Hybrid-Security: Integration Cloud und On-Premises Security

DRAFT: UPDATE NACH OOW

Michael Fischer
ORACLE Deutschland B.V. & Co. KG
München

Schlüsselworte

Identity Management, IAM, IDaaS, Provisionieren, SingleSignOn, Federation, SAML, OAuth.

Einleitung

Mit der zunehmenden Nutzung von Cloud Services stellt sich die Frage wie man die Securityvorgaben oder Best Practices des Unternehmens auch in der Cloud sicherstellt. Dabei spielt es keine Rolle ob man Plattformangebote (IaaS), Services (z.B. DBaaS) oder Entwicklungen (z.B. Container) in der Verantwortung hat. Voraussetzung ist dass das Thema Verantwortung geklärt ist.
Der Vortrag zeigt wie man "nahtlos" OnPremise und Cloud hinsichtlich der Security Mechnismen und Policies integrieren kann. Damit sind es nicht mehr zwei getrennte Welten sondern nur noch verschiedene Betriebsmodelle. Fokus liegt hierbei auf Oracle Datenbankthemen, z.B. Verschlüsselungen als auch auf dem Thema Berechtigungen, Wer darf was wo wann warum. Ergänzt durch das Reporting dass im Rahmen von Audits gefordert wird wie eine Aufstellung Wer hat welche Berechtigungen und Wer hat wann Berechtigungen genehmigt.

Hybrid-Security: Integration Cloud und On-Premises Security

Oracle bietet die Möglichkeit eine zentralistische Sicherheitsinfrastuktur umzusetzen. Zentralistisch erlaubt dabei beide Modelle, physisch oder eine logisch. Die verschiedenen Betriebsmodelle On-Premise, Cloud und Hybrid werden dabei unterstützt. Durch die Unterstützung der jeweiligen Standards an den Schnittstellen ist eine Integration mit non-Oracle Komponenten vorgesehen.

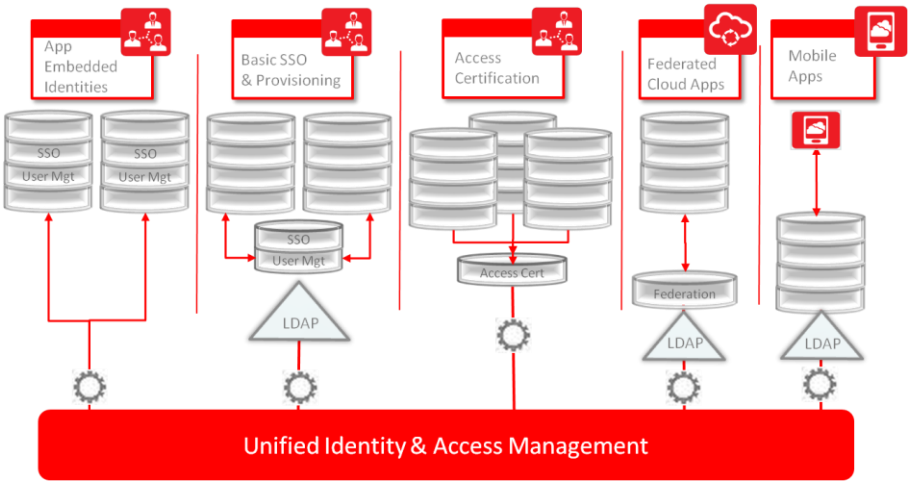

Bild 2: Zentrale Sicherheitsarchitektur (logische Sicht)

Die Komponenten leisten dabei:

- Unified Identity & Access Management:
  Authentifizierung und Authorisierung an Anwendungen inkl. Single Sign On und starker Authentifizierung.
  Provisionierung von Accounts und Berechtigungen über Systeme hinweg
  Nachweis und Reporting Wer hat welche Berechtigungen
  Rezertifizierung der bestehenden Berechtigungen
  Segregation of Duties (SoD) Prüfungen und Durchsetzung oder "Heilung"

- LDAP oder Datenbanken: Benutzerspeicher für Accounts und Berechtigungen als Basis für Anwendungen

- Datenbanken: Verschlüsselte Datenhaltung, Auditierung, SoD

Diese Funktionen werden so auch in der Cloud und für die Cloud bereitgestellt. So ist das Modell eines "hybriden" Identity- und Accessmanagement möglich. Auch eine rein cloud-basierte Lösung wird dadurch möglich.

Beispiel:

a. Neuer Mitarbeiter
   Ein neuer Mitarbeiter tritt ins Unternehmen ein. Er wird zuerst im HR System geführt und erhält zum Eintrittsdatum z.B. einen Arbeitsplatzaccount und Mailadresse. Dieser Account wird durch das (Provisionierungs-)System automatisch angelegt und ihm durch seinen Vorgesetzten übermittelt. Nutzt der Mitarbeiter auch Cloudservices, z.B. ein CRM, wird er ebenfalls dort angelegt (Provisionierung). Da der zweite Account ggf. Zusatzkosten verursacht wird er erst nach zusätzlicher Genehmigung angelegt und durch den Vorgesetzten alle 3 Monate verlängert (Rezertifizierung).
   Der Mitarbeiter meldet sich einmal an seinem Arbeitsplatz an und kommt dann ohne erneute Anmeldung in den Cloudservice (SSO). Ruft er den Cloudservice von ausserhalb des Unternehmens auf so muss er sich um auf Kundendaten zugreifen zu können über ein Einmalpasswort stärker authenitifizieren. Der Mitarbeiter stösst ein Kopieren der Cloud CRM Daten in ein lokales Datawarehouse (BI System) an. Dort werden die Daten beim Einladen verschlüsselt damit sie von Unbefugten (und Schädlingen) nicht gelesen werden können. Diese Verschlüsselung ist auch in etwaigen Backups vorhanden. Datenbankadministratoren können keinen Blick auf diese personenbezogenen Daten werfen, diese Berechtigung könnten Ihnen nur ein Fachadministrator erteilen. Der Mitarbeiter kann im Datawarehouse (BI System) nur die Daten sehen für die er freigeschaltet wurde. Diese Freischaltung über verschiedene Systeme hinweg wurde durch die Provisionierung umgesetzt.

b. Neuer Kunde
   Ein neuer Kunde findet auf dem Portal oder der App des Unternehmes nützliche Angebote für die er sich, um diese weiter nutzen zu können, registriert. Dazu gibt er nur seinen google oder facebook Account an, da er nicht noch einen Account anlegen will. Später bei kostenpflichtigen Angeboten würde die Registrierung fortgesetzt. Da das Unternehmen weitere neue Apps entwickelt hat, z.B. auf Basis eines anderen Cloudproviders, wird dies dem Kunden beim nächsten Login mitgeteilt oder per email geschickt. Die Kundendaten werden

durch die Provisionierung auch dorthin verteilt und geeignete bereitgestellte SSO Mechnismen ermöglichen dem Kunden die Nutzung ohne weiteres Login oder Registrierung. Die Kundendaten sind sowohl beim Cloudprovider 1 und 2 verschlüsselt. Der Kunde hat die Möglichkeit zu steuern wer welche seiner Daten sehen kann (z.B. Emailweitergabe an das Unternehmen oder nicht).

c. Neue (externe) Anwendung oder App
   Das Unternehmen vergibt die Entwicklung einer Anwendung oder mobile App an eine externe Agentur, die auch das Hosting für die Pilotphase übernehmen soll. Nach dem Erfolg will man sich über die künftige Plattform Gedanken machen. Die Anwendung nutzt für Selbstregistrierung und Kundendaten bereitgestellte Service die entweder remote (rest oder nativ) genutzt werden oder inkl. der Serviceschnittstelle (rest, soap) als ablaufbare Module/Container bereitgestellt wurden. Damit ist die Basis für Kundendaten/-verwaltung, Authentifizierung, Authorisierung, Audit vorhanden und muss nicht später mit Aufwand überführt werden.

Wie kann eine vorhandene IT überführt werden?

Fall On-Premise:

Anwendungen die schon vorhanden sind haben in der Regel ein eigenes Benutzermanagement und eine eigene Anmeldung. Nicht wenige Unternehmen haben daher aus verschiedensten Gründen mehrere Directory Server, Access Management oder sogar Provisionierungslösungen unterschiedlicher Hersteller im Einsatz. Sinnvoll ist zu Anfang eine Bestandsaufnahme um herauszufinden für welche Systeme sich eine Integration lohnt (Kosten/Nutzen, Kritikalität). Ein zentralisierter Ansatz kann von zwei Seiten vorgehen, Integration in das zentrale Berechtigungsmanagement um eine Provisionierung über Systeme hinweg zu ermöglichen. Damit erreicht man die sofortige Durchsetzung von geänderten Rahmenbedingungen wie z.B. Deaktivierung bei Verlassen des Unternehmens oder Abteilungswechsel. Die Nachweise für Auditing sind damit auch vorhanden (wer hat wann welche Berechtigung, wer hat genehmigt etc) und die Möglichkeit einer Rezertifizierung wird bereitgestellt (Verlängerung von Berechtigungen).
Der zweite Ansatz ermöglicht den Nutzern mit einer einmaligen Anmeldung nahtlosen Zugriff zu den Systemen (SSO) zu erhalten. Aus Unternehmensgesichtspunkt können damit Problemfälle mit notierten Passwörtern, zu einfachen Passwörtern oder zu schwacher Anmeldeverfahren gelöst werden.

Für beide Fälle sind die Komponenten mit ensprechenden Konnektoren ausgestattet und setzen Standardprotokolle um so dass eine Integration begrenzt aufwendig wird.

Diese Komponenten können dabei sowohl On-Premise als auch in der Cloud laufen.

Oracle bietet hierzu:

- Datenhaltung: Verschlüsselung, Gewaltentrennung, Audit
- Identitäten und Accounts: Provisionierung, Workflows, Rezertifizeirung, SoD, Audit
- Zugriff: (starke) Authentifizierung, Authorisierung, Kontextbasierend, Accesslogs

Fall Cloudbasiert

Für die cloudbasierten Systeme treffen die oben angegebenen Ansätze ebenfalls zu. Technisch gesehen sind lediglich die verwendeten Protokolle verschieden. Beim SSO kommt typischerweise SAML oder OAuth zum tragen, bei der Provisionierung REST Schnittstelle an der Cloud API.
Die im vorangegangenen Abschnitt aufgeführten Komponenten unterstützen direkt oder integrativ die verschiedenen Betriebsmodelle OnPremise, Cloud, Cloud-On-Premise (Cloud @ Customer) und Hybrid. Hier kann ein umfassender Schutz im Rahmen einer zentralen IT Sicherheit abgebildet werden.

Abbildung: Oracle Betriebsmodelle

Im Idealfall ist die IT Sicherheitsarchitektur für OnPremise und Cloud identisch. Dies ist erreichbar durch Einsatz gleicher Komponenten, die dann die gleichen Security Massnahmen umsetzen. Sind die Komponenten verschieden, so kommen Schnittstellen bzw. Best Practices auf Standards basierend zum Einsatz die von beiden Welten unterstützt werden. Eine zentrale Architektur ermöglicht die einfachere Durchsetzung und Überprüfung der Richtlinien.

Beispiel für gleiche Komponenten sind Verschlüsselung und Management der Keys die lokal zentral erfolgen kann, die Umsetzung der Gewaltentrennung in der Datenbank oder die zentrale Aggregation der Audit-logs. Identity Management und Enterprise Manager können beide Umgebungen verwalten (Policies, Berechtigungen).

Für diejenigen die die Cloud im eigenen Rechenzentrum haben wollen oder müssen bietet Oracle mit „Cloud@Customer“ eine Appliance (Hardware und Software) an. Es handelt sich dabei um ein Abbild der Oracle Public Cloud mit einer Auswahl der IaaS und PaaS Services. Vorteile neben der "fertigen" Cloud Appliance ist das flexible abonnement-basierte Lizenzmodell aus der Oracle Public Cloud und das enthaltene Management der Appliance. Beim Management partizipieren an der gleichen Erfahrung, Servicequalität und den neuesten Innovationen und Updates die die Oracle Cloud kennzeichnen.

Zusammenfassung
Oracle bietet einen konzeptionellen Ansatz zur Umsetzung der IT Datensicherheit und umfassende Komponenten zur Umsetzung. In Oracle Produkten und Oracle Cloud Services wird sowohl der Ansatz (End-to-End Security/Defense in Depth) als auch die Komponenten selbst (wie Access Management für Single Sign on in Anwendungen) verwendet. Kernpunkte der IT Datensicherheit dabei sind:

- Schutz jeder Schicht (protect every layer)
- Schutz beginnt so "tief" wie möglich (push down security the stack)
- Schutz im Standard (security should always be on)
- Eine übergreifende IT Securityarchitektur über Systeme und Cloud hinweg
- Wahlmöglichkeit der Ablaufumgebung der Komponenten die Security nutzen: OnPremise, Cloud, Cloud@Customer, Hybrid

Kontaktadresse:

Michael Fischer

ORACLE Deutschland B.V. & Co. KG

Riesstr. 25

D- 80992 München

Telefon: +49 (0) 172 8323654

E-Mail michael.fischer@oracle.com

Internet: www.oracle.de