

HELPDESK

Sicherheit für Datenbanken von Oracle

Wie sicher sind Oracle-Datenbanken? Und wie kann man sich vor Angriffen schützen?

Datenbanken sind weit verbreitet und bilden oft das technische Herzstück von Business-Prozessen – wann immer es um Geld in Netzwerken geht, sind meist Datenbanken im Spiel. Die Anwendungsarten sind vielfältig. Falls die Datenbanken nicht allein für die Nutzung im LAN gedacht sind, können sie sowohl direkt vom Internet als auch als Backend-systeme via eine Webseite angesprochen werden.

Das gleichnamige Produkt der Firma Oracle ist eine sehr populäre Datenbanksoftware, die auf diversen Betriebssystemen verfügbar ist. Oracle ist sehr komplex und bietet einen grossen Funktionsumfang. Zwar hört man oft, dass Oracle «sicher» sei – dennoch werden immer wieder Sicherheitslücken publik. Vor dem Jahre 2000 waren vier Verwundbarkeiten für Oracle bekannt, zwischen den Jahren 2000 und 2004 wurden dann über 70 weitere Verwundbarkeiten veröffentlicht.

Oracle kann über das Netzwerk detektiert werden, insbesondere der Oracle-TNS-Listener (TCP Port 1520-1530, normalerweise 1521) ist einfach zu finden. Auch andere Oracle-Dienste belegen spezifische Ports. Beispiele sind der Oracle-Enterprise-Manager (HTTP auf TCP Port 3339), Ora-

«Standard-Installationen von Oracle-Datenbanken sind nicht als sicher zu erachten.»

cle-OAS (HTTP Ports TCP 7777 und 7778 sowie HTTPS Port TCP 4443) und Oracle-XDB (HTTP Port 8080 und FTP Port TCP 2100).

Der Oracle-TNS-Listener kann benutzt werden, um Oracle zu identifizieren (etwa mit Tools wie «lsnrctl» oder «tnscmd.pl»). Dies lässt sich aber auch über Webservices (fcgi-bin/echo und demo/basic/info.jsp) bewerkstelligen. Standardmässig wird erst ab Oracle Version 10g ein Passwort für den Oracle-TNS-

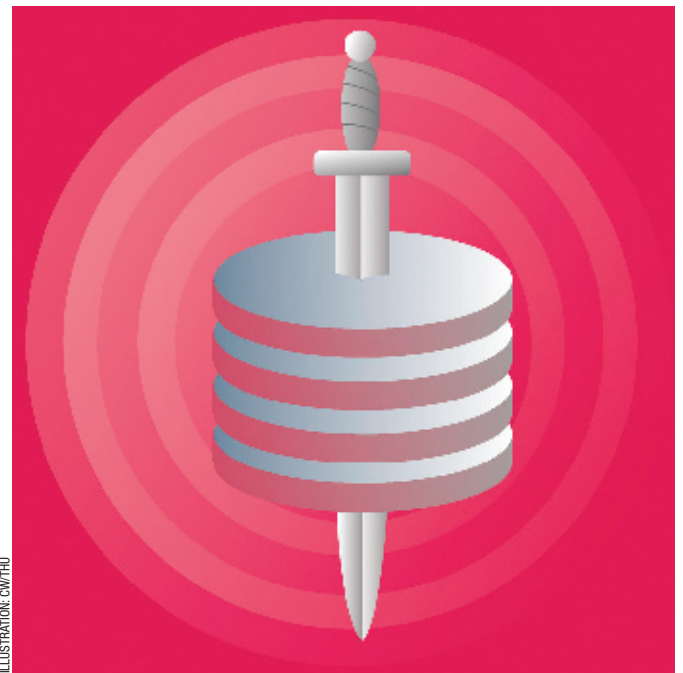


ILLUSTRATION: OWTHÜ

Listener benötigt. Es existieren Listen von Default-Passwörtern für Oracle, welche bereits über 500 Passwörter enthalten.

Oracle verwendet die PL/SQL, die mittels SQL-Injection attackiert werden kann. Auch ein allfällig vorhandener PL/SQL-Gateway (der zwischen Datenbank und Webapplikation interagiert) kann attackiert werden. Dasselbe gilt für sonstige PL/SQL-Prozeduren und -Applikationen. Dabei

kann unter Umständen auch auf das Filesystem oder auf Betriebssystembefehle zugegriffen werden.

Die Sicherheit von Oracle ist abhängig vom Härtnungsgrad. Dabei müssen auf der Netzwerkkseite die nicht notwendigen Dienste abgeschaltet, der Oracle-TNS-Listener mit ACL und Passwort geschützt, interne Dienste auf 127.0.0.1 gebunden, Verschlüsselung (SSL oder IP-Sec) verwendet sowie eine netzwerk-basierte Filterung (ACL, Firewall und IDS) implementiert werden.

Die Datenbank selbst sollte zeitnah gemäss veröffentlichter (und verifizierter) Patches aktualisiert werden. Wann immer möglich sind verschiedene Instanzen und Tabellen zu ver-

wenden, um die Benutzerrechte besser einschränken zu können. Es gibt verschiedene gute Hardening-Guides im Internet, etwa von CISecurity oder SANS Institute. Wichtige Punkte sind Password Policies und User Access Control, was immer sorgfältig berücksichtigt werden sollte – zudem kann eine Oracle-Datenbank mit Verschlüsselung versehen werden (DBMS_Crypto). Zusätzliches Schutz bietet die Implementierung von Virtual Private Databases, was eine feinere Rechteverteilung zulässt.

Generelle Massnahmen sind ebenfalls applizierbar, namentlich Logging aller Art (Oracle-TNS-Listener, Oracle-Redo-Log, SYS.AUD, Oracle-HTTP-Logs) sowie das dazugehörige Auswerten der Logs. Dies hilft auch im Fall einer Kompromittierung der Datenbank, weil die Aktionen der Attacke nachvollzogen werden können.

Damit wird klar: Oracle-Datenbanken können mit entsprechenden Härtnungsmassnahmen solide abgesichert werden – eine Standard-Installation ist allerdings nicht als sicher zu erachten. ■

 Archiv aller Helpdeskartikel: www.computerworld.ch



Der Autor
Martin Rutishauer ist Consultant und OPST/OPSA bei der Security-Beraterin OneConsult, Bern, www.oneconsult.com

Jede Woche beantworten Sicherheitsexperten Ihre Leserfragen:

Haben Sie Fragen rund ums Thema IT-Sicherheit?

Schreiben Sie uns:
it-security@computerworld.ch