HANSER

Oracle Security in der Praxis

Sicherheit für Ihre Oracle-Datenbank

ISBN 3-446-40436-8

Vorwort

Weitere Informationen oder Bestellungen unter
http://www.hanser.de/3-446-40436-8 sowie im Buchhandel

Vorwort

Mitte der 90er Jahre machte ich das erste Mal nähere Bekanntschaft mit der Sicherheit. Bis zu diesem Zeitpunkt hatte ich schon in verschiedenen Bereichen der IT gearbeitet, vornehmlich aber im technischen Support bei Oracle. Wenn Sie im technischen Support arbeiten, gilt vor allem eines: Sie müssen schnell sein. Die Kunden rufen Sie normalerweise erst an, wenn das Problem richtig brennt, und möchten eine schnelle Lösung – am liebsten vorgestern. Damals erforderte diese Arbeit oft den Zugriff auf das Kundensystem; für Sie als Supporter bedeutete das auch, dass Sie im Regelfall einen hochprivilegierten Zugriff auf das Kundensystem brauchten, zumindest mal den Oracle-Benutzer. Das Problem konnte ja alle möglichen Ursachen haben, und speziell am Anfang muss man oft erst eingrenzen, wo das Problem nun genau liegt.

Diese Arbeitsweise war ich also gewohnt, als ich einen Auftrag für Onsite-Support bei einer Bank erhielt. Wie Sie sich denken können, wird das Thema Sicherheit bei einer Bank besonders groß geschrieben. Wie groß, war mir bis dato auch nicht klar. Mir gingen die Augen auf! Wenn mir dort ein Problemfall gemeldet wurde, der Zugriff auf ein produktives System erforderte, mussten zuerst alle nötigen Bewilligungen eingeholt und ganz genau angegeben werden, was man denn vorhatte. Der ganze Prozess war zum Teil umständlicher als der eigentliche Support.

Das ist eines der Kennzeichen der Sicherheit innerhalb der IT: Sicherheit wirkt sich immer auch auf andere Bereiche aus; sei es, dass etwas umständlicher wird oder auch nur länger dauert. Das ist keine Kritik an der Sicherheit, sondern einfach eine Eigenschaft, über die man sich klar sein sollte. Oder anders ausgedrückt: Alles hat seinen Preis, auch die Sicherheit.

Um eine Analogie zu verwenden: Zur Sicherung einer Wohnung bedarf es zumindest eines Türschlosses. Wenn Sie jedes Mal die Tür abschließen, wenn Sie die Wohnung verlassen, müssen Sie beim Zurückkommen auch jedes Mal wieder aufschließen. Das erfordert natürlich mehr Zeit, als wenn Sie die Tür einfach unverschlossen lassen. Wenn die Tür aber nicht verschlossen ist, kann andererseits jeder rein- und rausspazieren, wie es ihm passt.

Sicherheit hat zu einem großen Teil viel mit Prozessen und Organisation zu tun. Sicherheit ist eine Aufgabe ohne Ende. In diesem Buch beschränke ich mich allerdings´auf die technischen Aspekte der Sicherheit, die in einem Oracle-Umfeld von Belang sind. Oder um noch einmal mit einer Analogie zu sprechen: Ich zeige Ihnen, welche Schlösser es gibt und wo Sie diese Schlösser einbauen können. Ob und wann Sie die Tür dann abschließen oder nicht und wem Sie die Tür aufmachen oder besser nicht, ist nicht Thema dieses Buches.

Tatsächlich gibt es sehr viele Bücher zum Thema Sicherheit, aber speziell zu Oracle sind es nicht besonders viele. In diesem Zusammenhang möchte ich lediglich auf das ausgezeichnete Buch von David Knox [KNOX2005] hinweisen, das allerdings nur auf Englisch erhältlich ist. Abgesehen davon sind die verschiedenen Oracle Manuals, speziell der Security Guide [ORASEC102], ein guter Einstiegspunkt.

Sie sollten als Leser allerdings bereits mit Oracle vertraut sein – eine Einführung in Oracle bietet das vorliegende Buch nicht.

Oracle bietet verschiedene Produkte für das Identitätsmanagement an, die hier aber nur am Rande, wenn überhaupt, besprochen werden; mehr hätte den Rahmen dieses Buches gesprengt. Abgesehen davon ist Sicherheit in Oracle vor allem Sicherheit in der und durch die Datenbank, und dieses Thema wird detailliert besprochen.

Nach der Lektüre dieses Buches sollten Sie in der Lage sein, die verschiedenen Sicherheitskomponenten und -Tools, die Oracle zur Verfügung stellt, beurteilen und einsetzen zu können.

- Im ersten Kapitel werden die verschiedenen Formen der Identifizierung und Authentisierung inklusive Enterprise User Security detailliert besprochen.
- Das zweite Kapitel ist das umfangreichste, dort wird die Kontrolle des Datenzugriffs genauer untersucht. Diese Zugriffskontrolle kann in Oracle auf verschiedenen Ebenen realisiert werden. Zum einen kann das auf oberster Ebene über Benutzer und Rollen erfolgen, zum anderen aber auch durch die spezifische Vergabe von Rechten. Es werden sowohl die „groben" Kontrollmechanismen wie System- und Objektprivilegien als auch die „feinen" Mechanismen – als Stichworte seien hier Virtual Private Database (VPD) und Oracle Label Security (OLS) genannt –, die eine Zugriffskontrolle bis hinunter auf einzelne Spalten und Zeilen erlauben, dargestellt.
- Das anschließende dritte Kapitel ist wieder kürzer, es beschreibt die Sicherheitsmechanismen für die Kommunikation mit Oracle im Netzwerk, das bedeutet: den Verkehr über SQL*Net. Der Schwerpunkt liegt hier neben der Zugriffskontrolle auf IP-Adressebene auf Prüfsummen und der Verschlüsselung der Kommunikation.
- Das vierte Kapitel behandelt die Verschlüsselungsmöglichkeiten der Daten in der Datenbank, das heißt auf Dateiebene und bei der Datensicherung.
- Das abschließende fünfte Kapitel stellt zu guter Letzt die verschiedenen Überwachungsmöglichkeiten vor. Neben dem traditionellen Audit wird hier auch auf die Überwachung auf Datenebene – das Stichwort ist hier Fine-grained Auditing (FGA), sowie die Überwachung unter Oracle Label Security – eingegangen.
- Im Anhang finden Sie eine sehr einfache Sicherheits-Checkliste, die Ihnen einige Anregungen für die Überprüfung der Datenbanksicherheit geben soll.

Die im Buch verwendeten Beispiele können Sie natürlich wieder bei Hanser (http://downloads.hanser.de) direkt herunterladen. Ich habe mich bemüht, die Beispiele so einfach wie möglich zu halten, meistens genügt das bekannte SCOTT/TIGER-Schema; das Thema ist schwierig genug, da wollte ich Sie als Leser nicht noch zusätzlich verwirren.

Noch eine Anmerkung zum SCOTT/TIGER-Schema: Bei diesem Schema handelt es sich um einen Demobenutzer, der seit Urzeiten in Oracle existiert, allerdings immer separat installiert werden muss. In früheren Versionen erfolgte dies immer über irgendeine Variante des Scripts DEMOBLD.SQL, in Version 10.2 fand ich interessanterweise das Schema für meine PC-Version 10.2 im Script SCOTT.SQL. Wenn Sie den Benutzer installieren, werden auch einige Beispieltabellen angelegt, von denen vornehmlich die beiden Tabellen EMP und DEPT verwendet werden.