Selbstlernendes Single Sign-On

Zufriedene Nutzer und mehr Effizienz

Foto: pixelio.de

Fast jeder IT-Anwender hat sich schon einmal über ein vergessenes Passwort geärgert. Aber diesen Alptraum muss man sich erst einmal vorstellen: Man arbeitet täglich mit bis zu 15 verschiedenen Anwendungen. In vielen hat man unterschiedliche Benutzernamen, manche so kompliziert wie eine zehnstellige Personalnummer. Regelmäßig muss man die Passworte ändern.

Dies muss natürlich in unterschiedlichen Abständen und ohne dass man ein zuvor schon einmal verwendetes Passwort erneut benutzen darf geschehen. Arbeitet man an etwas anderem, wird man nach einiger Zeit automatisch wieder aus den Anwendungen abgemeldet. Dann ruft ein Kunde an und man muss sich gleichzeitig mit ihm am Telefon erst einmal erneut einloggen.

Problem Passwort-Liste

Für die Mitarbeiter in den Callcentern von T-Mobile gehörte dieses Szenario ebenso zur täglichen Realität wie in praktisch jedem anderen Callcenter der Republik: Um die Anfragen von Kunden kompetent zu bearbeiten, müssen Agenten vom hausinternen CRM-System bis zum externen Track & Trace der Logistikpartner auf eine ganze Reihe von Applikationen zurückgreifen. „Problematisch waren vor allem die Anwendungen, die nur selten benutzt wurden", erinnert sich Eckhard Henkel, Leiter Enterprise Integration bei T-Mobile, der Ende 2004 die Login-Praxis in den Callcentern untersuchen ließ. Da sich deren Passwörter niemand merken konnte, hatte fast jeder Callcenter-Mitarbeiter irgendwo an seinem Schreibtisch eine Passwort-Liste versteckt. Zusätzlich zum Sicherheitsgewinn bewegte am Ende aber auch das Einsparpotenzial durch Single Sign-On T-Mobile zum Handeln.

Im Auftrag von Henkel hatte sich nämlich ein Team mit der Stoppuhr ins Callcenter begeben und akribisch gemessen, wie viel der täglichen Arbeitszeit jeder Agent für das Einloggen in die verschiedenen Anwendungen, den Wechsel von Passwörtern und ähnliche Login-be-

zogene Aufgaben verbrauchte. Das Ergebnis wurde mit den jährlichen Arbeitstagen, der Anzahl der Callcenter-Mitarbeiter – bei T-Mobile immerhin rund 3.000 – und den vom Controlling benannten Kosten pro Callcenter-Arbeitsstunde multipliziert. So ergab sich ein siebenstelliger Betrag pro Jahr. „Damit war der Business Case gefunden, das Projekt würde sich in weniger als einem Jahr alleine über die Produktivitätssteigerungen bezahlt machen", resümiert Henkel.

Der Business Case ist gefunden

Bei diesen Aussichten war die Geschäftsführung um CIO Dr. Steffen Roehn leicht zu überzeugen, zumal das geplante Projekt perfekt in das gerade unternehmensweit angelaufene Wachstums- und Effizienzprogramm „Save for Growth" passte. Anfang 2005 konnte das Projekt mit einer ersten Orientierungsphase beginnen. „Auf eine umfassende Evaluierung aller SSO-Suiten am Markt wurde dabei verzichtet", erläutert Henkel. „Bei verschiedenen anderen Konzernsäulen und im Netzbereich der T-Mobile war nämlich bereits AccessMaster von Evidian im Einsatz und hatte sich dort bestens bewährt."

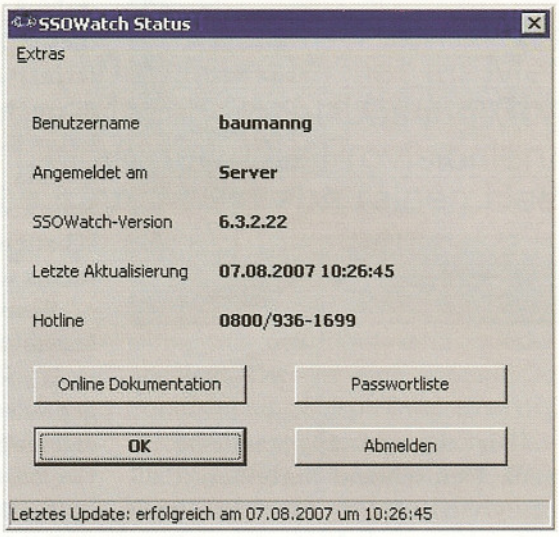

Bild 1: Screenshot Status SSOWatch.

Vor allem war AccessMaster auch die einzige Lösung, die T-Mobile eine Selbstregistrierung von Benutzern zur Verfügung stellte. Bei 3.000 Nutzern mit jeweils zehn oder mehr Benutzerkonten hätte eine manuelle Aufnahme sonst Jahre verschlungen. So fehlte nur noch der passende Dienstleister für die Implementierung. Diesen fand man rasch in der Konzernschwester T-Systems, die gerade offizieller Integrationspartner von Evidian geworden war. Ohnehin sollte diese den späteren Betrieb von Lösung und User Help Desk übernehmen, so dass auch hier die Entscheidung leicht fiel.

Ab dem Frühjahr 2005 erarbeiteten die T-Systems-Consultants zusammen mit den Anwendungsspezialisten von T-Mobile das Be-

Bild 2: Screenshot SSOEngine.

triebskonzept für die SSO-Software. Den wichtigsten Baustein hierzu bildete eine Client-Komponente namens SSOWatch, die auf den Client-Rechnern aller Callcenter-Agenten installiert werden sollte, um dort alle Benutzerinteraktionen zu verfolgen. Erkennt die Software eine Anmeldemaske, fragt sie selbst Benutzernamen und Passwort beim Anwender ab, übergibt diese dann an die Anmeldemaske und trägt sie für die zukünftige Verwendung in ein zentrales Verzeichnis ein. Bei weiteren Anmeldeversuchen für diese Applikation sind die Login-Daten also bereits bekannt und die Anmeldung erfolgt automatisch ohne jedes Zutun des Benutzers.

Single Sign-On: Einer für alle

So entsteht nach und nach ein vollständiges Verzeichnis der Benutzerkonten in sämtlichen verwendeten Anwendungen. Da die SSO-Lösung auch die regelmäßigen Passwort-Wechsel der Anwendungen unterstützt und automatisch durchführt, muss der Nutzer seine verschiedenen Passwörter nicht mehr kennen. Er benötigt nur noch sein Windows-Passwort, mit dem er sich zu Beginn seines Arbeitstages einmalig nacheinander bei Windows und der SSO-Software anmeldet.

Für die auf 19 Standorte in ganz Deutschland verteilten Callcenter-Arbeitsplätze wurden zwei redundant ausgelegte Server-Konfigurationen in den T-Systems-Rechenzentren Münster und Bielefeld eingerichtet. Dort arbeiten ein Administrationsserver, der das zentrale Verzeichnis der Nutzerkonten verwaltet, und zwei Slave-Server, über die sich die Benutzer anmelden. Aus Sicherheitsgründen werden diese Systeme exklusiv für die SSO-Software genutzt.

Im ersten Schritt sollten zunächst 33 Anwendungen angebunden werden, die im Callcenter regelmäßig verwendet wurden – darunter lokale Windows-Applikationen, Anwendungen im internen T-Mobile-Intranet und externe Web-Portale von Geschäftspartnern. Eine der wichtigsten Vorarbeiten war es, die SSO-Lösung auf die Erkennung der verschiedenen Anmelde- und Passwortwechsel-Masken anzulernen. Dabei traten während der heißen Phase der Implementierung unerwartete technische Probleme auf, die sich zwischen T-Mobile und T-Systems nicht mehr lösen ließen. „Da hat der Hersteller wirklich vorbildliches Engagement bewiesen", lobt Henkel. „Als wir nicht mehr anders weiter kamen, ließ Evidian am nächsten Tag die Entwickler aus Paris einfliegen."

Mit eigenem Know-how zum Erfolg

Henkels Team nutzte das Implementierungsprojekt, um sich eigene Kompetenz in den Evidian-Produkten anzueignen. „Wir haben in dieser Zeit wirklich viel dazu gelernt", ist Henkel überzeugt. „Vor allem wissen wir heute, dass Zeit beim Single Sign-On ein kritisches Thema ist. Schließlich haben wir Schnittstellen zu zig Systemen geschaffen, die davon überhaupt nichts wissen.

Wenn sich irgendwo eine Login-Maske ändert, können wir heute in Stunden reagieren und eine angepasste Konfiguration mit einem eigens geschaffenen Verteilungsservice ausrollen."

Als die Lösung im Oktober 2006 in Betrieb ging, waren die Anwender auf Anhieb begeistert. „Unser SSO läuft seit sechs Monaten stabil und ohne jeden Ausfall", freut sich Henkel. „Wir bedienen jetzt über 3.000 Callcenter-Mitarbeiter mit fast 30.000 Benutzerkonten." Dem Engagement von Henkel und seinem Team ist es zu verdanken, dass die Zahl der angebundenen Anwendungen inzwischen auf fast 50 gestiegen ist. „Und wir mussten bei keiner aufwendige Implementierungen einer SSO-Schnittstelle durchführen lassen", betont er.

In Zukunft: mehr

Klar ist bereits, dass auch die Zahl der Anwender rasch weiter steigen wird. Damit diese es in Zukunft noch etwas leichter haben, ist schon die Umstellung auf einen neuen SSOWatch-Client geplant, der auch Java und Firefox unterstützt. Aber für Henkel ist vor allem eines wichtig: „Der Return of Invest ist heute schon erreicht. Mir sind nicht viele Projekte bekannt, die das in so kurzer Zeit tatsächlich geschafft haben."

Michael Ihringer