




Alle Identitäten und Rechte im Griff

Deutsche Telekom setzt mit Projektunterstützung von TWINSOFT auf IdM



Was passiert, wenn die Schar der Teilnehmer, vorangetrieben durch die Kommunikation über das Internet, immer größer wird? Dann wächst das Risiko, dass viele Teilnehmer nicht oder nicht korrekt registriert werden. Das wiederum hat verheerende Folgen für die Zugriffskontrolle gegenüber Intranet, Extranets und Internet. Denn nur wer mit seinem Namen zentral eindeutig geführt wird, dem können generelle Zugriffsrechte fürs Unternehmensnetz (Authentisierung) und spezielle Zugriffsrechte für einzelne Anwendungen (Autorisierung) eingeräumt werden, um alle anderen, unberechtigten Zugriffe verlässlich abzuwehren.

► Besonders gefordert

Besonders Telekommunikationsanbieter, wie die Deutsche Telekom, sind mit dieser Problemstellung konfrontiert. Das Ressort „Voicemail und Server Systeme“ (VSS) der Deutschen Telekom betreibt überregional die Systeme, des Anrufbeantworters im Netz (mit und ohne UM-Funktionen), das SMS-Gateway für die SMSe im Festnetz und einige weitere Mehrwertdienste wie z.B. SoundLogo und MusikGruß.

In diesem Ressort machen über zweihundert Benutzer, verteilt über unterschiedliche Standorte, teils auch mobil unterwegs, eine lückenlose Registrierung unverzichtbar. Das Mittel dazu: Identity-Management. Kommt der Baustein Access-Control hinzu, kann der Telekommunikationsanbieter durch die Zuordnung von persönlichen Rechten oder Gruppenrechten auf dieser soliden Registrierungsbasis eine sichere Zugriffskontrolle aufbauen, die für unberechtigte Zugreifer keine Lücken lässt. So entsteht Identity-Management, kurz: IdM. Die IdM-Lösung des Ressort VSS mit den Bausteinen zentrale Benutzerverwaltung, Zugriffskontrolle und Single Sign-on (SSO) wurde von TWINSOFT konzipiert und auf Basis von Access Master von Evidian umgesetzt. Der dritte Baustein, SSO, ordnet zur Freischaltung der berechtigten Anwendungen im Hintergrund automatisch die Passwörter zu, ohne dass die Teilnehmer sie zu sehen bekommen.

► Überzeugende Vorteile

Die Vorteile, die sich der Telekommunikationsanbieter über die IdM-Lösung erschlossen hat, können sich sehen lassen. Durch die zentrale Führung von Teilnehmern und ihren Rechten geht die Benutzeradministration gegenüber den zuvor dezentralen Administrationsstrukturen viel einfacher und kostengünstiger über die Bühne. Dieser Zentralismus kommt zudem einer hoch sicheren Zugriffskontrolle zugute, zumal er die Etablierung konzernweiter Passwort-Richtlinien stützt. Zu einer zusätzlichen Effizienzsteigerung trägt eine über alle installierten Zielapplikationen einheitliche Konsolenoberfläche und Menüführung für die Administratoren bei. Durch den konsequenten Einsatz von Rollen, also Gruppenrechten, für einzelne Fachbereiche oder Fachgruppen wird die Benutzer- und Rechteadministration weiter vereinfacht. Tritt ein neuer Teilnehmer in diese Gruppe, erhält er automatisch alle in der Rolle nur einmal hinterlegten Zugriffsrechte.

Der SSO entbindet die Teilnehmer nicht nur davon, sich ihre unzähligen Passwörter merken und sie jeweils eingeben zu müssen. Dadurch, dass die Passwörter im Hintergrund bleiben, können sie auch nicht länger von Angreifern abgeschaut oder abgegriffen werden. Zudem entlastet der Single Sign-on den Helpdesk. Er ist, wie in der Vergangenheit, nicht immer wieder gefordert, vergessene oder (vermeintlich) aufgedeckte Passwörter neu vergeben und sicher den Teilnehmern zuweisen zu müssen. Noch mehr: Über den SSO können sich die Teilnehmer, sofern berechtigt, kostensparend im Self-Service im Netz anmelden. Daraufhin bekommen sie automatisch die für sie nicht einsehbaren Privilegien zugewiesen

► Lukrative Einsparungen

Darüber hinaus konnte der Telekommunikationsanbieter über eine klare Personalisierung und Rechtezuordnung sein Auditing über den automatischen Mitschnitt aller Zugriffe verbessern – sowohl mit Blick auf interne Revisionsanforderungen als auch Compliance, also der Erfüllung rechtlicher Anforderungen. IdM mit den Bausteinen zentrale Benutzeradministration, zentrales Rechte- und Rollen-Management sowie SSO macht sich durch all diese Vorteile für Unternehmen schnell bezahlt. Zumal sie mit erheblichen Kosteneinsparungen

TWINSOFT GmbH & Co. KG

Europaplatz 2
64293 Darmstadt
Tel.: 06151 39756-0
Fax: 06151 39756-50

Siemensstr. 8-10
40885 Ratingen
Tel.: 02102 3004-0
Fax: 02102 3004-50

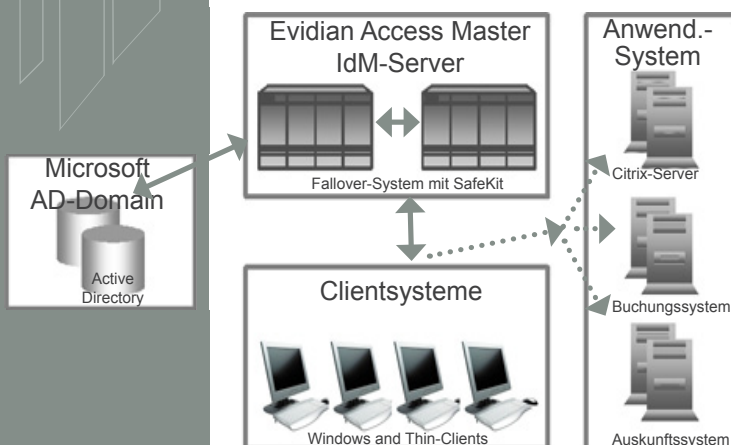
Einsteinstr. 55
89077 Ulm
Tel.: 0731 407697-0
Fax: 0731 407697-50

www.twinsoft.de
info@twinsoft.de

TSM V 03.09

Alle Identitäten und Rechte im Griff

verbunden sind. Gartner veranschlagt die Einsparungen durch die zentrale Identitäten- und Rechteverwaltung, einschließlich Rollen-Management, auf 30 Prozent und mehr gegenüber dem kostspieligen, dezentralen Status quo zuvor. Dem SSO mit all seinen Vorteilen misst das Marktinstitut Helpdesk-Einsparungen von bis zu 30 Prozent gegenüber der Zeit ohne den SSO-Mechanismus bei, von den Produktivitätszuwächsen durch beschleunigte Teilnehmerzugriffe einmal abgesehen.



■ Mit dem Projektverlauf zufrieden

Bald wird beim Telekommunikationsanbieter die Einbindung von Web-Applikationen in die IdM-Infrastruktur folgen. Die IdM-Lösung Access Master ist bereits durch TWINSOFT auf diese Integration vorbereitet worden. Für eine noch sichere Authentisierung ist zudem angedacht, dass die Teilnehmer in der nächsten Zeit statt auf Passwörter auf Smartcards zurückgreifen können. Auch dieser Wechsel wird – aufgrund der Unterstützung durch Access Master und der Vorarbeit durch TWINSOFT - für den Telekommunikationsanbieter sanft über die Bühne gehen.

■ Unterstützung von Anfang an

Ein wohlkoordiniertes IdM-Projekt braucht professionelle Unterstützung. TWINSOFT stand der Deutschen Telekom von Anfang an zur Seite bei:

- Recherche und Informationsbeschaffung
- Systemüberblick
- Test und Bewertung

- Dokumentation der Ergebnisse der Produktrecherche
- Dokumentation der Testinstallation und Betriebsparameter
- Erstellung des Einführungskonzepts
- Unterstützung bei der Systemeinführung
- Implementierung
- Konfiguration

„Schwierig war vor allem die Integration der hoch heterogenen und über verschiedene Subnetze verteilte Serverlandschaft in die einheitliche Verwaltungsplattform und das zu Grunde liegende Benutzerkonzept“, sagt Michael Dümesnil, Projektleiter bei der TWINSOFT.

■ Gute Entscheidungsgründe

Unter den sieben geprüften IdM-Produkten wurden drei für Workshops mit Demo-Installationen ausgewählt. Letztlich machte „Access Master“ von Evidian das Rennen. Michael Dümesnil von TWINSOFT nennt die wichtigsten Gründe, die für diese Lösung den Ausschlag gaben: „Das Produkt passte am besten auf die Prioritäten, die zu Projektstart mit der Deutschen Telekom erarbeitet und festgelegt wurden:

- Der Benutzer muss sein Passwort nur einmal beider Anmeldung an seinem Arbeitsplatz ein geben; weitere Passwörter für die Zielapplikationen oder Server müssen dem Benutzer nicht bekannt sein.
- Die Funktion ist auch für mobile Benutzer gewährleistet.
- Applikationen nach Server Based Computing auf einem Citrix Metaframe Server werden unterstützt“

Und aus Sicht der Deutschen Telekom kommentiert Andreas Brandes dort: „Aus Sicht der Konzernsicherheit ist es wichtig, eine zentrale Stelle zu etablieren, an der die Audit-Informationen über Benutzerlogins, Änderungen an den Berechtigungen usw. gespeichert werden. Außerdem sollte die Lösung sich in den täglichen Betrieb der Serverlandschaft integrieren. Dazu gehört z.B. dass für das Backup der Benutzerdatenbank kein neues Verfahren etabliert werden musste. Technisch ist die Benutzerdatenbank in einer Oracle DB implementiert; davon betreiben wir bereits über 50 Installationen, mit einem bewährten Backup-Verfahren.“