Ressort: Sicherheit/Netzwerk

Baukonzern Alpine modernisiert das Identity-Management

Directory auf Meta-Ebene steuert heterogene IT-Systemwelt

Eine zentrale Benutzerverwaltung und Single Sign On auf Basis des offenen Standards Lightweight Directory Access Protocol (LDAP) senkt bei Alpine den IT-Verwaltungsaufwand und erhöht den Komfort für die Benutzer.

Der Nutzen von IT liegt in den Prozessen, das ist seit geraumer Zeit das Credo von Marktforschern und Kennern der IT. Investitionen in Soft- und Hardware sollen sich also in Arbeitsabläufen positiv niederschlagen und dadurch sichtbar werden – sonst gibt es von der Geschäftsleitung kein Geld. Das ist grundsätzlich richtig, birgt allerdings die Gefahr, dass für IT-Projekte, die erst auf den zweiten Blick erkennbaren Nutzen bringen, die Geldhähne zugedreht werden. Wehe dem IT-Leiter, der ein Infrastrukturvorhaben plant, von dem die Anwender nicht direkt etwas merken.

„Nur damit die IT technisch auf dem neuesten Stand ist, macht keine Unternehmensleitung Geld locker“, bestätigt Hans Lechner, IT Leiter beim Baukonzern Alpine Mayreder. Dennoch haben die Österreicher ein Projekt gestemmt, das die IT-Betriebskosten senkt und bei genauerer Betrachtung gleichzeitig deutliche Verbesserungen für die User bringt. Alpine hat eine historisch gewachsene Systemlandschaft mit einem hohen Verwaltungsauf-

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

wand. Im Einsatz sind die unterschiedlichsten Betriebssysteme etwa diverse Microsoft-Windows-Versionen (NT Server, Server 2003), und darüber hinaus gehören Server unter Linux zum IT-Inventar.

Gekennzeichnet ist die IT von Alpine zudem durch eine Vielzahl von Web-Anwendungen sowie Office-, Mail- und Backend-Applikationen. „Viele unserer Mitarbeiter sind in unterschiedlichen Niederlassungen sowie Außenstellen tätig und auch der Anteil an mobilen Arbeitsplätzen etwa auf den Baustellen wächst stetig. Die Kollegen brauchen vor Ort Zugriff auf ihre Daten, Projektpläne, Mails und Drucker – das müssen wir sicherstellen“, erklärt Lechner weiter. Die Kommunikation zwischen der Zentrale in Salzburg, den rund 90 europaweiten Niederlassungen und den externen Stellen muss daher reibungslos funktionieren.

Eine besondere Herausforderung für Alpine bestand vor allem darin, das Identity-Management mit der Benutzer- und Rechteverwaltung in der komplexen IT-Landschaft zu bewerkstelligen. Die Vielfalt der IT-Systeme spiegelte sich in einem heterogenen Management-Konzept wider, wie Lechner erklärt. So wurden rund 100 NT-Domänen unter Samba für jeden Standort separat verwaltet. Samba ist ein Open-Source-Projekt, welches Linux bzw. UNIX Servern ermöglicht, Verzeichnis- und Drucker-Freigaben für Windows Clients zur Verfügung zu stellen. Zugleich existierte für das Linux-basierende E-Mail-System und den Webproxy-Dienst seit einigen Jahren ein zentrales LDAP Directory, das die konzernweite Benutzerverwaltung regelte. Damit die rund 2500 User von Alpine ortsunabhängig Zugang und Zugriff auf ihre Daten hatten, mussten sie zum Teil mehrfach angelegt werden

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

– sowohl in der Zentrale als auch in den Außenstellen, in denen sie tätig waren. Entsprechend ihrer Berechtigung galt es, ihnen die Ressourcen wie Drucker lokal zuzuordnen. Auch mussten sie sich für jede Applikation, zu der sie einen berechtigten Zugriff hatten, einzeln anmelden.

Fast noch problematischer als das Anlegen der Nutzer und deren verfügbarer Ressourcen im jeweiligen lokalen Netz, war das korrekte Löschen, etwa wenn ein Mitarbeiter ausscheidet oder sich seine Berechtigungen änderten. Lechner dazu: „Es war sehr aufwändig nachzuprüfen, in welchen lokalen Directorys ein User angelegt war, um und ihn vollständig löschen zu können.“ Das barg potenzielle Sicherheitsrisiken, da die Gefahr bestand, Einträge in den unterschiedlichen Systemen schlicht zu vergessen.

„Wir haben uns daher Mitte letzten Jahres entschlossen, eine Lösung zu finden, welche die rund 2500 Windows 2000 und Windows XP-Arbeitsplätze in den Außenstellen in das zentral betriebene LDAP Directory, basierend auf Linux Open LDAP, integriert“, erinnert sich IT-Leiter Lechner. Die Server-Landschaft sollte dabei weiterhin konzernweit auf Linux/Samba bestehen bleiben, an den bisher eingeführten Technologien sollte sich also nichts ändern. Darüber hinaus war geplant, das in Salzburg zentral betriebene Active Directory für die Anwendungen Microsoft Exchange und SQL Server, ohne zusätzlichen Verwaltungsaufwand in diese heterogene Systemlandschaft zu integrieren.

Alternativ hätte Alpine die vorhandenen Verzeichnisse vollständig durch ein zentrales Active Directory ersetzen

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

können, um damit alle dezentralen Server zu managen. Das zentrale LDAP-Verzeichnis war bereits detailliert aufgebaut, enthielt sehr viele Hierarchieebenen in denen die Benutzerprofile und Ressourcen festgelegt waren. „Die getätigten Investitionen wollten wir sichern“, wie Lechner sagt. „Zudem haben wir zahlreiche Open-Source-Systeme im Einsatz und dafür ist LDAP die Lösung.“ LDAP ist ein offener Standard und herstellerunabhängig.

Insofern fiel die Entscheidung, den LDAP-Standard als Basis für ein integriertes Identity- und Berechtigungs-Management zu verwenden. „LDAP bietet zu marktgängigen Systemen Schnittstellen, sowohl in die Microsoft-Welt als auch zu SAP, Oracle, unterschiedlichsten Datenbanken, Portalen und Mobile-Interfaces. „Es ist so etwas wie der kleinste gemeinsame Nenner, mit dem wir unsere Landschaft zentral managen können“, sagt Lechner. Aufgrund der großen Community biete es darüber hinaus die nötige Zukunftssicherheit. So entstand die Idee, eine Meta-Ebene einzuziehen, aus der heraus sich die heterogenen Systeme zentral – ohne Änderungen an der bestehenden Struktur – verwalten lassen.

Nach einer Marktrecherche im Sommer 2005 wurden die Salzburger bei der Wiener Comtarsia GmbH und deren „SignOn“-Produktfamilie fündig. Die Comtarsia „SignOn Solutions“ bestehen aus zwei Systemmodulen, dem „Comtarsia Logon Client“ und dem „Comtarsia SignOn Gate“. Der Logon Client ermöglicht am Arbeitsplatz eine direkte Anmeldung an ein LDAP Directory. Durch eine LDAP Schema-Erweiterung können Informationen wie Benutzerverzeichnispfad, Benutzerprofilpfad, Drucker und Laufwerkszuordungen, Single-Sign-On-(SSO-) Da-

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

ten, im LDAP-Benutzer- oder –Gruppen-Objekt abgelegt werden, welche der Logon Client bei jeder Anmeldung auswertet. Die automatische Benutzerverwaltung auf den Ressourcensystemen (Windows NT, Windows 2000, Windows XP, Linux, Terminal Server/Citrix) übernimmt das Zusatzprodukt Comtarsia SignOn Gate.

„Den ganz großen Vorteil von Comtarsia sehen wir darin, dass zwei Welten, in unserem Fall Linux und Windows, miteinander verknüpft und zentral gemanagt werden können. OpenLDAP in der zentralen Benutzerverwaltung, Active Directory für einige Server-Anwendungen und Linux/Samba als Fileserver lässt sich mit den Lösungen ohne zusätzlichen Aufwand vereinen“, erklärt IT-Leiter Lechner. Ein Mausklick genüge, um zu wissen was ein Benutzer dürfe und was nicht. Auch die Unabhängigkeit, die die Lösung bietet gefällt den Alpine-IT-Spezialisten. „Wir können uns bei der Auswahl neuer Lösungen frei am Markt bedienen und sind durch die Vorgaben eines Herstellers nicht eingeschränkt.“

Die heutigen Systeme bleiben eigenständig und es müssten keine Zertifikate untereinander ausgetauscht werden (sharing). Das sei wichtig für den Supportfall. „Wenn man Samba mit dem Active Directory verbindet (join), kann man Probleme bekommen, da einmal vorgenommene Einstellungen nicht mehr funktionieren, nachdem ein neues Service Pack von Microsoft eingespielt wurde“, erklärt Lechner. Im dritten Quartal begann der Rollout des Produkts und inzwischen sind alle 2500 Arbeitsplätze installiert.

Da Alpine bereits ein zentrales LDAP-Verzeichnis aufgebaut hatte, bestand die Option durch das Einspielen der

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

Comtarsia LDAP-Schemaerweiterung die Benutzer- und Gruppenobjekte (welche im LDAP standardmäßig vorhanden sind) durch zusätzliche Attribute zu ergänzen (etwa Homedirectory Path, Profile Path, SSO Informationen etc.) Comtarsia verbindet die Benutzerdaten und Systeme dazu. Damit die Implementierung so rasch von statten gehen konnte, waren allerdings einige Vorarbeiten nötig, wie sich Lechner erinnert: „Eine Herausforderung bestand darin, das historisch gewachsene LDAP Directory, welches in seiner Hierarchiestruktur sehr komplex war und sich nicht 1:1 als Zentrale Benutzerverwaltung übernehmen ließ, für das gesamte Netzwerk zu verwenden“, sagt Lechner. Hier mussten zunächst einfachere LDAP-Struktur erarbeitet werden. Lechners Tipp lautet daher: vor einem umfassenden Projekt im Bereich Identity Management und bei der Konsolidierung von Benutzerverwaltungsdatenbanken darauf zu achten, eine der Verzeichnisstruktur zu definieren, die der Verschachtelung der Organisationseinheiten entspricht. „Nicht komplexer als absolut notwendig“, ist sein Motto heute.

Durch die Implementierung des einheitlichen Directory-Managements hat Alpine quasi nebenbei ein Single Sign On (SSO) realisiert. Heute muss sich der Anwender lediglich einmal anmelden, um Zugang zu allen Applikationen zu erhalten, zu denen er Zugriffsrecht hat. In punkto SSO-Projekt empfiehlt Lechner nach seinen Erfahrungen, die Benutzer-ID's in allen Systemen zu vereinheitlichen. „Das erleichtert die Implementierung.“ Nachdem die neue Lösung im Einsatz ist und der Verwaltungsaufwand deutlich gesenkt werden konnte und die Management-Qualität verbessert wurde, ist für Alpine nun das Thema Sicherheit groß geschrieben: In Zukunft soll die

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

Anmeldung nur noch mittels Smart Card oder Token möglich sein. Die Einführung einer Public-Key-Infrastructur (PKI) soll die Sicherheit im Alpine-Netzwerk erheblich steigern und den Benutzerkomfort, durch den Wegfall des Passwortes, ebenfalls erhöhen. „Die Lösungen von Comtarsia ermöglichen uns hier eine schrittweise Umstellung der Anwender und Arbeitsplätze auf eine sichere Anmeldung mittels Benutzerzertifikat“, so Lechner. Eine PKI-Teststellung konnte im Alpine-Netzwerk bereits erfolgreich realisiert werden.

Kästen

Kasten 1

Alpine
Der weltweit tätige Baukonzern wurde 1965 gegründet. Er erwirtschaftet einen Umsatz von knapp zwei Milliarden Euro pro Jahr und beschäftigt rund 9 000 Mitarbeitern. Alpine ist der zweitgrößte Baukonzern Österreichs. In den letzten sechs Jahren konnte der Konzern seine Bauleistungen mehr als verdoppeln, die Finanzierung erfolgte aus der Ertragskraft des Unternehmens. Der Konzern hat mittlerweile rund 150 Tochtergesellschaften und Beteiligungen. Zu den Kerngeschäftsfeldern gehören:
Hochbau, Straßen- und Ingenieurtiefbau,
Tunnel- und Spezialtiefbau, Kraftwerksbau, Projektentwicklung und die Alpine-Energie-Gruppe.

Kasten 2:
Projektsteckbrief
Projektstart: Identity-Management und Single Sign On

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

Branche: Baubranche
Zeitrahmen: Q3 2005 bis laufend
Stand heute: implementiert und im produktiven Einsatz
Produkte: Comtarsia Logon Client, Comtarsia SignOn Gate
Dienstleister: Comtarsia GmbH
Ergebnis: zentrale Kontrolle und Management, geringerer Administrationsaufwand, mehr Sicherheit, einmalige Anmeldeprozedur, erhöhte Transparenz
Herausforderung:
Vereinheitlichung von Verzeichnisstrukturen, Rollout ohne Einschränkungen des produktiven Betriebs

Kasten 3
Was ist LDAP
LDAP ist ein Netzwerkprotokoll, das bei so genannten Verzeichnisdiensten (Directories) zum Einsatz kommt. Es vermittelt die Kommunikation zwischen dem LDAP-Client (zum Beispiel einem Mailserver, einem Mailclient oder einem digitalen Adressbuch wie im Outlook-Client) und dem Verzeichnis (Directory Server), aus dem benutzerrelevante Daten ausgelesen werden (Suche mir die Mailadresse von ‚Joe User' heraus). Mittlerweile hat sich im administrativen Sprachgebrauch eingebürgert, dass man von einem LDAP-Server spricht, dabei meint man einen Directory-Server, dessen Daten-Struktur der LDAP-Spezifikation entspricht und der über das Netzwerkprotokoll LDAPv3 Daten mit Client-Systemen austauschen kann. Das Protokoll bietet alle Funktionen, die für eine solche Kommunikation notwendig sind: Anmeldung am Server (sog. bind), die Suchabfrage (Suche mir bitte alle Informationen zum Benutzer mit dem Namen

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München

'Joe User'!) und die Modifikation der Daten (Beim Benutzer 'Joe Cool' ändere bitte das Passwort!).
Neuere Implementierungen, die über RFC 2251 hinaus gehen und Gegenstand für eine mögliche Erweiterung des Protokolls sind, berücksichtigen die Replikation der Daten zwischen verschiedenen Directories

Kasten 4
Hier lesen Sie…

- Wie sich heterogene Netzwerkstrukturen zentral managen lassen;
- Worauf bei der Einführung eines übergreifenden Verzeichnisdienstes und Identity-Managements zu achten ist;

warum ein offener Standard, einem herstellergebunden Protokoll vorzuziehen ist.

Presse-Kontakt:
Comtarsia IT Services GmbH, Maria Henickl, Neulerchenfelder Str. 32/Top 2-5,
A-1160 Wien, Tel.: +43-1-9578917-0, Fax: +43-1-9578917-20,
E-Mail: maria.henickl@comtarsia.com, Internet: http://signon.comtarsia.com
Autor: Bernd Seidel, freier Journalist in München