Wie entkomme ich dem Passwort-Chaos?

Wolfgang Rölz, ORACLE Deutschland GmbH

Immer mehr Applikationen, Systeme und Zugänge, die abgesichert werden müssen, sind eine Herausforderung für Anwender, alle Anmeldedaten und Passwörter präsent haben zu müssen.

Wer hat es nicht schon erlebt: Nach der dritten Falscheingabe der Anmeldedaten wird der Zugriff auf die Applikation gesperrt. Deshalb ist das Thema Single Sign-On aktuell und wird auch immer wichtiger. Single Sign-On entlastet nicht nur den Anwender, sondern reduziert auch Kosten. Auch für die Einhaltung von Regularien kann man Single Sign-On einsetzen.

Anwender haben zu viele Passwörter und Zugänge zu unterschiedlichen Applikationen, Plattformen und Web-Seiten. Sie neigen dazu, diese Daten in einer Datei abzuspeichern oder irgendwo auf Papier zu notieren. Folgende Nachteile ergeben sich:

- Sicherheitslücken
- Einfache Passwörter, die nicht oder selten geändert werden
- Häufige Helpdesk-Anfragen und somit Kosten in der IT sowie eine verminderte Produktivität des Anwenders
- Weitergabe von Passwörtern

Alternativ meldet sich der Anwender einmalig am Arbeitsplatz an und die Single-Sign-On-Technologie übernimmt die Anmeldung zu den weiteren Zugängen. Es entstehen folgende Vorteile:

- Benutzerfreundlichkeit und Akzeptanz der Applikationen steigen
- Höhere Sicherheit durch komplexe Passwort-Richtlinien
- Passwörter werden nicht mehr unsicher gespeichert
- Benutzerfreundlichkeit
- Kostenreduktion durch weniger Helpdesk-Anfragen
- Vereinfachtes Passwort-Management

Oracle Enterprise Single Sign-On

Die Oracle Enterprise Single Sign-On (eSSO) Suite besteht aus fünf integrierten Komponenten, die nach Bedarf zum Einsatz kommen:

- *Oracle eSSO Authentication Manager*
  Mit dem Authentication Manager können zusätzliche starke Authentifizierungsmechanismen wie Smart-Cards und Token eingebunden werden
  Oracle eSSO Password Reset
  Mit Passwort-Reset haben Anwender die Möglichkeit, einen Self-Service-Passwort-Reset durchzuführen, der in der Windows-Anmeldung integriert ist
- *Oracle eSSO Kiosk Manager*
  Der Kiosk Manager erlaubt den schnellen Wechsel und die garantierte Beendigung von Sitzungen bei Arbeitsplätzen, die von mehreren Anwendern gleichzeitig benutzt werden
  Oracle eSSO Provisioning Gateway
  Das Provisioning Gateway ermöglicht die Integration in Provisioning-Systemen, um Anmelde-Informationen zentral zu verwalten
- *Oracle Logon Manager*
  Oracle Logon Manager ist die Hauptanwendung am Arbeitsplatz für Single Sign-On.

In diesem Artikel liegt der Fokus auf Single Sign-On, dafür sind der Logon-Manager der Oracle eSSO Suite und die administrative Konsole notwendig (siehe Abbildung 3). Diese Konsole wird auf den Administratoren-Arbeitsplätzen installiert und übernimmt folgende Funktionen:

- Konfiguration der Zentral-Applikationen für eSSO
- Zentrales Management der Client-Logon-Manager-Konfiguration
- Zentrale Erstellung und Verwaltung von Passwort-Regeln
- Verwaltung der eSSO-relevanten Informationen in einer Datenbank / einem Verzeichnisdienst

Über den Logon-Manager nimmt der Benutzer Anpassungen vor und fügt eigene Anwendungen hinzu. Diese Funktionalität ist in einer typischen eSSO-Implementierung nicht aktiv. Der Logon-Manager wird zentral über die globalen Einstellungen konfiguriert. Mit diesen Einstellungen lässt sich genau steuern, welche Möglichkeiten der Benutzer hat – und welche Anwendungen mit eSSO zur Verfügung stehen. Der Logon-Manager ist als MSI-Datei vorhanden, somit ist ein einfaches Verteilen der Software

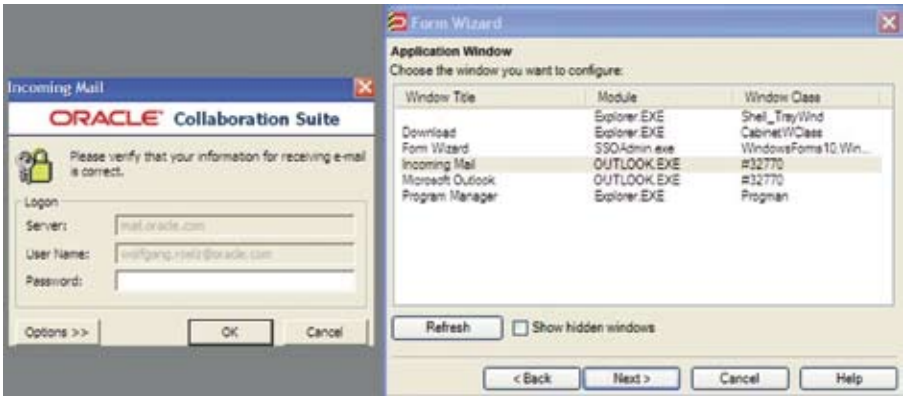

Abbildung 1: Erkennung der Anwendung über den Wizard

möglich. Die Logon-Manager MSI-Datei lässt sich durch Tools wie Orca den individuellen Bedürfnissen entsprechend anpassen und über alle gängigen Desktop-Management-Produkte auf die Arbeitsstationen verteilen.

Funktion

Der Logon-Manager erlaubt es, die Authentifizierungs-Informationen des Anwenders ohne Veränderung der Applikation in die bestehende IT-Landschaft zu integrieren. Alle hinterlegten Authentifizierungs- und Konfigurations-Informationen bezieht der Logon-Manager aus einem Verzeichnisdienst oder einer Datenbank. Folgende Verzeichnisdienste oder Datenbanken unterstützen die Speicherung:

- Microsoft Active Directory 2000, 2003
- Microsoft Active Directory Application Mode 2003 SP1
- IBM Tivoli Directory Server 5.2
- Sun Java System Directory Server 5.1, 5.2
- Oracle Internet Directory 10.1.4.0.1
- Novell eDirectory 8.8 SP1
- Open LDAP Directory Server 2.0.27, 2.2
- Critical Path Directory Server 4.0
- IBM DB2 Database 8.1.6

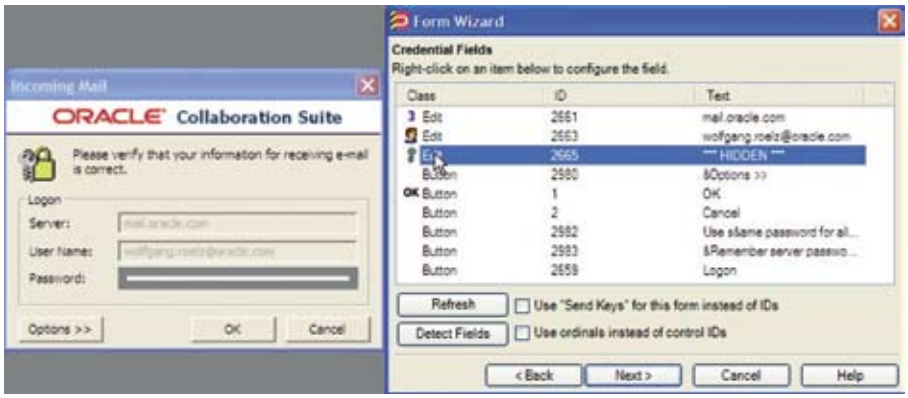

Abbildung 2: Zuweisung der erkannten Felder

- Oracle Database Management System 10*g*
- Microsoft SQL Server 2000

Die Authentifizierungs-Informationen werden beim Start einer Applikation, die eine Authentifizierung benötigt automatisch ohne Benutzer-Interaktion an die Applikation übergeben. Der Logon-Manager unterstützt sogenannte Shared Credentials, das sind Anmelde-Informationen die von mehreren Anwendungen innerhalb einer definierten Anwendungs-Domäne gemeinsam verwendet werden. Falls Anwender mehrere Benutzerkennungen für einzelne Anwendungen haben, können diese auch über den Logon-Manager verwaltet werden.

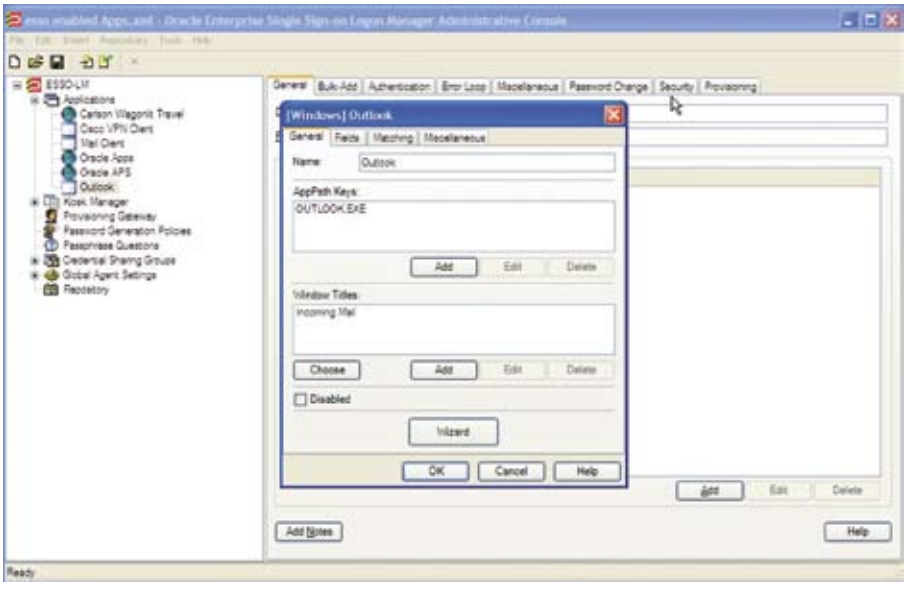

Abbildung 3: Administrative Konsole mit dem neuen Applikationsprofil

Der Logon-Manager bietet zudem eine Offline-Funktionalität, somit kann der Anwender auch Single Sign-On ohne eine Verbindung zum Netzwerk nutzen, die Authentifizierungs-Informationen sind lokal verschlüsselt abgespeichert. Passwort-Änderungen, die durch die Anwendung erzwungen werden, lassen sich mit dem Logon-Manager auf Wunsch nach vorgegebenen Regeln automatisieren. Die Passwort-Änderung findet ohne Benutzer-Interaktion statt. Es sind auch Passwort-Änderungen in Anwendungen möglich, die der Logon-Manager forciert.

Die Oracle eSSO Suite Software ist auf OTN unter http://www.oracle.com/technology/software/products/ias/htdocs/101401.html verfügbar und kann auch lokal ohne Verzeichnisdienst oder Datenbank installiert werden, die Authentifizierungs-Informationen sind lokal verschlüsselt auf der Festplatte gespeichert.

Integration von Windows-Anwendungen

In der administrativen Konsole identifiziert ein Wizard die Anwendung, die in Single Sign-On eingebunden werden soll, in diesem Beispiel Microsoft Outlook (siehe Abbildung 1).

Im nächsten Schritt erhalten die erkannten Felder (diese werden in den meisten Fällen automatisch über „detect Fields“ erkannt) die Bedeutung wie Benutzername, Passwort und andere Felder zugewiesen (siehe Abbildung 2).

Nach der Zuweisung ist das Applikationsprofil für Microsoft Outlook erstellt und kann an den Logon-Ma-

Abbildung 4: Zuweisung der erkannten Felder auf Web-Seiten

nager verteilt werden (siehe Abbildung 3).

Im Logon-Manager wird als nächster Schritt Microsoft Outlook als neue Applikation hinzugefügt. Der Anwender wird zur Eingabe seiner Anmeldeinformationen aufgefordert.

Wenn der Microsoft Outlook Client nun gestartet wird, ist keine weitere Eingabe durch den Anwender nötig. Oracle eSSO erkennt die Felder der Login-Maske und führt das Login automatisch durch. Die neue Anwendung ist nun im Logon-Manager für den Anwender vorhanden und kann immer wieder ohne weitere Eingabe neu gestartet werden.

Integration von Web-Anwendungen

Die Vorgehensweise bei der Integration von Web-Anwendungen ist ähnlich wie bei Windows-Anwendungen; der Hauptunterschied besteht in der Art und Weise der Erkennung der Anmelde-Informationen. Wie in Abbildung 4 dargestellt, wird die Web-Anwendung in der administrativen Konsole gestartet, den erkannten Fenstern werden Benutzername und Passwort zugewiesen, diese werden abgespeichert und an den Logon-Manager verteilt (siehe schmaler roter Rahmen). Analog zur Windows-Anmeldung gibt der Anwender seine Anmelde-Informationen ein. Beim nächsten Start der Anwendung werden die Anmelde-Informationen automatisch übergeben.

Integration von Terminal-Emulatoren

Die Integration von Terminal-Emulatoren findet auch über die administrative Konsole statt, wie im Falle von Telnet (siehe Abbildung 5). Die Zuweisung der Anmelde-Informationen und die Verteilung der Anwendung an den Logon-Manager folgen als nächste Schritte.

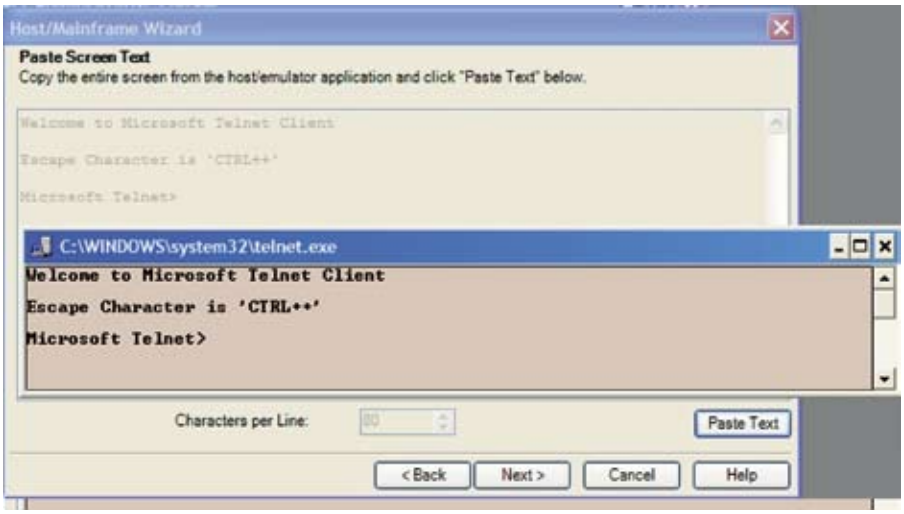

Abbildung 5: Zuweisung der erkannten Felder im Terminal-Fenster

Durch die direkte Integration von Logon-Manager in Terminal-Emulationen kann auf fehleranfällige Integrationsmethoden wie Screen-Scraping verzichtet werden.

Fazit

Das modulare Konzept der eSSO-Suite von Oracle lässt sich leicht in die bestehende Infrastruktur integrieren. Durch die einfache Integration von Anwendungen und durch die Möglichkeit, deklarativ Schritt für Schritt vorzugehen, werden schnell Ergebnisse erzielt. Mit jeder weiteren Anwendung, die in Single Sign-On aufgenommen wird, können weitere Kosten gespart werden – und die Sicherheit steigt. Die Oracle eSSO verzichtet gezielt auf Scripting für die Integration von Anwendungen. Zusätzliche spezielle Hardware wie Appliances ist nicht nötig. Weitere Informationen unter

- Produktseite Enterprise Single Sign- On: www.oracle.com/products/middleware/identity-management/enterprise-single-sign-on.html
- Technische Informationen Oracle Enterprise Single Sign-On: www.oracle.com/technology/products/id_mgmt/esso/index.html

Kontakt:
Wolfgang Rölz
wolfgang.roelz@oracle.com