Derzeit planen oder implementieren viele Unternehmen den Aufbau von privaten und virtuellen Datenbank-Clouds, um Kosten durch Konsolidierung und Standardisierung zu sparen. Bei diesen Projekten wird die Sicherheit oft vergessen. Dieser Artikel beschreibt die Härtung von Datenbanken, um eine Grundsicherheit für private Datenbank-Clouds zu erreichen.

Datenbank-Härtung oder Aufbau von sicheren Referenz-Datenbanken

Carsten Mützlitz, ORACLE Deutschland B.V. & Co. KG

Unter dem Härten von Datenbanken [1] wird eine Konfiguration verstanden, die ausschließlich die Funktionen zulässt, die die Anwendung benötigt. Zusätzlich wird überprüft, ob Standardfunktionen beziehungsweise notwendige Zusatzfunktionen entsprechend den Anforderungen sicher eingestellt sind, wie keine Nutzung von Standard-Kennwörtern, Zurücknahme von nicht notwendigen Privilegien, Zugriffskontrolle auf sensible Daten, Datenverschlüsselung etc. Die DOAG *News* hat zu diesem Thema bereits einen Artikel [2] veröffentlicht. Betrachten Sie jetzt den vorliegenden Artikel als eine aktuelle Erweiterung dazu mit Bezug auf das Hype-Thema „Private and Virtual Database Clouds" und eine Tool-gestützte Härtung von Oracle-Datenbanken.

Private Database Clouds

Viele Unternehmen verlassen den Pfad der dedizierten Datenbank pro Anwendung mit eigener Hardware, eigenem Peak-Load-Sizing und kostspieliger Administration. Dabei bewegen sie sich nunmehr wieder in Richtung Konsolidierung. Sie virtualisieren vorhandene Applikationen auf virtuellen Hardware-Plattformen, um damit die Flexibilität zu erhöhen sowie eine bessere Auslastung und Effizienz zu erlangen. Es entsteht eine sogenannte „Shared-Infrastruktur", die eine Mandantenfähigkeit für Anwendungen unterstützt. Applikationen wie eine Datenbank können in diese neue Infrastruktur schnell provisioniert werden, etwa vollautomatisch via Self-Services mittels Cloning-Verfahren im Enterprise Manager oder als Oracle VM Templates. Das ermöglicht unter anderem einen schnellen Aufbau von Test- und Entwicklungsumgebungen und erhöht die Agilität eines Unternehmens (siehe Abbildung 1).

Die Zusammenführung von Datenbanken auf eine gemeinsame und zentrale Hardware-Plattform muss bei der Planung ebenso den Aspekt der bestehenden Risiken und notwendigen Sicherheitsanforderungen beinhalten. Um den Administrationsaufwand zu reduzieren, empfiehlt es sich, für bestimmte Datenbank-Typen einen Unternehmensstandard zu etablieren, der die notwendigen Sicherheitsanforderungen berücksichtigt. Ein praktikabler Ansatz ist die Definition von Referenz-Datenbanken über ein Konfigurations-Template, die dann per Knopfdruck mittels „Enterprise Manager" installiert werden können. Ist dieser Standard implementiert, sind alle neuen Datenbanken mit dem notwendigen Sicherheitsstandard ausgestattet und als gehärtet zu betrachten.

Fahrplan für eine Datenbank-Härtung

Es gibt verschiedene Vorlagen von Oracle (siehe [2], [3], [4, [5]), um eine Datenbank zu härten. Zwei wesentliche Punkte sind zu ergänzen: Nach Erfahrung des Autors werden viele produktive Datenbank-Landschaften mit sensiblen Daten ohne das einfache Auditing der Datenbank (Standardfunktion) verwendet. Doch das Bundesdatenschutzgesetz (BDSG) und andere Regularien wie „Payment Card Indus-

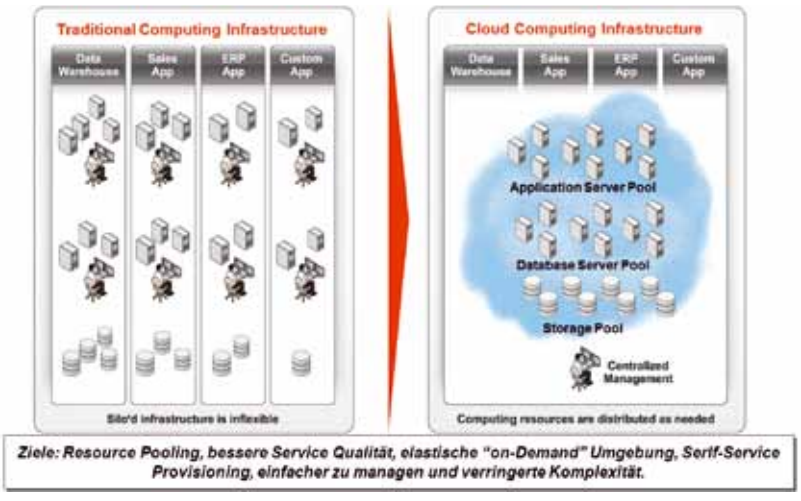

Abbildung 1: Cloud Computing

try Data Security Standard (PCI DSS)“ fordern ganz klar eine Protokollierung von wesentlichen Zugriffen auf das Datenbank-System, wenn personenbezogene oder andere sensible Daten dort abgelegt sind. Audit-Funktionalität ist eine Standardfunktion innerhalb der Datenbank, die eingeschaltet werden kann. Somit können automatisiert verschiedene Aktivitäten in der Datenbank protokolliert und überwacht werden. Unabhängigkeit vom BDSG sollten immer folgende Audit-Einstellungen [4] eingestellt sein:

- *Fehlerhafte Datenbank-Logins*
  audit create session whenever not successful;
- *Hochprivilegierte Datenbank-Aktivitäten der SYSDBAs protokollieren*
  Den „init.ora“-Parameter „audit_sys_operations=TRUE“ einstellen

Ein weiterer wichtiger Punkt, der auch im PCI-DSS-Standard definiert ist, ist die Forderung nach aktuellen Patches. Oracle liefert vierteljährlich sogenannte „kritische Sicherheitspatches (CPU)“. Diese gilt es einzuspielen, wenn das Scoring des Patches entsprechend sicherheitskritisch eingestuft ist. Für das Härten von Datenbanken bedeutet das, die aktuellen Patches in den Produktivsystemen einzuspielen. Hierfür ist es notwendig, eine geeignete Planung und ein Konzept zu definieren, um die Datenbanken in einem sicheren Zustand zu halten.

Anforderungen aus bestehenden gesetzlichen Regularien sind eine gute Grundlage, um auch eigene Sicherheitsstandards abzuleiten. Denn was für Kreditkarten- oder personenbezogenen Daten gilt, ist für sensible Unternehmensdaten sicherlich auch relevant.

Manuelle oder Tool-unterstützte Datenbank-Härtung

In der Regel entwerfen Unternehmen einen Sicherheitsstandard und setzen diesen manuell um. Die Erfahrung zeigt aber eindeutig, dass entsprechende Sicherheitsverantwortliche wie der Chief Security Officer (CSO) oder der Datenschutzbeauftragte keine Transparenz und Kontrolle über die Durchsetzung der definierten Sicherheitsstandards im Unternehmen haben. Daraus folgt, dass der Glaube eine höhere Sicherheitsumsetzung vermutet – die Realität jedoch eine andere Wahrheit spricht.

Die Lücke zwischen Glaube und Realität lässt sich Tool-basiert lösen. Gerade in Bezug auf Datenbank-Härtung beziehungsweise „sichere Konfiguration“ bietet Oracle eine umfangreiche Regelbibliothek an, die hier unterstützen kann und die aktuelle Konfiguration einer Datenbank auf Sicherheit prüft. Diese Funktionalität verbessert die Kontrolle und Transparenz bei der Durchsetzung von unternehmensweiten Sicherheitsstandards. Die Regelbibliothek ist Bestandteil des Enterprise Managers und wird im Funktionsumfang des Configration-Management-Packs angeboten.

Configuration Management

Das Configuration-Management-Pack sammelt Systemdaten des Hosts und der Datenbank und legt diese im Enterprise-Manager-Repository ab. Somit lassen sich Berichte über den Systembestand sowie Vergleiche der Systembestände durchführen. Idealerweise definiert man eine Baseline über eine Referenz-Datenbank und vergleicht damit die produktiven Systeme, um somit die Einhaltung des Unternehmensstandards aufzuzeigen. Für die Härtung von Datenbanken ist insbesondere der Policy-Manager interessant. Der Fokus liegt hier auf der Überwachung der Unternehmens- und Sicherheitspolicies.

Das Configuration-Management-Pack beinhaltet Hunderte automatisch ablaufbare Regeln für die Überprüfung der Sicherheit der Datenbank und deren Host. Diese können durch eigene Regeln erweitern werden. Es genügt ein Klick im Enterprise Manager, um einen Überblick über die sichere Konfiguration all seiner Datenbanken zu erhalten (siehe Abbildung 2). Der Administrator oder Sicherheitsverantwortliche erhält einen Überblick, gegen welche Regeln verstoßen wurde, wie sich die Compliance über einen Zeitraum verändert hat und welche Security Patches unbedingt eingespielt werden sollten.

Eine Policy-Group für die sichere DB-Konfiguration fasst wesentliche Regeln zusammen. Sie überprüft beispielsweise das Vorhandensein von Standard-Kennwörtern, Einstellungen der File-Permissions (Unix, Windows) von Oracle-Dateien, Init.ora-Parameter, Audit-Einstellungen, Kennwort-Policies sowie die Zugriffskontrolle auf DB-Objekte wie Tables (siehe Abbildung 3).

Eine weitere Policy-Group überwacht einige wichtige Konfigurationen auf dem Host. Es werden offene Ports, unsichere Services und Filesystem-Einstellungen überprüft. In der Summe bieten diese Policy-Gruppen einen Best-Practice-Ansatz, um die Überprüfung der Datenbank-Konfiguration auf gängige Sicherheitsaspekte zu kontrollieren. Der Policy-Manager kann Regeln und Regelgruppe automa-

Abbildung 2: Ausschnitt aus der DB-Security zusammengefasst

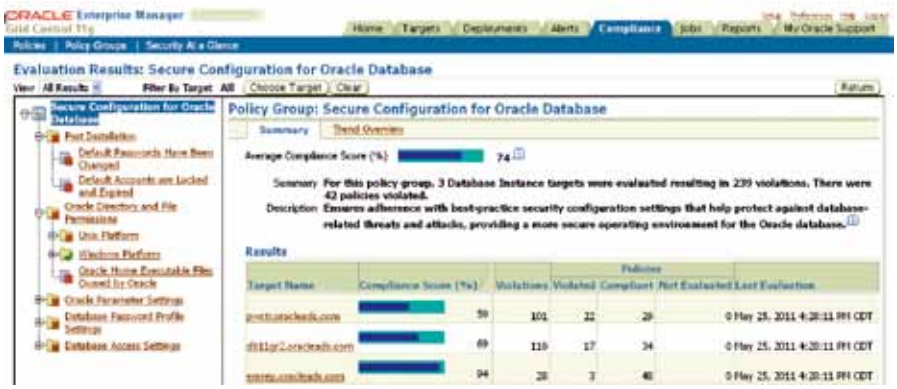

Abbildung 3: Policy Group „Secure Configuration for Oracle DB“ ausgeführt

tisiert ablaufen lassen und liefert einen aktuellen Zustand der sicheren Konfiguration. Zusätzlich werden Trends abgeleitet, die eine Verbesserung beziehungsweise Verschlechterung der Zustände visualisieren. Für die Härtung sind grundsätzlich vier Regel-Kategorien anzuwenden, die in vier Policy-Groups zusammengefasst sind:

- Database Instance Security Policies (122)
- RAC Database Security Policies (50)
- Host Security Policies (4)
- Listener Security Policies (36)

Jede dieser Regeln kann einzeln und automatisiert ablaufen (via Scheduler). Um den Automatisierungsgrad zu erhöhen, lässt sich für jede Regel zusätzlich eine automatische Korrektur bei Verletzung implementieren. Zum Beispiel wenn zwei Sample-Accounts in der Datenbank den Status „open“ aufweisen. Dieses Sicherheitsrisiko soll automatisch gelöst werden. Hierfür wird die Security-Regel „Well known Accounts“ editiert und eine automatische Korrektur implementiert, wenn eine Verletzung der Policy auftritt. Die automatisierte Korrektur einer Verletzung wird der Policy hinzugefügt und ein SQL-Script beigelegt, das alle bekannten Sample-Accounts sperrt sowie das Kennwort „expired“. Es können auch eigene Policies implementiert werden, um somit einen unternehmensweiten Standard für die sichere Konfiguration von Oracle-Datenbanken zu definieren.

Dieser kurze Einstieg in das Configuration Management Pack zeigt auf, wie einfach unternehmensweite Sicherheit-Policies für Datenbanken automatisiert durchgesetzt und überwacht werden können. Neben einer automatisierten sicheren Datenbank-Konfiguration („Härtung“) wird automatisch die Produktivität vieler Mitarbeiter erhöht, die sich im Unternehmen mit Security befassen.

Standardberichte

Der Enterprise Manager beinhaltet ebenfalls eine Vielzahl von Standardauswertungen. Beispielsweise kann pro Datenbank ein Überblicksreport ausgeführt werden. Dieser zeigt wesentliche Informationen einer DB-Instanz an. Ein weiterer guter Standardbericht ist die Konfigurationszusammenfassung einer Datenbank-Instanz, um den Zustand nach Fertigstellung einer Datenbank-Installation automatisch per Knopfdruck zu dokumentieren.

Oracle bietet weitere Lösungen an, die die Sicherheit der Datenbank wesentlich erhöhen:

- Für eine starke Authentisierung wie Kerberos, Datenverschlüsselung und Netzwerkverschlüsselung gibt es die Oracle-Advanced-Security-Option
- Für die Funktionstrennung (Segregation of Duties) und Durchsetzung diesbezüglich implementierter Policies bietet Oracle Database Vault an
- Eine zentrale Protokollierung von Datenbank-Aktivitäten und Ablage der Protokolle in einem revisionssicheren Repository ermöglicht Audit Vault
- Die Klassifizierung von Daten, um einen Zugriffsschutz auf Daten-Ebene zu erzielen, kann durch Label Security erlangt werden
- Die Überwachung von Datenbankzugriffen und Blockierung unerlaubter Zugriffe auf die Datenbank gewährleistet die Database Firewall

Fazit

Eine Härtung des Datenbanksystems hat zwei wesentliche Ziele: Risiko-Minimierung und Nachweisbarkeit. Zum einen soll eine kontrollierte Vorgehensweise definiert werden, die eine Datenbank den Anforderungen entsprechend konfiguriert. Dieses Vorgehen implementiert einen Grundschutz und verfolgt das zweite Ziel, nämlich die Verringerung des Risikos vor Missbrauch.

Weitere Informationen

[1] BSI, M 2.363 Schutz gegen SQL-Injection, hier Beschreibung zur Härtung von Datenbanken: https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02363.html

[2] DOAG News, 2007 Q3, Heinz-Wilhelm Fabry, Härten – effektiver Grundschutz für Datenbanken: http://www.doag.org/pub/docs/Publikationen/DOAG-News/2007/2007-3/12_Haerten_DNQ3_07.pdf

[3] Oracle Project Lockdown: http://www.oracle.com/technetwork/articles/index-087388.html

[4] Oracle Database Security Guide 11gR2, Chapter 10 Keeping your Oracle database secure: http://download.oracle.com/docs/cd/E11882_01/network.112/e16543/guidelines.htm#CHDCEBFA

[5] Oracle Database Security Checklist: http://www.oracle.com/technetwork/database/security/twp-security-checklist-database-1-132870.pdf

Carsten Mützlitz
ORACLE Deutschland B.V. & Co. KG
carsten.muetzlitz@oracle.com