WebLogic Goes Security

Frank Burkhardt

Quality Technology Solutions GmbH
Nürnberg

Schlüsselworte
WebLogig Server, Forms, Reports, Oracle Accessmanager (OAM), Oracle Internet Directory (OID), Authentication, Authorization, Single Sinn-on (SSO), Identity Management (IDM); Kerberos, Microsoft Active-X Directory, Key Distribution Center

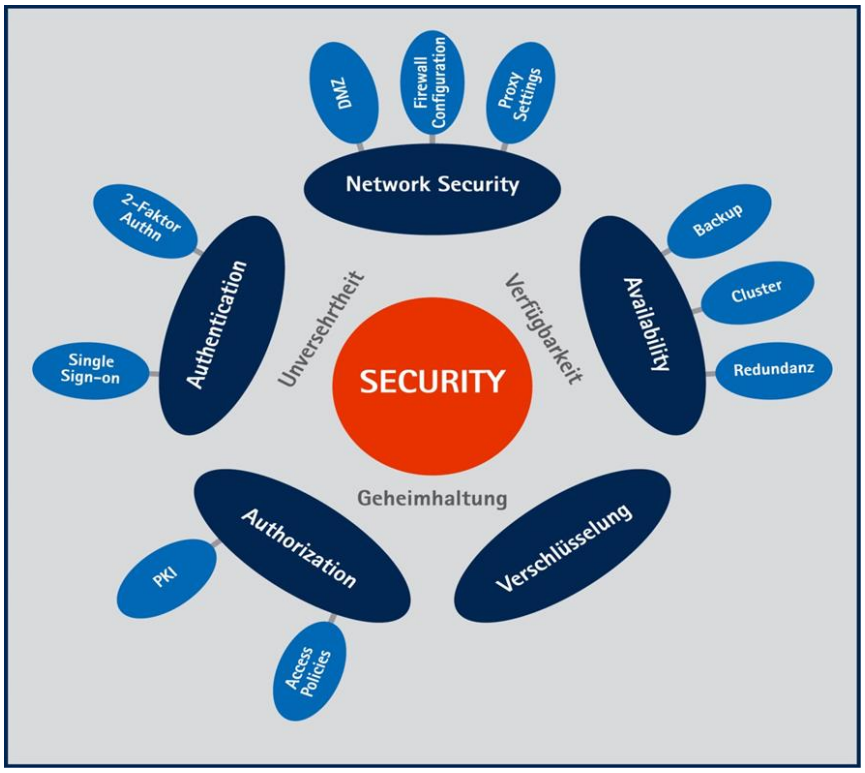
Einleitung
Forms ist in die Tage gekommen, deshalb aber nicht alt. Auch an eine über die Jahre gewachsene Systemarchitektur im Forms-Kontext werden hohe sicherheitsrelevante Anforderungen gestellt. Wie entstehen neue Sicherheitsanforderungen? Was ist bei der Planung und Umsetzung solcher Anforderungen zu beachten und gibt es kritische Aspekte? Nach einer kurzen Beschreibung der Ausgangssituation geht der Referent sehr konkret auf die Herausforderung bei der Projektrealisierung ein und beschreibt die Lösungsansätze von Oracle. Neben Forms und Reports erläutert er dabei die Oracle-Produkte Oracle Access Manager (OAM) und Oracle Internet Directory (OID) näher. Die Definition weiterer Integrationsanforderungen in die bestehende IT-Infrastruktur sprengen bei der Umsetzung die Dokumentationswege und sind nur durch die Erarbeitung eigener Lösungsansätze zu realisieren. Schließlich teilt der Referent gesammelte Erfahrungen, Tipps und Tricks mit der Community. Folgende Themen stehen dabei im Mittelpunkt:

- Wie war die Ausgangssituation
- Authorization / Authentication
- Windows Native Authentication (WNA)
- Wo findet die Rechtevergabe statt
- Welche Lösungsansätze gibt es
- Integration in die bestehende Systemlandschaft
- Microsoft Active Directory (AD)
- Wie entstanden aus dem Projekt weitere Anforderungen

Herausforderungen
IT-Architekturen werden insbesondere im Middleware Bereich immer komplexer. Dies ist auch der Tatsache geschuldet, dass heterogene Systeme in ein Sicherheitskonzept integriert werden müssen. Eine gewachsene Lagacy-Anwendung zur Stammdatenpflege muss ebenso aktuellen Sicherheitsanforderungen genügen, wie neue Software, basierend auf aktuellen Technologien. Die Projektanforderungen entstanden durch die Erweiterung der Systemlandschaft durch ein zusätzliches Softwareprodukt. Eine Lagacy-Anwendung als Stammdatensystem muss für ein neues CRM-System transparent zugänglich gemacht werden so, dass für die Benutzer kein Anmeldedialog mehr erscheint.

IT-Sicherheit / Grundverständnis
Zunächst gilt es den Begriff der IT-Sicherheit genauer zu schärfen um die im Projekt gegebenen Aufgabenstellung richtig einschätzen zu können. IT-Architekturen entwickeln sich immer weiter, was

sich insbesondere im Middleware Bereich durch eine steigende Komplexität wiederspiegelt. Dies ist auch der Tatsache geschuldet, dass auch Altanwendungen und damit heterogene Gesamtsysteme den steigenden Sicherheitsanforderungen genügen müssen. Daraus resultiert eine wachsende Komplexität der gesamten Systemlandschaft. Dem gegenüber steht die Anforderung, alle IT-Systeme zu härten und sicherer zu machen.



Komplexität von IT-Sicherheit
IT-Security ist für verschiedene Aspekte und alle Schichten relevant. Je nach Sicherheitsbedarf entstehen so sehr komplexe Sicherheitssysteme. Sicherheit wird nicht nur durch eine Komponente, z.B. Firewall, realisiert. IT-Sicherheit ist ein systematisches Zusammenspiel aus vielen Komponenten aller relevanten Infrastruktur Layer.
In der Netzwerkarchitektur und damit Netzwerksicherheit eines Unternehmens spiegelt sich bereits der Sicherheitsbedarf wieder, eine demilitarisierte Zone schützt so beispielsweise vor direkten Zugriff auf Applikationsschichten. Perimeter Security Systeme wie Firewalls werden heute häufig noch durch Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS) ergänzt. Bei der Weiterentwicklung der IT-Infrastruktur, besonders der Sicherheitsarchitektur ist es wichtig zu wissen, an welchen Stellen Authorization und Access Control stattfinden. All die bereits bestehenden Funktionen gilt es in einen Lösungsansatz mit einzubeziehen und wo möglich, zu nutzen. Bei der Entwicklung des Lösungsbildes ist es wichtig die vorhandenen und die neuen Technologien genau zu betrachten. Sind Protokolle kompatibel, sind sichere Kommunikationswege im Hinblick auf die bestehende Netzwerkarchitektur möglich und wenn ja, wie? Können beschriebene Zielfunktionen mit bestehenden Tools nicht realisiert werden, muss neue Software gefunden werden. Ziel ist es, die aktuellen, aber auch spätere Anforderungen erfüllen zu können. Es gilt also das bestehende Sicherheitskonzept zukunftsfähig weiter zu entwickeln.

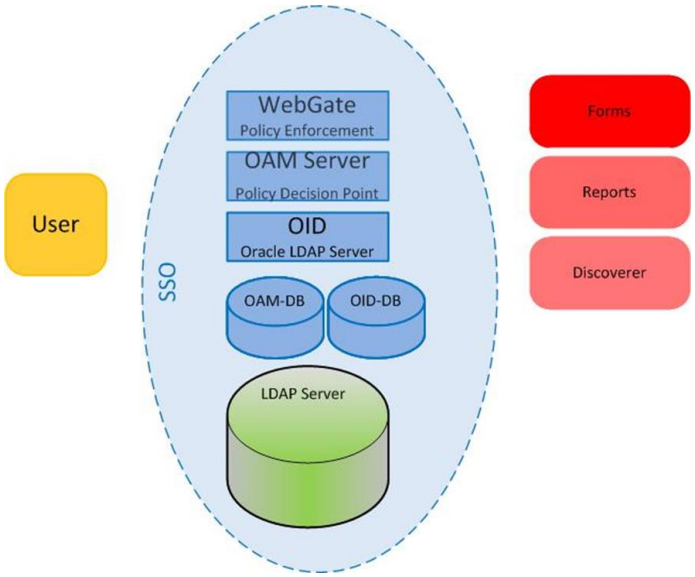
Auch muss bei jeder Weiterentwicklung die Frage nach dem Schutzbedarf der Daten gestellt werden. Der definierte Schutzbedarf bestimmt die Sicherheitsarchitektur.

Arbeitsteiligkeit
Für die Bereitstellung von IT-Infrastruktur sind häufig mehrere Abteilungen beteiligt, die sich in der Regel stringent arbeitsteilig organisieren. Klassisch ist z.B. eine strikte Trennung zwischen Betriebssystem und Middleware Software anzutreffen. Proxy Server und Firewalls werden häufig von Netzwerkadministratoren betreut und das Identity Management System ist in der Regel bei den Windows Administratoren angesiedelt. Schnittstellen werden dadurch häufig schlecht bis nicht besetzt, was zu erheblichen Verzögerungen führen kann. Sicherheitsaspekte bezüglich des fach- oder abteilungsspezifischen Aufgabenbereichs werden berücksichtigt, nicht jedoch als übergreifendes, ganzheitliches Ziel.

Die Konkrete Anforderung
Es soll ein neues CRM-System in die bestehende IT-Infrastruktur integriert werden. Hauptaugenmerk liegt dabei auf den sicheren und transparenten Zugriff auf das Stammdatensystem. Ein erneuter Login-Dialog soll vermieden, das fachliche Berechtigungskonzept darf bei der Umsetzung jedoch nicht verändert werden.

Produktfindung
Welche produktspezifischen Möglichkeiten ergeben sich aus der Kombination von Anforderungen und Infrastrukturgegebenheiten bzw. technischen Voraussetzungen in der bereits bestehenden IT-Infrastruktur. Beim Stammdatensystem handelt es sich um proprietäre Legacy-Software, die es gilt um die oben beschriebene Anforderung zu erweitern. Es müssen also Softwarekomponenten gefunden werden, für die der Hersteller die Kompatibilität und damit den späteren Support gewährleistet. Erschwerend kann hinzukommen, dass Lagacy Anwendungen den technologischen Spielraum erheblich einschränken, weil beispielsweise nur bestimmte Protokolle unterstütz werden.
Aspekte wie Lifecycle Support und Zertifizierung sind grundlegend für Identifizierung von strategischen und nachhaltigen Produkten.
Neue Komponenten dürfen nicht nur den neuen projektspezifischen Anforderungen genügen, sondern müssen auch für die Weiterentwicklung der IT geeignet sein. Weitere Anwendungen, neue und bereits vorhandene Anwendungssysteme sollen bei Bedarf integriert werden können.
Welche Technologien kommen überhaupt für die Erfüllung der Anforderungen in Frage?
Bei der Lösungsfindung müssen auch herstellerspezifische Voraussetzungen berücksichtigt werden, um mit der Lösungsimplementierung weiterhin den Supportstatus zu behalten. Nicht zuletzt muss der Aspekt Lizenzkosten immer mit betrachtet werden, also die Frage nach zusätzlichen Lizenzkosten für neue, oder für die Funktionserweiterung bereits vorhandener Produkte. Dieser Aspekt ist unbedingt detailliert mit den Softwareherstellern schriftlich abzustimmen.
Vor dem Hintergrund all dieser genannten Faktoren sollte immer möglichst die aktuellste Produktversion zum Einsatz kommen.
Bei der Wahl des geeignetsten Access Control Produktes war auch entscheidend, dass es mehrere Authentifizierungstechniken unterstütz. So können nachgelagerte Anforderungen besser umgesetzt werden.

Isoliertes Lösungsbild
Das Lösungsbild besteht aus den identifizierten Produkten und aus der daraus entstehenden Infrastruktur. Entscheidende Kriterien für die Zielarchitektur waren der Schutzbedarf der Daten, die Verfügbarkeitsanforderungen und das bestehende Berechtigungskonzept der Stammdatenanwendung. Aus der beschriebenen funktionalen Anforderung eines transparenten Zugriffs des CRM-Systems auf das Stammdatensystem (Oracle Forms) ergab sich die Anforderung einer Single Sign-on (SSO) Lösung mit Kerberos. Windows Native Authentication (WNA) ermöglicht den Zugriff von einer Softwarekomponente auf die andere, ohne erneute Authentifizierung. Im Rahmen der oben beschriebenen Produktfindung hat sich der Oracle Access Manager (OAM) als bestes Tool für gegebenen Rahmenbedingungen und die definierten Zielsetzungen ergeben. Der OAM beherrscht verschiedene Authentifizierungsmethoden, so auch Kerberos und Web-SSO. Über Plugins kann auch Software von Drittanbietern, z.B. SAP integriert werden. Der OAM als Access Control Instanz – Policy Decission Point und Policy Enforcement Point – bedient sich in diesem Lösungsszenario des Active Directories als Enterprise Directory. Als Besonderheit bei der Integration der Formsanwendung ergibt sich bei diesem Lösungsansatz, dass die Forms Instanz ebenfalls Zugriff auf die Identitäten des Unternehmens haben muss, um die SSO-Funktionalität umzusetzen. Da Forms die Benutzer nur aus einem Oracle Internet Directory (OID) erhalten kann, musste eigens dafür eine OID-Instanz installiert und mit dem AD synchronisiert werden.



Integration in die bestehende IT-Infrastruktur
Die für die Zielerreichung notwendigen zusätzlichen Softwareprodukte sind identifiziert, eine isolierte Architekturschicht erstellt. Wie aber lässt sich dieses Konstrukt in die bestehende IT-Infrastruktur integrieren?
Um das Lösungsbild umsetzen zu können, muss man die bestehende Systemlandschaft verstehen. Für die Nutzung vorhandener Komponenten, wie etwa das AD, ist entscheidend, wie dort die definierte Verfügbarkeit realisiert wurde. Sind die Domain Controller (DC) ausfallsicher und wie sind die redundanten Systeme erreichbar? Welchen Impact hat diese Implementierung auf die projektspezifischen Komponenten?
Betrachtet man sich die Netzwerk Infrastruktur, muss überlegt und mit den betroffenen Stakeholdern abgestimmt werden, wo die neuen, zusätzlichen Systeme verortet werden.

Netzwerkkomponenten, z.B. Firewalls, Proxy Server und IPS-Systeme müssen bei Inbetriebnahme der Lösungsarchitektur unbedingt berücksichtigt werden. Für Kommunikationsstrecken müssen dedizierte Ports freigeschaltet und IPS-Systeme angepasst werden.
Für den GoLive entschied man sich für einen sanften Übergang auf das SSO-System.
Dies war möglich, da das alte und das neue System parallel betrieben werden konnten.
Damit war ein stufenweiser Übergang möglich und es gab die Möglichkeit des Fall Back, wenn SSO-System ganz ausfallen sollte.
Mit der Implementierung der SSO-Funktionalität ergab sich für das gesamte System eine verbesserte Sicherheit. Die Realisierung der beschriebenen Anforderungen konnten durch den Einsatz neuer Funktionen im Middleware Bereich und in der Datenbank umgesetzt werden. Nachdem das Zielbild umgesetzt war, ergaben sich neue Anforderung mit dem Fokus, das bestehende Identity Management im Hinblick auf das Stammdatensystem zu optimieren. Diese Entwicklung zeigt auf, dass IT-Sicherheit kein Zustand, sondern ein dauernder Prozess ist.