Beoordeling van de beveiliging van Oracle-databases

A.A. van Dijke en ing. L.S. Binken CISSP

Een auditaanpak voor de Oracle-database waarin aandacht is voor beveiligingsmaatregelen op de verschillende relevante niveaus in de technische infrastructuur is cruciaal om de relevante beveiligingsrisico's te kunnen identificeren. Het is van belang om tijdens het onderzoek naar de beveiliging van de Oracle-database de maatregelen op alle lagen in de technische infrastructuur te toetsen aangezien de beveiligingsmaatregelen in hogere lagen in belangrijke mate steunen op de maatregelen die in de onderliggende lagen zijn getroffen.

Inleiding

De keuze voor het onderwerp van dit artikel is primair ingegeven door de ervaringen die zijn opgedaan in de KPMG-auditpraktijk bij het beoordelen van de beveiliging van Oracle-databases.

Allereerst heeft de ervaring ons geleerd dat de samenhang van de Oracle-database met haar omgeving als steeds belangrijker wordt ervaren. Dit is mede ingegeven door ontwikkelingen in het kader van de Sarbanes-Oxley Act 404. Ook de steeds verdere integratie van financiële, personele en logistieke informatiesystemen heeft bijgedragen aan de behoefte aan een meer geïntegreerde auditbenadering van databases.

Verder wordt de beoordeling van de Oracle-database zelf als complex ervaren. Dit komt voornamelijk doordat auditors niet eenduidig kunnen vaststellen of zowel voor opzet als bestaan voldoende maatregelen zijn getroffen teneinde de integriteit, vertrouwelijkheid en beschikbaarheid van Oracle-databases te waarborgen.

Twee aanleidingen dus om tot het schrijven van dit artikel over te gaan. Het artikel is zowel bedoeld voor IT-auditors als voor professionals binnen organisaties die betrokken zijn bij het beheer van Oracle-databases. In dit artikel wordt een aanpak beschreven die kan worden gebruikt bij het beoordelen van de beveiliging van Oracle-databases.

Hierbij is getracht de lezer inzicht te verschaffen in de volgende twee aspecten:
- de samenhang van de Oracle-database met haar omgeving binnen de technische infrastructuur;
- de veelvoorkomende beveiligingsrisico's van een Oracle-database.

A.A. van Dijke
werkt sinds 1999 bij KPMG Information Risk Management. Hij houdt zich bezig met technische auditing en advisering op het gebied van besturingssystemen, databases en applicaties. Hij is gespecialiseerd in SAP-, Oracle- en Unix-beveiliging. Ook is hij betrokken bij de ontwikkeling van audit tools.

vandijke.ad@kpmg.nl

Ing. L.S. Binken CISSP
werkt sinds 1998 bij KPMG Information Risk Management. Hij heeft zich gespecialiseerd in technische auditing en advisering op het gebied van beveiliging van netwerken, besturingssystemen en databases. Tevens voert Laurens opdrachten uit op het gebied van ethical hacking.

binken.laurens@.kpmg.nl

Auditaanpak

Bij het uitvoeren van een audit naar de beveiliging van Oracle-databases hanteren wij de volgende fasering:

1. Informatie verzamelen omtrent de context van de database:
   – Waar wordt de database voor gebruikt en welke gegevens bevat de database?
   – Wat is het belang van de database voor de bedrijfsvoering?
2. Beschrijven van de technische infrastructuur:
   – Wat is de relatie tussen Oracle en het netwerk?
   – Hoe grijpt Oracle in op het besturingssysteem?
   – Welke applicaties en gebruikers benaderen de gegevens en op welke wijze?
3. Terugkoppeling uitkomsten stap 1 en stap 2 met de opdrachtgever.
4. Uitvoeren van een risicoanalyse.
5. Opstellen en afstemmen van de beveiligingsnormen met de opdrachtgever.
6. Inventariseren en beoordelen van de effectiviteit van beveiligingsmaatregelen en het maken van een inschatting van de restrisico's.
7. Afstemmen van bevindingen met de opdrachtgever en het opstellen van een rapportage met conclusie, bevindingen, risico's en aanbevelingen.

In het kader van de doelstelling van dit artikel zal worden ingegaan op de fasen 2 en 6.

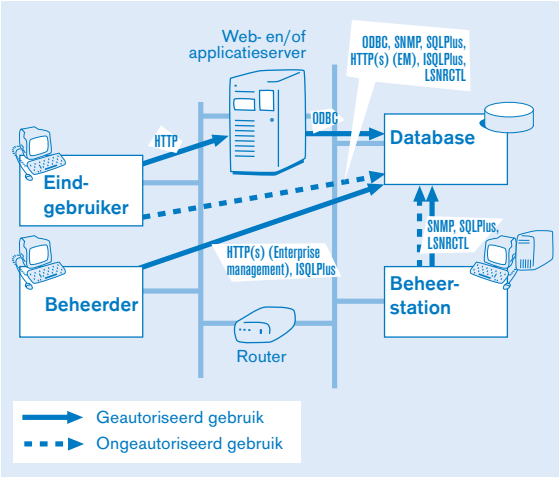
Beschrijven technische infrastructuur

Alvorens met een Oracle-databasebeveiligingsonderzoek wordt gestart, is afbakening van de te onderzoeken objecten essentieel. Hierbij wordt gebruikgemaakt van een analyse waarbij alle componenten worden geïdentificeerd die bij het zogenaamde logische toegangspad zijn betrokken. Deze componenten zijn vrijwel altijd netwerkapparatuur, besturingssystemen, de database zelf en de applicaties voor gebruik en beheer. Het niet onderzoeken van één van deze componenten kan betekenen dat mogelijk bepaalde toegangsmethoden tot de databases over het hoofd worden gezien.

In figuur 1 is een voorbeeld weergegeven van manieren waarop verbindingen met de Oracle-database tot stand kunnen worden gebracht.

De toegang tot de Oracle-database vindt in veel gevallen plaats via een client-serverapplicatie of via een web- of applicatieserver. Eindgebruikers communiceren met een applicatieserver via de webbrowser of een client-applicatie. De applicatieserver communiceert vervolgens meestal via ODBC (Open Database Connectivity), JDBC (Java Database Connectivity) of SQL*Net om SQL-statements op de achterliggende Oracle-database te kunnen uitvoeren.

Beheerders benaderen meestal via het lokale netwerk direct de Oracle-database voor beheeractiviteiten. Dit gebeurt over het algemeen via Oracle Enterprise Manager (SQL*Net of HTTP), TOAD (The Oracle Application Developer), ISQL*Plus (SQL via het web) en/of SQL*Plus lokaal op het systeem.



Figuur 1. Voorbeeld toegangspaden tot een Oracle-database.

Een veel gemaakte foutieve veronderstelling is dat zowel op het netwerk, de applicatie als de database identificatie en authenticatie noodzakelijk is om op de Oracle-database in te loggen. Voor toegang tot de Oracle-database is het niet noodzakelijk voor een gebruiker om zich op al deze drie niveaus te identificeren en te authenticeren. Alleen een gebruikersnaam en wachtwoord voor de Oracle-database kunnen volstaan, zonder aanmelden op het netwerk en/of de applicaties. Al met al zijn vele logische toegangspaden mogelijk waarmee de Oracle-database kan worden benaderd. Identificatie en authenticatie vinden op verschillende niveaus plaats en kunnen vaak ook worden omzeild.

De Oracle-database kan langs vele logische toegangspaden worden benaderd

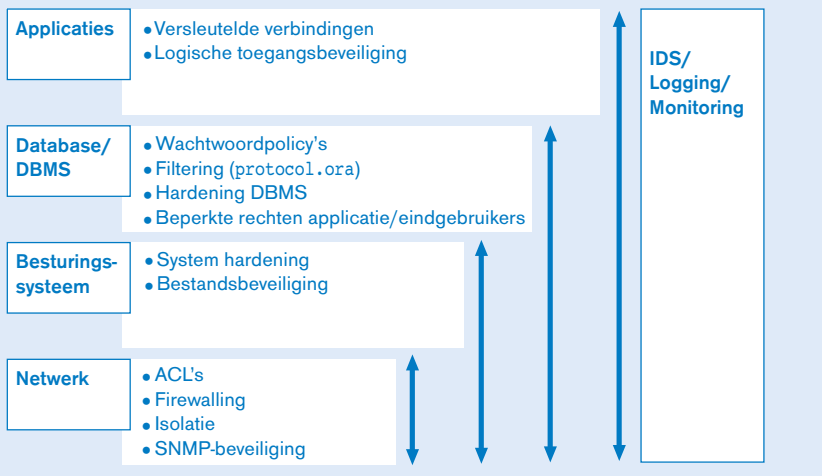
In omgevingen waarin bijvoorbeeld monitoringsystemen aanwezig zijn, vinden we overigens vaak alternatieve mogelijkheden voor toegang tot de database.

Beveiligingsrisico's per gebied

In de vorige paragraaf is aangegeven dat identificatie- en authenticatiemaatregelen op verschillende niveaus in de technische infrastructuur onderkend moeten worden om een volledig overzicht te krijgen van beveiligingsrisico's. Bij de beoordeling van de Oracle-database is het daarom van belang op deze niveaus de beveiligings-

risico's adequaat te analyseren, zoals in figuur 2 is afgebeeld.

In figuur 2 zijn voorbeelden gegeven van maatregelen die getroffen kunnen worden om de bedreigingen rond de Oracle-database te beperken. De figuur geeft ook aan dat beveiliging een gelaagdheid kent. Dit is een algemeen principe dat ook op de beveiliging van Oracle-databases toepasbaar is.



Figuur 2. Gelaagdheid in beveiligingsmaatregelen.

Het is van belang om tijdens het onderzoek naar de beveiliging van de Oracle-database de maatregelen op alle lagen te toetsen aangezien de beveiligingsmaatregelen in hogere lagen steunen op de maatregelen die in de onderliggende lagen zijn getroffen. In de nu volgende paragrafen wordt een aantal veelvoorkomende risico's toegelicht.

Applicaties

Eindgebruikers hebben vaak toegang tot de database via applicaties. De applicatie meldt zich aan onder een generieke gebruikersnaam en haalt de gegevens voor de eindgebruiker op uit de database.

In de praktijk zien we dat dit logisch toegangspad de volgende beveiligingsrisico's oplevert:

Tabel 1. Locatie Oracle-wachtwoorden.

Pakket	Locatie wachtwoorden
iSQL*PlusExtension	Registry: ORACLE\iSQLPlus\Servers\ServerXX
Enterprise management EM	$OH/sysman/config/pref/dbastudio-root.crd
TOAD	<Drive>:\<Program Files>\questsoftware\toad\toad.ini
SQL*Navigator	Registry
Jdeveloper	connections.xml
Oracle Developer for .Net	Registry

- De generieke applicatieaccounts die namens gebruikers vanuit de applicatie inloggen op de database hebben vaak té hoge rechten in de database en kunnen hierdoor gegevens muteren die nooit voor de eindgebruiker toegankelijk hadden mogen zijn. Het risico van misbruik is aanwezig als eindgebruikers toegang tot deze applicatieaccounts weten te verkrijgen vanuit de applicatieschil.
- De namen van generieke applicatieaccounts zijn algemeen bekend en op het internet beschikbaar. Uit onze ervaring blijkt bovendien dat de wachtwoorden van deze applicatieaccounts zwak of zelfs identiek zijn aan de gebruikersnaam. Voorbeelden hiervan zijn gebruikersnamen zoals SAPR3, APPS, PEOPLE, TOAD en JDE.
- De wachtwoorden van de generieke applicatieaccounts zijn vaak niet gekoppeld aan een Oracle-wachtwoordbeleid (Oracle-profiles) en worden hierdoor niet periodiek gewijzigd.
- Ten behoeve van het beheer van de Oracle-database zijn diverse applicaties beschikbaar. Vele van deze applicaties slaan Oracle-gebruikersnamen en -wachtwoorden op het lokale systeem op. Een aantal voorbeelden van applicaties is in tabel 1 weergegeven.

Bij het onderzoeken van de beveiliging van een Oracle-installatie is het van belang specifieke aandacht te besteden aan de applicatieaccounts.

Database

Standaardwachtwoorden

Na installatie van Oracle 7-, 8- of 9-databases wordt een aantal gebruikersnamen met standaardwachtwoorden geïnstalleerd. In veel gevallen zijn deze accounts aanwezig ook als deze functioneel niet noodzakelijk zijn. Het is mogelijk in te loggen op de database met deze accounts en toegang te verkrijgen tot de gegevens in de Oracle-database.

Enkele veelvoorkomende standaardwachtwoorden zijn weergegeven in tabel 2.

Een uitgebreide lijst van standaardgebruikersnamen en -wachtwoorden is op de volgende url aanwezig: www.petefinnigan.com/default/oracle_default_passwords.xls.

In Oracle 10g wordt tijdens de installatie gevraagd de wachtwoorden van de standaardaccounts SYS, SYSTEM en DBSNMP te wijzigen, de overige accounts zoals OUTLN worden standaard geblokkeerd. Dit maakt Oracle 10g voor wat betreft standaardwachtwoorden minder kwetsbaar dan Oracle 7.x-, 8.x- en 9.x-installaties.

Gebruikersnaam	Wachtwoord	Functie
DBSNMP	DBSNMP	Oracle Intelligent Agent
OUTLN	OUTLN	Outline stored procedures
CTXSYS	CTXSYS	Oracle Text/Intermedia Text/Context option
MDSYS	MDSYS	Oracle Spatial administrator
SYS	CHANGE_ON_INSTALL	Super user
SYSTEM	MANAGER	Super user

Tabel 2. Standaard-wachtwoorden.

Databaselinks

Voor het maken van koppelingen tussen verschillende Oracle-databases wordt vaak gebruikgemaakt van zogenaamde databaselinks.

Wanneer Oracle-verbindingen worden gemaakt met databaselinks worden de authenticatiegegevens standaard onversleuteld verstuurd. Door het onderscheppen van het netwerkverkeer van databaselinks kunnen in dat geval authenticatiegegevens worden achterhaald. Deze authenticatiegegevens kunnen vervolgens worden gebruikt om in te loggen op de Oracle-database. Oracle 10g verstuurt deze authenticatiegegevens standaard versleuteld, in Oracle 9.2.0 en 8.1.7 dient versleuteling expliciet te worden aangezet door middel van het opnemen van de instelling `dblink_encrypt_login = TRUE` ('enforce password for distributed login always be encrypted') in `init<sid>.ora`.

Een ander veelvoorkomend risico is dat een databaselink is opgeslagen met een onversleuteld wachtwoord óf zelfs zonder wachtwoord. Indien bovendien de parameter `O7_DICTIONARY_ACCESSIBILITY` ('Version 7 Dictionary Accessibility Support') is geactiveerd, kan een Oracle-gebruiker met het `SELECT ANY TABLE`-privilege de onversleutelde wachtwoorden achterhalen om vervolgens toegang te verkrijgen tot de gekoppelde database(s).

Besturingssysteem

Afscherming Oracle-wachtwoorden

Het besturingssysteem waarop Oracle is geïnstalleerd, kan voor diverse beveiligingsrisico's zorgen die impact hebben op de beveiliging van de database. De Oracle-wachtwoorden zijn op diverse plaatsen te achterhalen zonder dat de beheerders en gebruikers zich hiervan bewust zijn.

1. *Onversleutelde wachtwoorden in de processenlijst van het UNIX-besturingssysteem*
   Indien het wachtwoord van de netwerkdienst SNMP (Simple Network Management Protocol) niet is gewijzigd, kan dit leiden tot het achterhalen van Oracle-wachtwoorden uit de UNIX-processenlijst. Door de SNMP MIB (Management Information Base)-tree op te vragen kan de processenlijst ongeautoriseerd worden verkregen. In deze processenlijst kan, indien er een SQL*Plus-commando actief is op UNIX, een Oracle-wachtwoord zichtbaar zijn waarmee vervolgens kan worden aangemeld op de Oracle-database.

2. *Oracle-configuratiebestanden, commandohistorie en commandoscripts op UNIX*
   In een aantal Oracle-configuratiebestanden kunnen onversleutelde wachtwoorden aanwezig zijn, bijvoorbeeld in de bestanden `SNMP_RW.ORA` ('configuration information for the Oracle Intelligent Agent') en `LISTENER.ORA` ('configuration file for the Oracle-listener').
   Op het UNIX-bestandssysteem zijn vaak commandohistoriebestanden aanwezig, bijvoorbeeld `.sh_history`. In de screenprint van figuur 3 is op regel 646 te zien dat SQL*Plus is opgestart op UNIX met de gebruikersnaam `DBA` en het wachtwoord `LETMEIN`.

In veel gevallen worden beheeractiviteiten en applicatieondersteunende processen op het niveau van het besturingssysteem uitgevoerd. Door middel van commandoscripts worden dan hulpprocessen gestart en SQL-queries op de Oracle-database gedraaid.

In deze commandoscripts worden vaak authenticatiegegevens opgeslagen met onversleutelde wachtwoorden. Wanneer de autorisaties op de bestanden niet adequaat worden beheerd, kan elke gebruiker die deze scripts kan lezen ongeautoriseerd toegang verkrijgen tot de Oracle-database. Een voorbeeld hiervan is een UNIX-script dat wordt gebruikt om periodiek een kopie te maken van de Oracle-database. In dit script zal dan het volgende commando voorkomen:

```
sqlplus -s <gebruikersnaam>/
<wachtwoord>@<sid>
```

Bestandspermissies

De Oracle-database slaat gegevens op die uiteindelijk worden opgeslagen in bestanden op het filesysteem. Deze bestanden dienen te worden beschermd tegen ongeautoriseerde toegang. Bij het beoordelen van de beveiliging van de Oracle-database dienen deze bestandspermissies dan ook te worden onderzocht.

```
xterm
631  l
632  cd admin/
633  l
634  cd ..
635  cd bin
636  l
637  ./lsnrctl
638  cd $ORACLE_HOME
639  rpm -qa | grep -i ucd-snmp
640  find . -name "*ucd*"
641  exit
642  cd /packages/Disk1
643  ./runInstaller
644  export DISPLAY=192.168.123.3:0.0
645  ./runInstaller
646  sqlplus dba/letmein@orcl
647  uname
648  id
649  ifconfig
650  history

oracle@linux:~>
```

Figuur 3. Authenticatie-gegevens in shell history.

Wanneer de bestandspermissies te ruim zijn gedefinieerd, bestaat het risico dat de databestanden kunnen worden gekopieerd of zelfs verwijderd.

De Oracle-gebruiker en de dba-groep dienen eigenaar te zijn van de Oracle-databestanden. Alleen de Oracle-gebruiker en de dba-groep moeten lees- en schrijfrechten hebben op de databestanden. De locatie van de databestanden kan per installatie verschillen. Oracle heeft hier echter een standaard voor ontwikkeld: OFA – de Optimal Flexible Architecture. Deze standaard bevat een aantal richtlijnen en aanbevelingen voor locaties van bestanden en directories.

Oracle kent naast databestanden een aantal configuratiebestanden. In deze bestanden is de configuratie van de Oracle-database vastgelegd. Voorbeelden van deze bestanden zijn: init<sid>.ora, listener.ora, protocol.ora en spfile<sid>.ora. Dit is mede afhankelijk van de gebruikte versie van de Oracle-database.

Deze configuratiebestanden bevatten belangrijke gegevens over de inrichting van bijvoorbeeld de toegangsbeveiliging. In de praktijk zien we dat deze bestanden vaak toegankelijk zijn voor alle gebruikers met een account op de server waar de Oracle-database op actief is. Wanneer de bestandspermissies te ruim zijn gedefinieerd, bestaat het risico dat de configuratiebestanden kunnen worden gemuteerd of zelfs verwijderd, wat de beschikbaarheid van de database negatief kan beïnvloeden.

Remote O/S-authenticatie

Binnen Oracle bestaat de mogelijkheid om naast de normale databaseaccounts zogenaamde OPS$-accounts te definiëren. OPS$-accounts zijn databaseaccounts waarbij op besturingssysteemniveau ook een account met dezelfde naam moet bestaan. Bijvoorbeeld, indien een databaseaccount OPS$<sid>adm bestaat, veronderstelt Oracle dat ook een (extern) UNIX-account `<sid>adm` is gedefinieerd.

In één van de Oracle-configuratiebestanden, te weten `init<SID>.ora`, kan men met de parameter `REMOTE_OS_AUTHENT` instellen dat de database (bij OPS$-accounts) vertrouwt op de authenticatie van een remote besturingssysteem.

Door de combinatie van beide parameterinstellingen is het mogelijk dat een (kwaadwillende) gebruiker vanuit een ander, niet-vertrouwd IP-adres met behulp van een OPS$-account ongeautoriseerd toegang kan verkrijgen tot de database.

Netwerk

De Oracle-listener (meestal TCP-poort 1521) verzorgt netwerkconnectiviteit tussen clients, applicatieservers en de database. De praktijk leert ons dat de beveiliging van de listener veel te wensen overlaat. De veel gemaakte fouten zijn bij beveiligingsspecialisten al jaren bekend. Toch komen we de configuratiefouten nog altijd tegen. Wij zullen hier een aantal van de meest voorkomende Listener-beveiligingsrisico's bespreken.

De listener wordt beheerd via de lsnctl utility. De listener-utility wordt onder meer gebruikt om de Oracle-listener (die noodzakelijk is voor het kunnen benaderen van de Oracle-database over het netwerk) te stoppen, (her)starten en de loggingconfiguratie in te stellen.

De listener is standaard *niet* voorzien van een wachtwoord en is via het netwerk te benaderen (met uitzondering van Oracle 10.x). Dit houdt in dat iedereen onge-

autoriseerd netwerkverkeer naar de databaseserver kan sturen waardoor de database onbenaderbaar kan worden. Dit risico is beperkt in Oracle 10.x doordat alleen vanaf de localhost de listener benaderd kan worden.

De listener kan worden beveiligd tegen ongeautoriseerd gebruik door deze te voorzien van een wachtwoord. Dit wachtwoord dient dan ook versleuteld te worden opgeslagen.

```
LSNRCTL> set password <password>
```

Verder is het mogelijk de logbestanden en locaties te definiëren. Hiermee is het vaak mogelijk toegang tot het besturingssysteem van de Oracle-server te krijgen, door bijvoorbeeld het logbestand van de listener de hernoemen naar /home/oracle/.rhosts en vervolgens een logentry te creëren met hierin '+ +'.

Op de databaseserver kan tevens filtering worden geactiveerd door middel van sqlnet.ora of protocol.ora (afhankelijk van Oracle-versie). De volgende instellingen kunnen in protocol.ora/sqlnet.ora worden opgenomen om alleen verbindingen vanaf geautoriseerde IP-adressen toe te staan:

```
tcp.validnode_checking = yes
tcp.invited_nodes  =  (x.x.x.x  |  name,
x.x.x.x | name)
tcp.excluded_nodes=  (x.x.x.x  |  name,
x.x.x.x | name)
```

De listener is standaard niet voorzien van een wachtwoord en is via het netwerk te benaderen

Conclusie

In dit artikel is de beoordeling van de beveiliging van de Oracle-database inzichtelijk gemaakt door in te gaan op de samenhang van de Oracle-database met haar omgeving binnen de technische infrastructuur. Bovendien zijn binnen het complex van componenten van de technische infrastructuur enkele veelvoorkomende beveiligingsrisico's van de Oracle-database uitgewerkt.

Betoogd is dat het bij de afbakening van de audit van groot belang is om alle logische toegangspaden naar de Oracle-database in de audit mee te nemen. Dit om er zeker van te zijn dat de relevante beveiligingsrisico's worden meegenomen in de beoordeling.

Een auditaanpak voor de Oracle-database waarin aandacht is voor beveiligingsmaatregelen op de verschillende relevante niveaus in de technische infrastructuur is cruciaal om de relevante beveiligingsrisico's te kunnen identificeren.