Oracle Security in der Praxis

Sicherheit für Ihre Oracle-Datenbank

Frank Haas

HANSER

Inhalt

1 Identifizierung und Authentisierung

Im ersten Kapitel geht es um Identifizierung und Authentisierung, also darum, als welche Person Sie sich gegenüber der Datenbank ausweisen; neben der Autorisierung, die wir im nächsten Kapitel behandeln, ist dies einer der Grundpfeiler der Sicherheit, wenn Sie mit Oracle arbeiten.

1.1 Einleitung

In den Anfangstagen der IT hatte Sicherheit vornehmlich zwei Aspekte: den physikalischen und den humanen. Unter physikalischem Aspekt verstehe ich hier in erster Linie den Zugang zum Computer. Die physikalische Sicherung des Computers bestand damals im Wesentlichen darin, dass er in einem gut verschlossenen Raum stand, zu dem nur autorisiertes Personal Zutritt hatte. Diese Art der Sicherung hat nach wie vor ihre Berechtigung und existiert auch noch heute; IT-Profis sind Serverräume wohl vertraut.

Auch der zweite Sicherheitsaspekt, der humane, ist nach wie vor aktuell und der bei weitem schwierigere. Zum einen geht es hier darum, dafür zu sorgen, dass nur autorisiertes Personal Zugriff auf den Computer und die Programme hat. Das ist aber nur ein Teilaspekt der Sicherheit. Zum anderen sollte sichergestellt werden, dass kein Schaden durch die eigenen Mitarbeiter verursacht wird. Für den Großteil der Sicherheitsverletzungen sind nicht die viel beschworenen Hacker, sondern die eigenen Mitarbeiter verantwortlich. Dabei braucht es sich auch nicht um böse Absicht zu handeln, manchmal genügen Fehler, wie sie immer wieder vorkommen. Natürlich gibt es auch den frustrierten Angestellten, der sich rächen will, aber das ist nur ein möglicher Verursacher. Die Kunst besteht hier darin, die Sicherheitslücken schnell zu entdecken und zu schließen.

Die Vernetzung der Computer untereinander und speziell das Internet haben eine zusätzliche Dimension ins Spiel gebracht. Jetzt war es plötzlich möglich, auf Computer zuzugreifen, die ganz woanders standen. Es war nicht mehr notwendig, dass man direkt vor dem Computer saß. Der Computer konnte in einem anderen Raum, in einer anderen Stadt oder sogar auf einem anderen Kontinent stehen. Das eröffnete natürlich auch auf der Gefährdungsseite ganz neue Angriffsszenarien. Um an die Daten eines Computers zu kommen, genügte es jetzt, Zugriff auf den Computer zu erlangen, der physikalische Zugang war nicht mehr notwendig. Dies und die rasante Ausbreitung des Internet führten vor einigen Jahren zu Architekturen, in denen der Zugang zum Rechner über das Internet über eine demilitarisierte Zone (DMZ) erfolgt.

Eine DMZ ist immer von Firewalls umgeben. Dabei reguliert zumindest ein Firewall die Kommunikation zwischen DMZ und Internet und ein weiterer Firewall übernimmt die Kommunikation zwischen DMZ und Intranet. Die eigentlichen Nutz- und Firmendaten stehen

im Intranet. Ein Firewall ist quasi ein Netzwerkrouter, der nur bestimmte Ports und Netzwerkprotokolle durchlässt. Durch die Abschottung des Intranets über die vorgelagerte DMZ soll gewährleistet werden, dass keine illegalen Meldungen/Protokolle vom Internet ins Intranet gelangen (und umgekehrt) und dass in Falle einer Übernahme eines Rechners durch einen Angreifer der Angriff auf den betroffenen Rechner beschränkt bleibt.

Selbstverständlich können auch mehrere DMZ-Zonen eingerichtet werden, typischerweise steht ja auch ein Applikationsserver, der die Präsentation der Daten übernimmt und seinerseits die Daten vom und ins Intranet überträgt, in einer DMZ.

Passwörter und ihre Nachteile

Moderne Computer arbeiten im Regelfall mit einem Betriebssystem, das den Benutzer zwingt, sich mit einem Namen und einem Passwort anzumelden. Diese Form der Authentisierung ist nach wie vor die gebräuchlichste. Sie wird nicht nur bei der Anmeldung im System, sondern ganz generell beim Arbeiten mit irgendwelchen Programmen verwendet. Man spricht hier auch von einem Berechtigungsnachweis (englisch Credential), wobei die Identifikation des Benutzers auch über andere Formen der Authentisierung – als Beispiel sei hier eine Chipkarte (englisch SmartCard) genannt -- erfolgen kann. Ein Credential aus dem täglichen Leben, das wir alle kennen, ist der Personalausweis. Ich verwende hier die Begriffe Identifizierung und Authentisierung gleichbedeutend, obwohl sie das streng genommen nicht sind (und auch Authentisierung noch von Authentifizierung unterschieden werden kann); wesentlich ist hier nur, dass der Benutzer eindeutig identifiziert wird.

Dabei braucht es sich beim Benutzer nicht um einen Menschen zu handeln, es kann ebenso gut ein anderer Computer oder auch nur ein anderes Programm sein.

Immer, wenn Sie mit der Datenbank arbeiten, müssen Sie sich vorher bei der Datenbank mit Benutzernamen und Passwort anmelden, eine anonyme Anmeldung gibt es bei Oracle nicht. Der Benutzer kann dabei in der Datenbank selbst angelegt sein oder auch als so genannter Enterprise-Benutzer in einem LDAP-Server, der dann seinerseits die Autorisierung für die Datenbank übernimmt, definiert werden. Hier können an Stelle von Passwörtern digitale Zertifikate verwendet werden. Eine weitere Möglichkeit schließlich ist die Autorisierung des Oracle-Benutzers durch das Betriebssystem; diese Variante ist sehr gut für Stapelverarbeitungen geeignet, da sie normalerweise kein zusätzliches Passwort benötigt; der Benutzer wurde ja schon durch das Betriebssystem identifiziert.

Passwörter bescheren uns allerdings ein gravierendes Problem: sie können erraten werden. Um das Erraten zu erschweren, werden oft bestimmte Anforderungen an ein Passwort gestellt: Neben einer Mindestlänge – 8 oder 12 Zeichen sind zum Beispiel ganz gute Werte – wird oft auch gefordert, dass das Passwort aus Klein- und Großbuchstaben besteht und mindestens ein Sonderzeichen oder eine Zahl enthält. Eine bekannte Form von Passwörtern, die uns allen aus dem täglichen Leben vertraut ist, sind beispielsweise Geheimnummern (auch persönliche Identifikationsnummer oder kurz PIN genannt), die nur aus Zahlen bestehen und für die Authentisierung an Geldautomaten und Handys benutzt werden.

Der große Vorteil von Passwörtern liegt sicher darin, dass die Kosten für Implementierung und Unterhalt relativ gering sind. Der große Nachteil ist, wie schon erwähnt, der relativ schwache Schutz. Man spricht bei der Authentisierung über Passwörter auch von schwacher Authentisierung.

Stärkere Formen der Authentisierung basieren zum Beispiel auf örtlichen Einschränkungen – der Zugang ist nur direkt am Computer oder von bestimmten Rechnern aus möglich – oder Dingen, die man besitzt. Solche Dinge können Chipkarten, Softwarelizenzschlüssel oder digitale Zertifikate sein. Biometrische Merkmale, die mit speziellen Geräten wie Fingerabdrucklesern und Irisscannern überprüft werden, bieten offensichtlich den stärksten Schutz, erfordern aber auch die größten Investitionen.

Selbstverständlich können und werden die verschiedenen Methoden auch kombiniert eingesetzt: Am Bankautomaten benötigen Sie Bankkarte und Geheimnummer (und Geld auf dem Konto, sonst gibt's auch nichts ...).

Passwörter werden aber wohl mit der Zeit verschwinden oder zumindest nicht mehr dieselbe Stellung wie heute einnehmen; neulich habe ich im Supermarkt schon ein Sonderangebot für einen Fingerabdruckleser gesehen.

Starke Authentisierung kann in einer Oracle-Umgebung mit der Oracle Advanced Security Option (ASO), die zusätzlich installiert und lizenziert werden muss, konfiguriert werden. Neben ASO ist bei diesen Formen der Authentisierung zusätzliche Hard- und/oder Software notwendig. ASO unterstützt RADIUS und damit auch SecureID, Entrust, Kerberos und SSL. Die Authentisierung über SSL wird im Folgenden noch im Detail beschrieben, für die Details zu RADIUS und Kerberos verweise ich Sie auf Teil 3 in [ORAASO102] und [ORAEUS102] .

Bei der Authentisierung gibt es ein weiteres Problem: Normalerweise arbeitet ein Benutzer nicht nur mit einer Applikation, sondern mit mehreren, was bedeutet, dass er sich bei jeder Applikation neu anmelden muss. Sie ahnen wahrscheinlich jetzt schon, wo das Problem liegt, oder kennen es bereits: Versuchen Sie mal, sich 20 unterschiedliche Passwörter zu merken. Das ist kein Spaß.

Eine Lösung hier verspricht Single Sign On (SSO). SSO bedeutet, Sie authentisieren sich nur ein einziges Mal auf einer Portal- oder Webseite und können dann auf alle Rechner und Dienste, für die Sie autorisiert sind, zugreifen, ohne sich neu anmelden zu müssen. Der SSO-Mechanismus übernimmt dann die weitere Authentisierung für Sie. Nachteilig ist hier natürlich, dass ein Hacker, falls er die Identität eines regulären Benutzers gestohlen hat, sofort Zugriff auf alle Systeme hat. Aus diesem Grunde empfiehlt es sich, bei SSO-Systemen stärkere Autorisierungsformen zu verwenden. Andererseits benötigen Sie gerade bei einem SSO-Portal einen Mechanismus, der auch die Anbindung von externen Applikationen erlaubt; das ist wiederum am einfachsten über Benutzername und Passwort zu realisieren. In einer Oracle-Umgebung kann SSO über Oracle Application Server Single Sign-On (OracleAS SSO) realisiert werden.

1.2 Warum ist Authentisierung wichtig?

Authentisierung ist in Oracle-Systemen vor allem deshalb so wichtig, weil Oracle nur anhand Ihres Benutzernamens bestimmt, welche Privilegien Sie haben. Es gibt keine anonyme Anmeldung an eine Oracle-Datenbank. Egal, wie die Anmeldung erfolgt, letzten Endes existiert immer ein Benutzer in der Oracle-Datenbank, und dieser Benutzername entscheidet, was Sie machen können und was nicht. Dabei können die Rechte und Privilegien des Benutzers, wenn man mal von den durch Oracle bereitgestellten vordefinierten Benutzern absieht, ganz unabhängig vom Namen des Benutzers definiert werden.

Die Liste der aktiven Benutzer sehen Sie übrigens immer im Data Dictionary View V$SESSION. Das SELECT in der folgenden Abfrage verwendet die Bedingung USERNAME IS NOT NULL, um die Oracle-internen so genannten Hintergrundprozesse auszuschließen, und die Bedingung PIECE=0, um nur die ersten 64 Zeichen des Benutzerkommandos anzuzeigen. Da sich der gleiche Benutzer theoretisch – praktisch kommt das aus verschiedenen Gründen auch sehr häufig vor – mehrmals an derselben Datenbank anmelden kann, gibt es in Oracle noch den so genannten Session Identifier oder kurz SID genannt. Damit können unterschiedliche Sessions des gleichen Benutzers unterschieden werden:

Listing 1.1 Benutzer inklusive verwendetem SQL

```
SQL> select sid,username as user, sql_text
 2 from v$session, v$sqltext
 3 where sql_address=address
 4 and piece=0 and username is not null
 5 order by username;

SID USER   SQL_TEXT
--- ------ ----------------------------------------------------------------
145 SYSTEM select sid,username,sql_text from v$session, v$sqltext where
```

Wie man in der obigen Abfrage sieht, ist der Frager in diesem Beispiel gleichzeitig auch der einzige aktive Benutzer.

Einen Benutzer legen Sie in Oracle im SQL mit dem Befehl CREATE USER an. Dabei kann der Benutzername bis zu 30 Bytes lang werden, und Sie können als Benutzernamen eigentlich alle Zeichen verwenden, die in [ORASQL102] als gültig aufgeführt werden. Oracle empfiehlt allerdings, dass Sie nur Zeichen aus dem ASCII- oder EBCDIC-Zeichensatz verwenden. Dem kann ich mich nur anschließen: So können Sie Portierungsprobleme, die eventuell eines Tages beim Wechsel der Plattform Ihrer Datenbank entstehen könnten, von vornherein ausschließen.

Daneben existieren in Oracle bereits einige vordefinierte Benutzer, am bekanntesten sind hier sicher SYS und SYSTEM. SYS ist quasi der Meta-User der Datenbank. Nach dem Anlegen der Datenbank gehören die internen Strukturen der Datenbank diesem Benutzer. Die vordefinierten Benutzer schauen wir im nächsten Abschnitt noch ein wenig genauer an. Diese Benutzer hatten lange Zeit Default-Passwörter. Auch das verschwindet zwar langsam, doch es besteht zumindest seit Version 9i bei der Installation die Möglichkeit, für

SYS und SYSTEM Passwörter zu setzen. Auch sind die meisten Default-Benutzer seit Version 9i nach der Installation gesperrt. Aber es gibt ja noch jede Menge Nicht-Oracle-Software, die Default-Benutzer verwenden. Das ist immer noch eine der besten Einbruchsmöglichkeiten in eine Oracle-Datenbank; die Default-Benutzer besitzen zum Teil recht mächtige Privilegien.

Deshalb gilt:
Verwenden Sie nie Default-Passwörter!

Eine sehr vollständige Liste der Default-Benutzer und -Passwörter inklusive der entsprechenden Check-Programme finden Sie im Internet auf den Seiten von Pete Finnigan (http.//www.petefinnigan.com).

Ein Benutzer kann nur einmal in einer Oracle-Datenbank existieren. Falls Sie also einen bereits bestehenden Benutzer noch mal anlegen wollen, erhalten Sie den Fehler ORA-1920.

Die Befehle ALTER/CREATE USER sind ganz gut für Batch-Verarbeitungen geeignet, es gibt aber auch komfortablere Möglichkeiten. Eine davon ist die Database Control Console, die mit Version 10g eingeführt wurde. Database Control Console ist eine abgespeckte Form des Oracle Enterprise Managers und lässt sich recht einfach mit dem Kommando „emca config dbcontrol“ anlegen. Während der Oracle Enterprise Manager einen zentralen Einstiegspunkt für die Verwaltung mehrerer Datenbanken bietet, funktioniert die Database Control Console nur gegen die Datenbank, für die sie konfiguriert wurde. Wie Abbildung 1.1 zeigt, ist damit auf einfache Art das Anlegen eines Benutzers möglich:

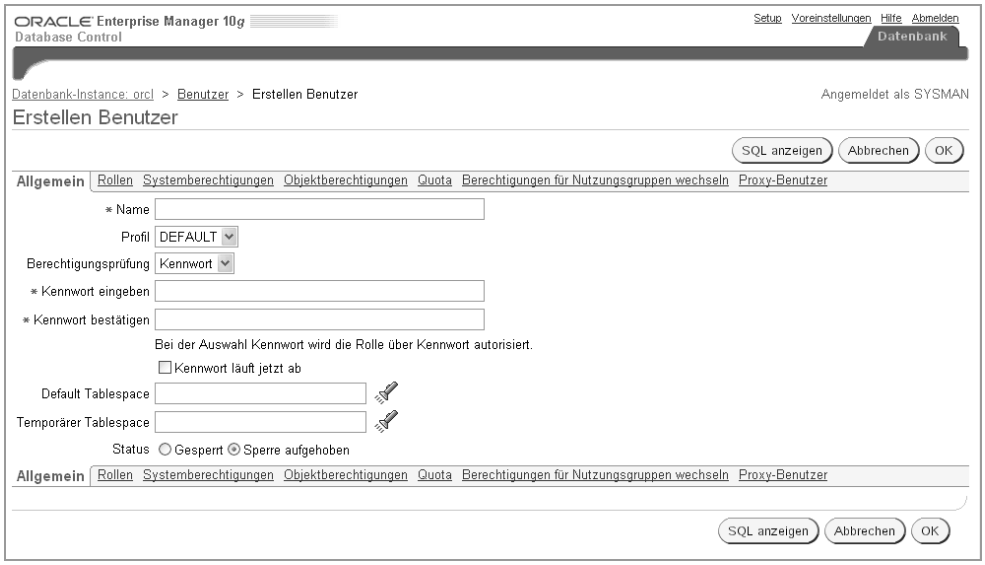

Abbildung 1.1 Anlegen eines Benutzers mit der Database Control Console

Register

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z