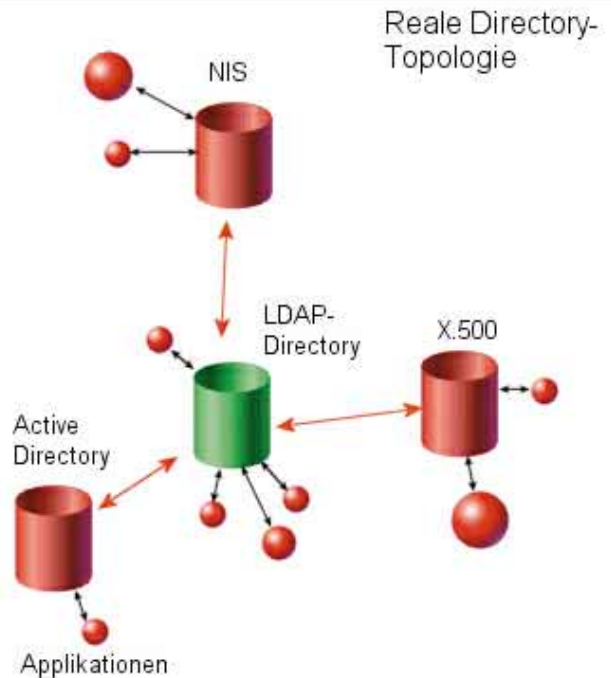
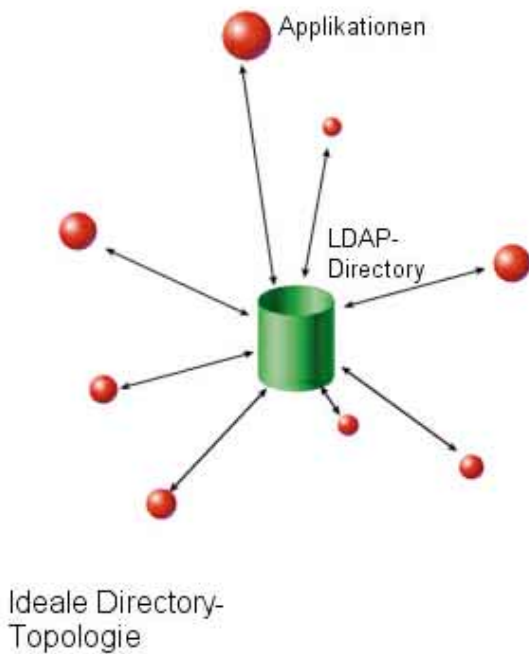
den Proxy-Server einen Webaufruf starten. Der Proxy-Server sendet eine Anfrage an das Directory mit der Bitte um Klärung, ob die UserID- und Passwort-Kombination, die der Mitarbeiter gesendet hat, gültig ist und ob sich dieser User in der Gruppe der Internet-Berechtigten befindet.

Der Vorteil liegt auf der Hand: Nicht nur eine, sondern viele Applikationen können diese zentralisiert vorge-

haltenen User-Daten verwenden. Damit kann sich der Anwender mit einem einzigen Nachweis seiner Identität - beispielsweise mit der Angabe seines Passwortes - gegenüber den Applikationen authentifizieren. Aus Administrationssicht hat dies natürlich ein enormes Einsparungspotential: Nur noch eine einzelne User-Datenbank muss gepflegt werden und nicht jede der Applikationen. Und ein weiterer Vorteil: Die Datenzuverlässigkeit steigt, weil mit einer zentralen Änderung alle Anwendungen direkt mit den aktualisierten User-Daten arbeiten.

In den letzten Jahren hat sich LDAP als Protokoll für die User-Datenübermittlung herauskristallisiert. Mit diesem Standard werden die Daten in einer Datenbank hinterlegt und über das standardisierte Protokoll an die Applikationen getragen. Führende Hersteller für Software in diesem Bereich ist Sun, IBM, Siemens, Oracle und Novell.

Teile und Herrsche. Nun wäre dieses Szenario zu schön, um wahr zu sein. In realen Unternehmensnetzwerken gibt es immer wieder Applikationen, die darauf bestehen, ihren eigenen Datenstamm zu halten. Bestimmte Daten



sind sehr sensitiv und verlassen diese lokalen Datenbanken nicht, andere können bestenfalls mit dem zentralen Directory synchronisiert werden. Beispiel: Ein SAP-System wird es nicht zulassen, dass Userdaten wie Gehaltsklassen in ein Global LDAP-Directory ausgelagert wird. Es wird bestenfalls gestatten, dass Daten wie Vorname, Nachname und Telefonnummer mit einem LDAP-System synchronisiert wird.

Damit hat man auch bereits ein Lösungs-Szenario beschrieben: Das Meta-Directory. Hier gibt es nach wie vor ein zentralisiertes Directory, das all die User-Daten aufnimmt, die für die angebundenen Applikationen von Relevanz sind. Bestimmte Daten aber werden mit Software-Tools synchronisiert, so dass eine Änderung in einer der Applikationen direkt in das zentrale Directory durchgereicht wird und umgekehrt. Der Begriff Meta-Directory beschreibt damit nicht mehr die zentralisierte User-Datentopologie, sondern eine - immer noch zentralisiert administrierbare - verteilte Benutzerdatenhaltung. Hersteller wie Sun bieten mit ihrem Directory sogenannte Konnektoren zu anderen Systemen wie SAP, Oracle, Microsoft Active Directory usw.

Die neue Freiheit. Ein Directory (sei es ein zentrales oder ein Meta-) verwaltet nur die Benutzerdaten. Identity-Management geht noch einen Schritt weiter. Sogenannt »Identity-Server« übernehmen die Kontrolle und die Verantwortung für die Authentizität eines Users - so weit es die Kommunikation auf Netzwerkebene betrifft. Sie überprüfen den User stellvertretend für alle Applikationen, sie »wissen« anhand von User-Profilen, wer was mit wem und welcher Applikation tun darf und stehen all den angeschlossenen Applikation Rede und Antwort. Damit werden zwei Anforderungen gelöst: Benutzerrichtlinien werden zentral verwaltet (diese können an einer Stelle aktiviert, entfernt und geändert werden) und ein Anwender muss sich nur noch einmal »am Netz« anmelden und ist direkt an allen für ihn relevanten Applikationen angemeldet. Dieses Anmeldeverfahren wird unter dem Begriff »Single Sign On« beschrieben. Beispiel: Der Mitarbeiter meldet sich an seinem Computer an und bekommt ohne weitere Kontrollen Zugriff auf seine Mail, seine Dokumente und seinen Kalender.

Aber nicht nur lokal kann dieses Anmeldeverfahren von Vorteil sein.

Angenommen, ein Identity-Server im Internet verwaltet User-Daten von drei Unternehmen: Ein Internet-Portal, eine Fluglinie und ein Auktionshaus. Diese Konstellation hätte für alle Beteiligten einen Vorteil:

1. Das Auktionshaus und die Fluglinie können dem Anwender individualisierte Seiten anbieten, die Identitäts-Prüfung übernimmt der Identity-Server
2. Der Portal-Anbieter kann sowohl die Fluglinie als auch das Auktionshaus in die Liste der konfigurierbaren Portalfenster übernehmen, da alle Beteiligten einem einzigen Identity-Server vertrauen.
3. Der Anwender loggt sich ein einziges Mal an dem Portal an und kann dort seine konfigurierten Nachrichten, seine Mail, seine Adressen und seinen Kalender verwalten. Ohne weitere Authentisierung hat er aber auch direkt einen Einblick auf seine Flugmeilen und den Stand seiner Gebote bei dem Auktionshaus.

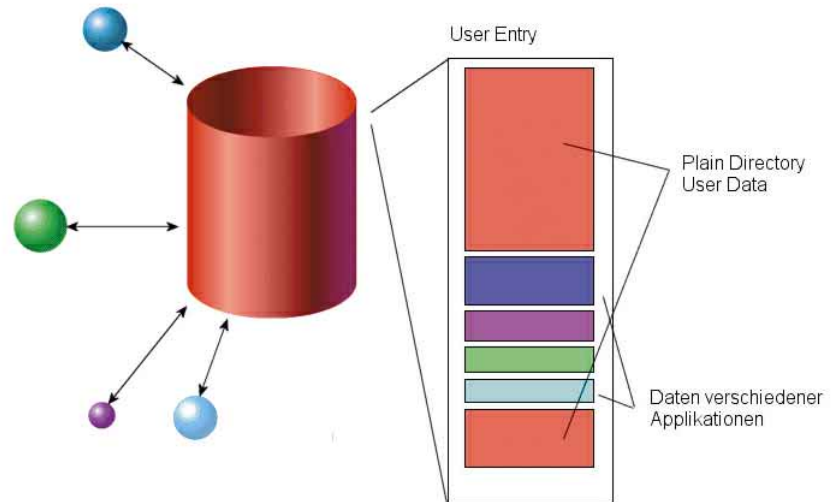
In einer solchen Konstellation wird eine vollkommen neue Dienstleistung geschaffen, die die Kundenbindung

stärkt, aber auch die Administrierbarkeit der Benutzerdaten vereinfacht.

LDAP ok, aber... Natürlich haben viele Kunden den Nutzen von LDAP erkannt, eingekauft und im Unternehmen eingeführt. Was aber im ersten Moment viele Probleme löst, wirft auf der anderen Seite neue Anforderungen auf. Was, zum Beispiel, ist schlimmer als ein Directory, das man gerne einsetzen möchte, das sich aber nicht mit anderen User-Repositorys verträgt? Wenn sich die Synchronisation innerhalb eines komplexeren Meta-Directorys als ein mittlerer Alptraum erweist?

Manche LDAP-Projekte scheitern nicht an der Implementierung des Basisdienstes, sondern an der Abstimmung der Daten mit anderen Systemen. Gerade deshalb haben sich Meta-Directory Projekte als der Alptraum vieler Anbieter wie Hersteller ergeben. Wo aber liegt denn eigentlich das Problem? Nun, um dies herauszufinden, muss man das Problem einmal etwas näher beleuchten. Grundsätzlich werden die Daten für ein Directory über eines oder mehrere Schnittstellen eingegeben. Sogenannte Provisioning Systeme sorgen dafür, dass der Administrator eine geeignete Plattform hat, über die er die Directory-Daten administrieren kann. Sind diese Datenänderungen einmal eingepflegt, ist der Datenbestand aus Directory-Sicht in Ordnung. Wer aber sorgt nun für den Abgleich mit den anderen Verzeichnissen? Ist es das Directory selbst, das diese Aufgabe übernehmen soll oder muss derjenige, der die Datenänderung verursacht, also der Administrator oder dessen Provisioning Tool dafür sorgen, dass Datenänderungen auch an die anderen Verzeichnisse gelangen. Hier ergibt sich immer wieder ein grundsätzlicher Streit, der bereits philosophischen Charakter besitzt. Für die eine Gruppe ist ein Directory ein selbst-konsistentes System, das sich automatisch und selbstständig austariert. Mithin werden alle Datenänderungen innerhalb der Meta-Directory Umgebung propagiert und der Administrator greift nur noch über eine einzige Schnittstelle auf das

Directory-Daten "Verschmutzung"



Verzeichnissystem zu. Auf der anderen Seite gibt es die Gruppe derjenigen, die die alleinige Aufgabe eines Directorys darin sehen, User-Daten zu liefern: schnell, konsistent und zuverlässig. Meta-Aktivitäten haben in diesem Weltbild keinen Platz, vielmehr sieht man hier die Aufgabe der Datenverteilung auf Seiten des Administrators beziehungsweise dessen Tools zur Provisionierung. Eine Diskussion dieses Ansatzes würde

erfahren hat. Dies ist eines der Probleme, mit denen die Directory-Hersteller zu kämpfen haben: der Bereitstellung einer Datenbank, die die zeitlichen Änderungen der Daten aufzeigt, in der richtigen Sequenz und Reihenfolge, damit nicht ein Passwort geändert von einem User geändert werden soll, der in einer vorherigen Aktion bereits gelöscht wurde. Dieses »Event-Repository« muss natürlich performant sein, gut auszulesen und immer vorhanden. Dieser Ansatz steht natürlich dem grundsätzlichen Anspruch eines Directorys entgegen, das Daten liefern soll und sonst nichts. Jedwede Protokollierung von Datenänderungen bremst das System aus und das ist genau das, was die Hersteller vermeiden möchten. Erfahrungsgemäß erfährt ein über mehrere homogene Server replizierter Datenstamm entweder eine schnelle Datenverteilung über Replikations-Mechanismen (bei denen der Server Replikations-Konflikte selbstständig auflöst und verarbeitet) und protokolliert dabei so wenig wie möglich die Datenänderungen, oder die Änderungshistorie wird aufbereitet und verfügbar gemacht, was mit einer ausgebremsten Verteilung der Daten erkauft wird.

**Nutzen Sie unser
Angebot für
Sonderdrucke oder
E-Publishing-Dateien
von Artikeln aus**

manage it

[IT-Strategien und Lösungen]

Tel.: +49 8092 87543

sich über die Vielzahl der Tools erstrecken, die auf dem Markt sind und die dieser Aufgabe mehr oder weniger gerecht werden. Betrachten wir also den Service-Automatismus und dessen Meta-Funktionalität. Das Problem ist, dass die meisten Directory-Server kaum Buch darüber führen, welche Daten geändert wurden. Vielmehr liefern sie bereits geänderte Daten. Um aber zu synchronisieren, muss man wissen, welche Datenänderungen das System

Datenschutz. Wer einmal mit viel Schweiß ein so genanntes Corporate Directory installiert hat und dabei die Grundregeln des Directorys beherzigt hat, in denen steht, dass nur Daten in

ein Verzeichnis gelangen, die von mehr als einer Applikation verlangt werden, der wird sich oft so manchen Hersteller von Applikationen herbeiwünschen, um ihnen den Marsch zu blasen. Moderne Applikationen haben mehr und mehr den Trend, ihre Daten in ein bestehendes Directory zu schreiben. Dies ist an und für sich nicht schlimm, erweist sich allerdings als Crux, wenn diese Daten eben nur von dieser einzigen Applikation verlangt werden. Noch schlimmer wird die Situation, wenn diese Daten auch noch häufig geändert werden. Beispiele hierfür gibt es zuhauf: Profildaten für User, in denen die Hintergrundfarbe des Desktops definiert wird, Portal-Daten, Kalender-Status, Mailserver-Präferenz. All diese Daten sind aus Applikations-Sicht wahrscheinlich gut im Directory aufgehoben, sie »verschmutzen« allerdings das

Verzeichnis mehr und mehr. Ganz schlimm wird es, wenn diese Daten unstrukturiert direkt in einen User-Eintrag hinterlegt werden. Nach der zehnten Applikation wächst ein ehemals schlanker User-Entry mittels Passbild-, Portal-Profil-, Desktop- und Browser-Cache zu einem Brocken von Megabyte-Gewicht. Spätestens dann ist der Directory-Ansatz verraten und das Verzeichnis ist von einem schlanken Corporate Directory zu einem Öltanker mutiert, der nur noch schwer unter administrativer Kontrolle zu bringen ist.

Resümee. Zweifellos hat LDAP einen großen Nutzen in vielen Unternehmen. Große Service-Provider kämen ohne eine solche Infrastruktur gar nicht mehr aus und viele Teenies könnten ohne diesen Dienst nicht ihre Bildchen per MMS durch das Netz

senden. Eine zentralisierte Benutzerdatenhaltung vereinfacht die Administration erheblich und sorgt für einen einheitlichen und zuverlässigen Datenbestand. Die Kunden sind aber auch anspruchsvoller geworden und glauben längst nicht mehr alles, was die Hersteller versprechen. Deren Credo, alles zu vereinheitlichen und ein einziges Verzeichnis im Unternehmen einzusetzen, ist schön, einfach, aber leider nicht immer praktikabel. Die Kunden verlangen hier Lösungen, die aus einer heterogenen Landschaft einen selbstkonsistenten und zuverlässigen Verzeichnisdienst machen. Und hier liegen die Herausforderungen, denen sich die Hersteller der Directory-Software stellen müssen, sei es über Erweiterungen in der Funktionalität der Produkte oder durch maßgeschneiderte Lösungen.

Peter Gergen

3 Monate lang

Einblick

Durchblick

Ausblick

f ü r d r e i z e h n f ü n f z i g !



[] **Ja**, ich bestelle » *manage it* « für drei Monate zum Preis von Euro 4,50 pro Ausgabe. Dieses Probeabonnement verlängert sich nicht automatisch.

Schicken Sie diesen Coupon an:

ap verlag GmbH
Postfach 1380
85554 Ebersberg

oder faxen Sie die Seite einfach an die Nummer

+49 8092 87544

Titel: _____

Vorname: _____

Nachname: _____

Position: _____

Firma: _____

Straße: _____

PLZ: _____ Ort: _____

E-Mail: _____

Telefon: _____

Fax: _____