von Patrick Botz

IBMS NEUES EIM FEATURE UND KERBEROS VEREINFACHEN DIE PRÜFUNG VON ZUGANGSBERECHTIGUNGEN

Künstler Burgy Zapp

Vergraben irgendwo zwischen all den neuen OS/400 V5R2 Hardware- und Partitionierungs-Funktionen findet sich EIM (Enterprise Identity Mapping), eine eigenständige Infrastruktur zur Benutzer-Authentifizierung. EIM ist – in Verbindung mit anderen Technologien – in der Lage, eine Single Sign-On (SSO)-Funktionalität zur Verfügung zu stellen. EIM bietet zusammen mit der Kerberos Authentifizierung SSO-Fähigkeiten über entsprechende Betriebssystem-Schnittstellen. Diese Schnittstellen können auch von Drittanbieter-Anwendungen genutzt werden, um SSO-Fähigkeiten bereitzustellen. Letztlich ermöglicht diese SSO-Funktionalität Entwicklern, ein ODBC-Programm zu schreiben, das auf einer Windows 2000 Plattform läuft und SQL-Anweisungen zur Ausführung übergibt, die Informationen aus Datenbanken auf unterschiedlichen Plattformen abruft ohne dabei interaktive oder hart codierte Benutzer-IDs oder Passworte bereitstellen zu müssen. Das bedeutet, dass ein Endbenutzer über völlig unterschiedliche IDs auf diversen Maschinen verfügen kann, trotzdem aber keine Benutzer-IDs oder Passworte zwischen den Maschinen übertragen werden müssen. Genau genommen benötigen die Benutzer-IDs auf den Server-Plattformen noch nicht einmal Passworte.

In diesem speziellen Szenario sind Entwickler nicht genötigt, in irgendeiner Form Code für die Server-Plattform zu schreiben und dennoch betreibt jede Server-Plattform ihre eigenen, plattformspezifischen Sicherheitsmechanismen zum Schutz der Daten.

Aber EIM umfasst mehr als nur SSO. Die EIM Infrastruktur bietet mit ihrem Design Anwendungsentwicklern die Möglichkeit, heterogene, auf mehrere Plattformen verteilte Anwendungen effizienter und kostengünstiger zu entwickeln, die einfacher als bisher zu schützen und zu administrieren sind.

EIM ist eine der ersten von IBM ausgelieferten eServer- und eLiza- (IBMs Projekt selbstverwaltender Systeme) Funktionen. Die Bereitstellung erfolgte zwar zuerst nur auf der iSeries Plattform aber IBM plant, EIM APIs und ein entsprechendes Schema mit den nächsten Releases der Basis-Betriebsysteme aller eServer-Plattformen bereitzustellen. IBM plant überdies, die Linux-

Implementierung der APIs als open source zur Verfügung zu stellen und somit ISVs die Möglichkeit zu geben, die APIs in ihre Anwendungen einzubauen, ohne dafür eine Gebühr an IBM entrichten zu müssen. Darüber hinaus plant IBM, eine Java-Implementierung der EIM APIs, um damit einen weit verbreiteten Einsatz auf IBM- und Nicht-IBM- Plattformen zu ermöglichen.

Hier soll die EIM Infrastruktur, die SSO-Fähigkeiten, die Verbindung zu OS/400 und IBM Pläne in Richtung Technologie näher erläutert werden. (Wobei hierzu anzumerken ist, dass bei der Erwähnung von IBM Zukunftsplänen diese als aktuelle IBM Planungen verstanden werden sollten, die durchaus Veränderungen unterliegen können, ohne dass dies der Öffentlichkeit explizit bekannt gegeben würde.)

Die Problematik mehrerer Benutzerverzeichnisse

Wir alle verfügen über eine Reihe von Benutzer-IDs und Passworten, die wir innerhalb und außerhalb unseres Unternehmens verwenden. Eine kürzlich angestellte Studie ergab, dass der durchschnittliche Benutzer über 15 Benutzer-IDs und Passworte verfügt. Wir alle wissen, welch „schmerzliche“ Erfahrungen das mit sich bringen kann.

Wie auch immer, das Vorhandensein mehrerer Benutzerverzeichnisse hat auch erhebliche Auswirkungen auf Administratoren und Anbieter von Anwendungslösungen. Administratoren müssen User-IDs und Passworte in diversen unterschiedlichen Benutzerverzeichnissen verwalten (anlegen, verändern oder löschen). Überdies muss oft durch eine Reihe von Mitarbeitern viel Zeit und Mühe investiert werden (meist User Help Desk Funktionen), um die durch UID-/Passwort-Probleme entstandenen Fehlerbedingungen zu bereinigen, Passworte (vergessen) zurückzusetzen und die Synchronisation von Passworten über mehrere Benutzerverzeichnisse vorzunehmen. Überdies müssen, wenn ein Mitarbeiter das Unternehmen verlässt, alle Zugangsberechtigungen in den unterschiedlichen Benutzerverzeichnissen rückgängig gemacht werden – ein fehlerträchtiger Vorgang, der überdies zu Sicherheitslücken führen kann.

Der günstigste Weg zur Umgehung der durch die unterschiedlichen Benutzerverzeichnisse entstehenden Problematiken ist bei Anwendungslösungen, die in einem auf mehrere Plattformen verteilten, heterogenen Umfeld ausgeführt werden sollen, oft die Erstellung eines zusätzlichen Layers, der eine anwendungsspezifische Benutzerregistrierung und eigene Sicherheitsregeln beinhaltet.

Unglücklicherweise beseitigt dieser Lösungsansatz für Benutzer und Administratoren nicht die Verpflichtung zur Pflege mehrerer Benutzerverzeichnisse, sondern erhöht eventuell, je nach Situation, hier den zu treibenden Aufwand zusätzlich.

Einige Produkte zur unternehmensweiten Benutzerverwaltung oder Single Sign On- Produkte haben mit unterschiedlichem Erfolg den Versuch unternommen, eine Lösung für die hier beschriebenen Problematiken der mehrfachen Benutzerregistrierung zu finden. Nach meiner Meinung gibt es bis heute keine Lösung, die wirklich breite Akzeptanz erfahren hat, da niemand bisher in der Lage war, die Belange aller beteiligten Parteien entsprechend zu würdigen.

Produkte zur Benutzerverwaltung auf Unternehmensebene – so wertvoll und nützlich sie in vieler Hinsicht auch sein mögen – lösen die Problematik des Umgangs mit mehreren Benutzerverzeichnissen eigentlich immer nur für den Administrator. Die Benutzer müssen nach wie vor diverse Benutzer-IDs und Passworte wissen und behalten. Die Produkte enthalten keinerlei Funktionalität, die beispielsweise Anwendungsentwicklern das Erstellen heterogener, auf mehrere Plattformen verteilter Lösungen vereinfachen würde.

SSO-Produkte, die auf der Speicherung aller benötigter User-IDs und Passworte und anschließender automatischer „Wiedergabe“ auf dem Weg eines Benutzers von Server zu Server beruhen, können ebenfalls recht nützlich sein. Einerseits werden hier aber nur die Benutzerbelange (Verwaltung mehrerer Benutzerverzeichnisse) abgedeckt, andererseits ergeben sich durch diese Produkte eventuell sogar zusätzliche Sicherheitslücken. Diese Art von Produkten löst das Problem meist durch Speicherung aller Benutzer-IDs und Passworte an einer zentralen Stelle, entweder als Klartext oder in verschlüsselter Form. Wird die verschlüsselte Form gewählt, muss der dazu benötigte Schlüssel irgendwo auf demselben System abgespeichert werden. Das aber bedeutet, dass alle Systemadministratoren mit nur geringfügigem Aufwand in der Lage sind, Kenntnis über sämtliche Passworte zu erhalten. Überdies tendieren SSO-Produkte, die mit Passwort-Wiedergabe arbeiten, dazu, nur in statischen Client/Server-Umgebungen – nicht jedoch in heterogenen, auf mehrere Plattformen verteilten Umgebungen – zuverlässig zu arbeiten.

Als IBM begann, diese Problematik in Angriff zu nehmen, stellte sich heraus, dass alle vorhandenen Ansätze in einem Punkt übereinstimmen: Sie alle versuchen, die Tatsache zu verbergen oder zu ignorieren, dass in Wirklichkeit mehrere Benutzerverzeichnisse existieren. Sie verkünden im Grunde: „Vergessen Sie einfach die Tatsache, dass Sie bereits Benutzer in existierenden Benutzerverzeichnissen definiert haben und dass Sie bereits viele Terabytes an Daten mit den zugehörigen Sicherheitsmechanismen geschützt haben. Verwenden Sie einfach das Benutzerverzeichnis dieses Produktes und Ihre Probleme gehören der Vergangenheit an.“