# Sichere Oracle-Datenbanken in der Cloud

Stefan Oehrli, Trivadis AG

Datenschutz, Sicherheit und Cloud Computing sind heiß diskutierte Themen mit vielen unterschiedlichen Meinungen und Standpunkten. Unabhängig vom jeweiligen Standpunkt wird in der Regel bei einfachen Standard-Dienstleistungen eher eine Cloud-basierte Lösung in Betracht gezogen. Doch wie sieht dies bei Datenbanken aus?

Datenbanken enthalten häufig kritische oder teilweise sensitive Daten. Lassen sich diese Datenbanken so ohne Weiteres sicher in einer Cloud-Umgebung betreiben? Welche Herausforderungen stellen sich bei Datenbanken in der Cloud? Was für Überlegungen gehören neben dem reinen Entscheid zugunsten von Feature und Optionen sonst noch dazu? Dieser Artikel beleuchtet diese Fragen und zeigt weitere Aspekte von Cloud-basierten Oracle-Datenbanken auf.

## Grundlagen

Unabhängig vom Speicherort sind Daten im Allgemeinen und Datenbanken im Speziellen unterschiedlichen Risiken ausgesetzt. Diebstahl, Verlust oder unerlaubte Manipulation der Daten können weitreichende Konsequenzen für ein Unternehmen und dessen Geschäft haben. Neben finanziellem Schaden, Image-Verlust, strafrechtlichen Folgen oder gar Existenzbedrohung stehen auch die Interessen der Mitarbeiter und Kunden im Mittelpunkt. Zudem werden die Herausforderungen für die Umsetzung von Cloud-Projekten mit der neuen europäischen Datenschutz-Grundverordnung (EU-DSGVO), die ab Mai 2018 in Kraft tritt, nicht abnehmen. Nichtsdestotrotz bietet eine europaweite, einheitliche Datenschutzregelung Chancen, die es zu nutzen gilt.

Ob On-Premise oder in der Cloud, Oracle-Datenbanken funktionieren technisch im Prinzip in beiden Umgebungen gleich. Für ihren Betrieb braucht es einen Server mit CPU, Memory und Speichersystem genauso wie Netzwerk- und weitere Infrastruktur-Komponenten für die Interaktion beziehungsweise den Zugriff auf die Daten.

Der wesentliche Unterschied bei Cloud-basierten Datenbank-Systemen ist ihr Standort. Diese Datenbanken und die entsprechenden Server stehen eben nicht mehr im Haus, im Gegensatz zu On-Premise-Systemen, bei denen die verschiedenen Infrastruktur-Komponenten, Standorte sowie die entsprechenden Administratoren bekannt sind.

Obwohl man heutzutage in größeren Unternehmen nicht mehr einfach im Rechenzentrum oder bei den Administratoren-Teams vorbeigehen kann, besteht doch eine definierte rechtliche Beziehung sowie eine Vertrauensbasis zwischen den Unternehmen und ihren Mitarbeitern. Sobald aber einzelne Dienste oder ganze Infrastruktur-Komponenten durch IT-Dienstleister betrieben werden, nimmt die Komplexität zu. Die rechtlichen Aspekte zwischen den beteiligten Parteien werden mit Dienstleistungsverträgen festgehalten. Das bedeutet nicht zwangsläufig, dass ein Unternehmen allen Mitarbeitern eines Dienstleisters das gleiche Vertrauen entgegenbringt wie den eigenen Mitarbeitern.

Geht man einen Schritt weiter und betreibt Datenbanken komplett in einer Cloud, sind viele Faktoren nicht mehr transparent. Einmal kurz dem Datenbank-Administrator auf die Schulter klopfen oder beim Datenbank-Server im Rechenzentrum vorbeigehen, ist nicht mehr möglich. Man gibt seine Daten beziehungsweise Datenbanken aus der Hand, ohne dass man mit absoluter Sicherheit sagen kann, wo die Daten sind und wer effektiv alles darauf Zugriff hat. Für Unternehmen ergeben sich daraus konkrete Fragen, die im Gegensatz zu On-Premise-Systemen bei Cloud-basierten Datenbanken zwingend zu klären sind. Dazu gehören:

- Welche Daten sind schützenswert, personenbezogen oder sensitiv?
- Sind davon ganze Datenbanken oder nur einzelne Datensätze/Tabellen betroffen?
- Welche Risiken/Angriffsvektoren bestehen für eine bestimmte Datenbank?
- Welcher Schaden kann entstehen (direkte Geschäftsschädigung, Imageverlust etc.)
- Wie lassen sich diese Risiken durch technische Maßnahmen verringern?
- Stimmt neben dem Preis, den Services und den vertraglichen Rahmenbedingungen auch das Vertrauen zum Cloud-Anbieter?

Speziell der letztgenannte Punkt spielt eine nicht zu vernachlässigende Rolle bei der Wahl eines geeigneten Cloud-Anbieters.

## Angriffsvektoren

Bei On-Premise-Datenbanken werden die Angriffsvektoren häufig vernachlässigt oder spielen nur eine untergeordnete Rolle. Aussagen wie „ist ja nur intern", „brauchen wir nicht", „da sehen nur die Administratoren alles" etc. sind in diesem Zusammenhang nicht selten.

Oft wird auch die Verantwortung für die Sicherheit auf andere Systeme wie Firewalls, Gateways und Proxys verschoben. Jedoch wäre es naiv anzunehmen, dass dies ausreiche. Bei komplexen IT-Architekturen, wie wir sie heute vorfinden, kann man sich nicht auf einzelne Systeme verlassen. Zudem kommen die Gefahren nicht zwingend immer von außerhalb, sondern häufig aus den eigenen Reihen.

*Abbildung 1* zeigt schematisch das Umfeld einer Datenbank und mögliche Angriffsvektoren. Ein Hacker kann von außen versuchen, in Systeme einzudringen und Daten abzuziehen. Doch wie angemerkt, geschieht dies häufig direkt innerhalb eines Unternehmens. Es gab in der Vergangenheit immer wieder bekannte Vorfälle, bei denen einzelne Datensätze oder ganze Datensammlungen durch Mitarbeiter abgezogen und weitergegeben wurden. Bei Cloud-basierten Datenbanken kommen dafür nicht nur die Mitarbeiter eines Unternehmens infrage,

sondern eben auch die Mitarbeiter und Administratoren der beteiligten Dienstleister und Cloud-Anbieter.

Damit sollen jedoch nicht alle Administratoren unter Generalverdacht gestellt, sondern vielmehr die Risiken und Herausforderungen, aber auch Chancen im Datenbank-Umfeld angesprochen werden. Bei Datenbanken spricht man üblicherweise von folgenden Top-10-Gefahren, die es zu bewältigen gilt. Dabei handelt es sich um eine Zusammenfassung aus unterschiedlichen Quellen wie dem Verizon Data Breach Report, Imperva White Paper sowie weiteren Quellen. Die effektive Reihenfolge und Zusammenstellung der zehn Gefahren variieren dabei je nach Quelle und Jahr:

1. Exzessive und nicht benötigte User-Berechtigungen
2. Missbrauch von Rechten
3. Input Injection/SQL-Injection
4. Malware
5. Schwaches Audit
6. Offenlegung/Zugang zum Speichermedium
7. Schwachstellen und Fehlkonfiguration
8. Nicht überwachte, sensitive Daten
9. Denial of Service
10. Unzureichendes Sicherheitsfachwissen

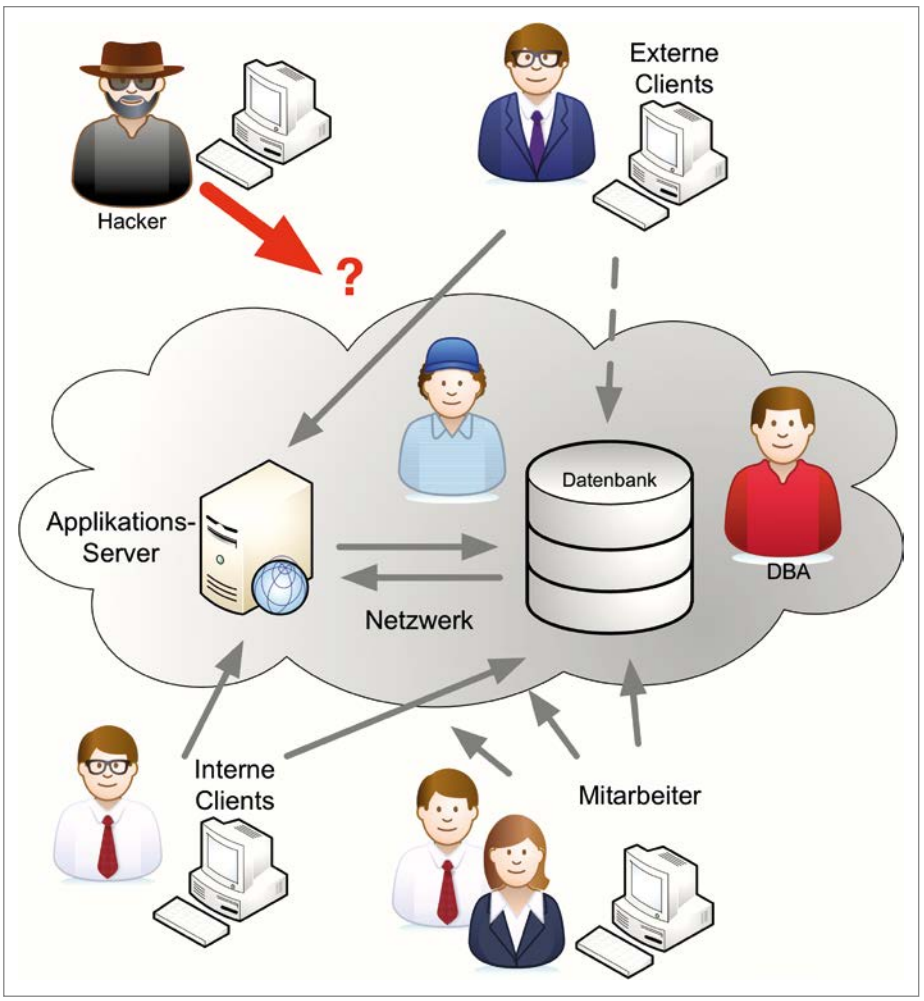


*Abbildung 1: Angriffsvektoren*

Viele der aufgeführten Gefahren lassen sich bereits mit wenigen, einfachen Maßnahmen reduzieren. Bei anderen wie dem Zugang zum Speichermedium braucht es umfassendere Aktivitäten, die zwangsläufig auch zu höheren Kosten führen. Im Grundsatz treffen diese Gefahren sowohl bei On-Premise-Systemen als auch bei Cloud-basierten Systemen zu. Es braucht daher zwingend ein geeignetes Sicherheitskonzept, das beide Arten von Datenbank-Umgebungen berücksichtigt.

Allerdings sind nicht alle Systeme beziehungsweise Daten gleich kritisch. Aus diesem Grund ist es nicht sinnvoll, alle Datenbanken gleich umfassend zu schützen.

Mit einer Risiko-Analyse können die Gefahren und Risiken für ein bestimmtes Umfeld festgelegt werden. Dazu gehört, dass der Daten-Eigentümer und der Applikationsverantwortliche die Sensitivität ihrer Daten kennen beziehungsweise definieren. Im Anschluss daran sind die Daten zu klassifizieren und einer entsprechenden Schutzklasse zuzuweisen. Für die unterschiedlichen Schutzklassen können dann verschiedene administrative sowie technische Maßnahmen für den Schutz der Daten definiert werden. Sinnvollerweise werden nicht zu viele unterschiedliche Schutzklassen gewählt. Für Datenbanken bieten sich folgende vier Schutzklassen an:

- *Öffentliche Daten*
  Sind im Internet oder an anderen Stellen öffentlich verfügbar – dürfen dort aber sicherlich nicht manipuliert werden

- *Interne Daten*
  Dürfen von allen Mitarbeitern eingesehen werden

- *Vertrauliche Daten*
  Dürfen nur von einem definierten Kreis von Mitarbeitern eingesehen werden

- *Geheime Daten*
  Stehen nur einem kleinen Kreis von Mitarbeitern zur Verfügung – wenn sie verloren gehen, ist die Existenz einer Unternehmung gefährdet

Können On-Premise noch Datenbanken aller Sicherheitsklassen betrieben werden, gibt es bei Cloud-basierten Datenbanken zwangsläufig gewisse Einschränkungen. So werden als „geheim" klassifizierte Systeme wohl primär lokal betrieben. In der Regel ist in einem Unternehmen der Großteil der Datenbanken als „intern" oder „vertraulich" klassifiziert. Dementsprechend ist Potenzial vorhanden, Datenbanken mit einer Cloud-basierten Lösung zu betreiben. Wie viel Sicherheit im Einzelnen für jede Schutzklasse benötigt wird, hängt immer stark von den effektiven Daten sowie allfälligen Compliance-Auflagen ab.

## Identity und Access Management

Unabhängig davon, welche Maßnahmen zur Verbesserung der Datensicherheit

getroffen werden, spielen die Authentifizierung und Autorisierung eine zentrale Rolle. Arbeiten die Benutzer mit unzureichend starken Passwörtern oder gibt es zu viele und zu hohen Rechte, bringen weitere Maßnahmen wie die Verschlüsselung nur bedingt etwas. Neben einer System- und Datenbank-Härtung braucht es eine gute Basis; also eine sichere Grundkonfiguration der Datenbank basierend auf Best Practices sowie ein geeignetes Benutzer- und Rollenkonzept.

Identity und Access Management (IAM) geht einen Schritt weiter. Der Fokus liegt nicht primär bei einer einzelnen Datenbank, sondern deckt mehrere Aspekte und Systeme ab. Mit Oracle Enterprise User Security und Oracle Unified Directory lassen sich Benutzer und Rollen zentral in einem Verzeichnis verwalten und somit in mehrere Datenbanken und Systeme benutzen. Die Integration in ein unternehmensweites IAM erhöht die Sicherheit; zudem ergeben sich Chancen, einheitliche und unternehmensweite Workflows zu implementieren.

## Verschlüsselung und Key Management

Auch wenn die Benutzer- und Rechteverwaltung korrekt gelöst und entsprechend umgesetzt wurde, besteht die Gefahr, dass Unbefugte direkten Zugriff auf die Daten erhalten, sei dies auf dem Transportweg vom Client zur Datenbank oder direkt auf dem Datenbank- oder Storage-Server. Dementsprechend gilt es, kritische Daten mit entsprechender Verschlüsselung zu schützen.

Oracle bietet ohne zusätzliche Kosten den Schutz des Transports („data in motion") mit der nativen Netzwerk- oder SSL/TLS-Verschlüsselung. Beide Verfahren bieten auf einfache Weise das Verschlüsseln der Netzwerk-Pakete auf dem Weg von und zum Datenbank-Server. Im Gegensatz zu SSL/TLS ist die native Netzwerk-Verschlüsselung einfacher zu konfigurieren und schneller ausgerollt. Wohingegen bei SSL/TLS zusätzlich eine Integritätsprüfung erfolgt und bei Bedarf die Client-Authentifizierung sichergestellt wird. Letzteres bedingt jedoch eine entsprechende Public-Key-Infrastruktur im Unternehmen.

Bei Cloud-basierten Lösungen ist zudem die Verschlüsselung der Daten am Speicherort ein wesentliches Kriterium („data on rest"). Oracle bietet mit Oracle Advanced Security die entsprechende Option. Mit Transparent Data Encryption (TDE) lassen sich einzelne Spalten sowie ganze Tablespaces verschlüsseln. Seit Oracle 12*c* R2 geht dies auch für die ganze Datenbank inklusive „SYSTEM"- und „SYSAUX"-Tablespaces. TDE benötigt für die Verschlüsselung jeweils einen Master-Key, der in einem lokalen Software-Keystore beziehungsweise Wallet abgelegt ist. Ist der Software-Keystore bei Cloud-Datenbanken ebenfalls in der Cloud abgelegt, liegt der Schlüssel für die verschlüsselten Daten direkt bei den Daten. Dies gilt es durch eine On-Premise-Key-Verwaltung zu vermeiden, entweder durch ein Hardware-Security-Modul (HSM) oder mit Oracle Key Vault.

Unglücklicherweise schützt TDE nur vor Zugriffen von außen, wenn also jemand direkt auf Datafiles, Backups etc. zugreift. Hat ein Administrator Zugriff via SQL*Plus, kann er die Daten mit hohen System-Privilegien lesen. Um dies einzuschränken, braucht es im Oracle-Umfeld zwingend ein Database Vault. Damit werden die Trennung der Verantwortlichkeit forciert und Systemprivilegien eingeschränkt.

## Datenbank-Audit und Security-Monitoring

Der aktive Schutz der Datenbank ist nur ein Teil. Ein weiterer Punkt ist die Überwachung beziehungsweise das Auditing der Oracle-Datenbank. Beim Auditing geht es in erster Linie darum festzustellen, ob jemand unerlaubt auf Daten zugreift oder diese manipuliert. Zudem ist die Nachvollziehbarkeit sichergestellt. Mit Unified Auditing und Audit Policies lassen sich entsprechende Regeln zur Überwachung von DDL- und DML-Statements definieren.

Mit Fine Grained Auditing (FGA) bietet Oracle zudem die Funktionalität, Audit-Events feingranular zu definieren. So kann etwa eine Abfrage nur auditiert werden, wenn jemand die Salär-Spalte abfragt, in der das Gehalt mehr als 10.000 pro Monat beträgt. Andere Abfragen generieren keinen Audit-Eintrag.

Unified Auditing, Fine Grained Auditing etc. protokollieren die Audit-Events grundsätzlich immer in einem lokalen Audit-Trail. Damit die Audit-Events zentral verwaltet


**Spiegelung kompletter System-umgebungen**

**Libelle Business*Shadow*®**

Unabhängig bezüglich
- ☑ Fehlerursache
- ☑ Entfernung
- ☑ Hardware / Architektur
- ☑ Komplexer Systeme

Schnelle Arbeitsaufnahme
- ☑ Mit konsistenten Daten
- ☑ Auf Knopfdruck
- ☑ Automatisiert
- ☑ ...

**Hans-Joachim Krüger**
Chief Technology Officer
Libelle AG

**Erfahren Sie mehr:**
**www.Libelle.com/business**

ORACLE Gold Partner

Libelle

**Libelle AG**
Gewerbestr. 42 • 70565 Stuttgart, Germany
T +49 711 / 78335-0 • F +49 711 / 78335-148
www.Libelle.com • sales@libelle.com

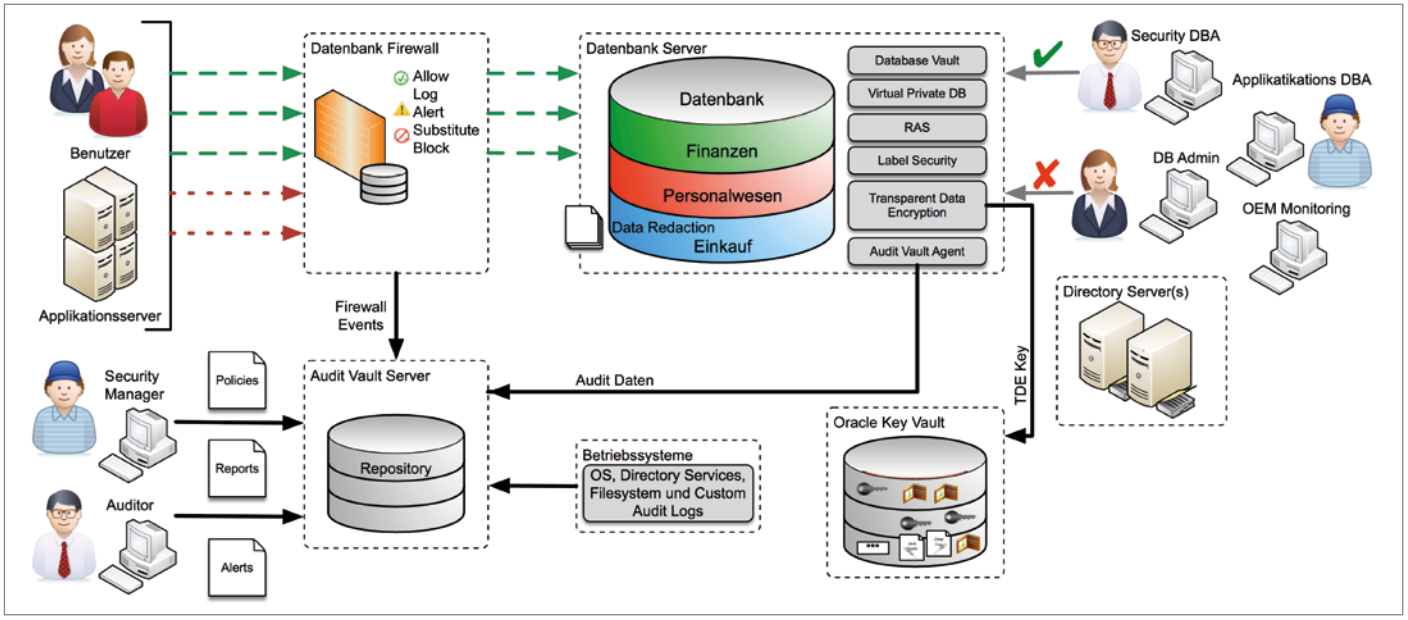


*Abbildung 2: Die Maximum-Data-Security-Architektur*

und entsprechend ausgewertet werden können, bietet Oracle mit Oracle Audit Vault and Database Firewall ein dediziertes Produkt. Damit werden alle Audit- und Firewall-Events in einem zentralen Repository abgelegt. Zudem wird so das Risiko minimiert, dass Audit-Events auf dem Datenbank-Server manipuliert werden.

## Maximum-Data-Security-Architektur

Werden alle möglichen Oracle-Security-Features und Optionen zusammen eingesetzt, lässt sich eine Maximum-Data-Security-Architektur aufbauen *(siehe Abbildung 2)*. Vom Prinzip her entspricht diese Architektur einer Zwiebel. Im Zentrum stehen die sensitiven Daten. Diese lassen sich dann Schicht für Schicht mit aktiven oder passiven Maßnahmen schützen. Dazu gehören:

- *Härtung der Datenbanken*
  Umsetzen von Security-Best-Practices, Einschränkung kritischer „init.ora"-Parameter, Betriebssystem-Zugriffe etc.

- *Authentifizierung und Autorisierung*
  Umfassendes Benutzer- und Rollenkonzept nach dem „Least Privilege"-Prinzip. Den Benutzern werden nur so viele Rechte wie nötig vergeben, damit sie ihre Aufgaben erledigen können, also kein „SELECT ANY TABLE".

- *Row-Level-Security*
  Einschränkung der Daten durch Virtual Private Database (VPD) und/oder Real Application Security (RAS). Ein Benutzer sieht also nur die für ihn relevanten Informationen.

- *Segregation of Duties und Database Vault*
  Zusätzlicher Schutz von kritischen Daten durch den Einsatz von Oracle Database Vault und Oracle Label Security. Mit der Definition von Realms, Rules und Command Rules lässt sich der Zugriff feingranular definieren. Zudem wird mit Database Vault eine Trennung der Verantwortlichkeiten explizit forciert. Kritische System-Privilegien sind eingeschränkt, so funktionieren etwa alle „ANY"-Privilegien oder „ALTER USER" nur noch für den eigenen Account.

- *Starke Authentifizierung und Enterprise User Security*
  Verwendung von starker Authentifizierung mit Kerberos oder SSL sowie dem Einsatz von Enterprise User Security zur externen Benutzer- und Rollenverwaltung. Benutzer und Rollen werden nicht mehr dezentral in jeder Datenbank verwaltet, sondern zentral in einem Oracle-Verzeichnis, etwa dem Oracle Unified Directory.

- *Transport-Verschlüsselung*
  Zur Verschlüsselung des Netzwerk-Verkehrs von/zur Datenbank mit der nativen Netzwerk-Verschlüsselung oder SSL/TLS.

- *Verschlüsselung der Daten*
  Verschlüsselung der ruhenden Daten mit Oracle Advanced Security und Transparent Data Encryption (TDE), wobei hier die Master-Keys beziehungsweise Oracle-Wallets außerhalb der Datenbank oder außerhalb der Cloud-Umgebung in einem zentralen Hardware-Security-Modul oder Oracle Key Vault verwaltet werden.

- *Auditing*
  Überwachung der Zugriffe mit Audit Policies, Fine Grained Audit etc. in Kombination mit dem Betriebssystem-Auditing.

- *Alerting*

- *Datenbank-Firewall*
  Überwachung der einzelnen Zugriffe mit einer Firewall, wobei kritische Abfragen direkt blockiert werden und/oder Events erzeugen.

- *Zentrale Auswertung*
  Zentrale Sammlung und Auswertung der Audit-Daten und Firewall Events mit Oracle Audit Vault and Database Firewall.

- *Testdaten-Management*
  Maskierung und Anonymisierung von Testdaten durch Oracle DataMasking.

Je nach gewählter Sicherheitsklasse sind die Daten durch mehr oder weniger Zwiebelschalen geschützt. Somit lassen sich der betriebliche Aufwand wie auch die Kosten moderat halten. Benötigte Features und Optionen werden nur dort eingesetzt, wo sie auch zwingend nötig sind.

## Die Alternativen

Bisher wurden primär Oracle-Features und -Optionen angesprochen. Selbstverständlich lassen sich viele der Maßnahmen teilweise oder ganz durch Produkte von Drittanbietern umsetzen. Speziell bei Cloud-basierten Systemen bieten sich Alternativen an, die bei einem spezifischen Anwendungsfall einfacher umzusetzen sind als eine rein Oracle-basierte Lösung. Als typisches Beispiel gilt die Verschlüsselung. Damit Oracle-Datenbanken sicher in einer Cloud verschlüsselt sind, braucht es neben Oracle Advanced Security und einem On-Premise-basierten Key Management zwingend immer auch Oracle Database Vault. Aber mit TDE ohne Database Vault kann ein Administrator die verschlüsselten Daten in den Datafiles nicht lesen, er kann dafür über die Benutzer „root" und „oracle" („SYSDBA") Zugriff via SQL*Plus erlangen und Daten dann direkt abfragen. Werden die Daten dagegen bereits vor dem Speichern in der Datenbank verschlüsselt, sind diese Daten auch für hochprivilegierte Benutzer nicht lesbar. Der Einsatz eines solchen Produkts hat üblicherweise aber Einfluss auf das Datenmodell und die Applikation.

Neben den verschiedenen Produkten zur Verschlüsselung auf Betriebssystem-, Datenbank- oder Applikations-Ebene bieten sich weitere Produkte zur aktiven und passiven Überwachung der Datenbank-Zugriffe. Unternehmen wie Imperva, IBM und McAfee, aber auch Oracle mit Oracle Audit Vault and Database Firewall, bieten in diesem Kontext verschiedene Produkte an.

Diese Lösungen überwachen den Netzwerk-Zugriff auf die Datenbank und entscheiden anhand von Firewall-Regeln, ob ein Zugriff ausgeführt werden darf, bevor diese bei der Datenbank ankommt. In Kombination mit lokal installierten Agenten kann eine Datenbank effektiv geschützt werden, ohne an der Datenbank oder an dem Datenmodell etwas ändern zu müssen. Auf diese Weise lassen sich recht einfach Compliance-Auflagen umsetzen. Nichtsdestotrotz braucht es für den Einsatz dieser Produkte genauso ein Sicherheitskonzept, Know-how sowie entsprechende Investitionen bei der Beschaffung, Konfiguration und Betrieb der Lösung.

## Fazit

Oracle sowie Drittthersteller bieten verschiedene Produkte, um das Risiko eines Datenverlustes zu reduzieren und Datenbanken in der Cloud sowie On-Premise sicher zu betreiben. Doch je nach eingesetzter Technologie und Architektur sind der Aufwand sowie die Kosten sicher maßgebliche Punkte, die explizit zu betrachten sind. Dennoch bieten moderne, Cloud-basierte Umgebungen interessante Alternativen, die heutzutage in jedem IT-Projekt zu berücksichtigen sind.

Jedes Unternehmen muss dazu aber seine Daten und deren Wert kennen. Mit entsprechenden Risiko-Analysen, genauen Definitionen der Ist- und der Sollwerte sowie Prüfung der Bedürfnisse können rechtliche Fallstricke gezielt umgangen werden.

Gepaart mit den technischen Vorkehrungen kann ein Unternehmen beruhigt seinen sicheren Weg in die Cloud antreten. Das Vertrauen zum gewählten Cloud-Dienstleister spielt dabei, wie mehrmals angemerkt, sicher eine wesentliche Rolle. Schließlich geht es um die Daten des Unternehmens.

Stefan Oehrli
stefan.oehrli@trivadis.com

# Oracle kauft Marketing-Cloud-Riesen MOAT

Der Software-Hersteller Moat ist auf Analyse großer Datenmengen zu Marketingzwecken spezialisiert. Die Daten werden zur leichteren Auswertung in Diagrammen und Übersichten anzeigt. Zu ihren mehr als 600 Kunden weltweit zählen führende Unternehmen wie Procter & Gamble, Nestlé, Unilever und viele mehr. Diese Kunden und Partner gehen mit dem Kauf an Oracle über und die Marke Moat wird Teil der Oracle Data Cloud. Ein genauer Übernahme-Termin wurde nicht genannt. „Moat werde weiterhin als unabhängige Plattform agieren", so Oracle.