Oracle en Security (I)

Back-up, recovery en security alerts

Er bestaat geen software zonder bugs. Ook een Oracle database is een IT applicatie als elke andere. Het feit dat de leverancier meer 'security conscientious' is dan gemiddeld, wil dan ook niet zeggen dat bij verkeerd of onzorgvuldig gebruik geen mogelijkheden ontstaan voor misbruik. In deze artikelenserie worden de komende tijd security-mogelijkheden belicht welke standaard of optioneel in de Oracle database aanwezig zijn. Daarbij worden vakgebieden beschreven die traditioneel tot de dba behoren, en wordt onderzocht wat het de security officer hieraan kan toevoegen. Tevens zullen regelmatig actuele security alerts aan de orde komen.

Bij Motiv IT Masters is security de rode draad door het portfolio op het gebied van database technologie, networking en webtechnologie. Met behulp van een aantal thema's levert het bedrijf zakelijke oplossingen waarbij security op passende wijze geregeld is. Gerard Uiterwaal, expert op Oracle- en securityterrein en medeoprichter van Motiv, licht vanaf heden in elke uitgave van Optimize een security-onderdeel toe.

Security in een Oracle omgeving kan vanuit twee totaal verschillende invalshoeken worden bekeken:

- *De klassieke dba* beschikt over veel technische kennis. Hij zoekt bescherming met technische hulpmiddelen tegen technische catastrofen. Sturing vindt plaats vanuit de techniek en niet vanuit het bedrijfsbelang.
- *De security officer* is aangesteld om te voorkomen dat mensen met kwade bedoelingen het bedrijf kunnen hinderen in het uitoefenen van de bedrijfswerkzaamheden.

Bij bedrijven met zelf geschreven Oracle applicaties, veelal geschreven voor de ondersteuning van de primaire bedrijfsprocessen, is de klassieke dba-functie altijd aanwezig. Het is de afdeling die zorgt voor de techniek rondom de Oracle database. De werkzaamheden betreffen zaken als de installatie van software, het creëren en onderhouden van de database, performance en tuning, oplossen van bugs, back-up en recovery. Hiernaast is de dba verantwoordelijk voor autorisatie rondom de Oracle database. De laatste twee onderdelen behoren tot het takenpakket van de dba, niet vanwege het security aspect, maar omdat de dba de techniek in huis heeft om die taken te kunnen uitvoeren. Voor zover er naar beveiliging gekeken wordt, heeft dat vooral betrekking op beveiliging tegen technische problemen die kunnen ontstaan.

Security in een Oracle omgeving kan vanuit twee totaal verschillende invalshoeken worden bekeken

Bedrijfsmatig

De security officer IT is een functie die relatief recent ontstaan is. De functie wordt veelal uitgevoerd door mensen met een bedrijfskundige achtergrond. De sturing is dan ook bedrijfsmatig. Binnen deze functie wordt wel degelijk rekening gehouden met mensen, van binnen of van buiten het bedrijf die kwade bedoelingen hebben. Een voorname invalshoek hierbij is het beschermen tegen hackers.

Het is niet ongebruikelijk dat beide afdelingen niet goed met elkaar overweg kunnen. Op de dba afdeling liggen eigenlijk altijd vele kleine projecten klaar die de Oracle applicaties kunnen verbeteren, waar men door de werklast echter niet aan toekomt. Verzoeken van de security officer voor aanpassingen worden ook als zo'n project beschouwd. De baten hiervan worden gezien als secundair. De dba-afdeling vraagt zich eerder af: 'Zolang we nog niet optimaal kunnen werken in onze omgeving, moeten we er dan meteen vanuit gaan dat iedereen kwade

bedoelingen kan hebben?' Dit wordt als onwaarschijnlijk ervaren. In de komende tijd willen we via deze rubriek enerzijds een aantal vakgebieden beschrijven die traditioneel op het terrein van de dba liggen en kijken wat het gezichtspunt van de security officer hieraan toevoegt. Hierbij worden ook de security-mogelijkheden belicht welke standaard of optioneel in de Oracle database aanwezig zijn. Te denken valt aan Advanced Security, Encryptie (o.a. label security), Virtual Private Database, Single Sign-on framework, Strong Authentication etc. Hiernaast zullen we een aantal actuele security alerts bespreken om u inzicht te geven in de gevaren waar deze alerts voor waarschuwen.

Back-up en Recovery

Back-up en recovery zijn wel degelijk security issues. Veel bedrijven kunnen zonder hun database(s) niet overleven en het bestrijden van het gevaar data kwijt te raken is dan ook een belangrijk onderdeel van het werk van de dba-afdeling. Het is onvermijdelijk om dit werk bij deze afdeling te leggen, dit is namelijk de plaats waar de benodigde technische kennis voorhanden is voor de uitvoering. Anderzijds heeft dit er in het verleden toe geleid dat er alleen met een technische blik naar dit onderwerp gekeken wordt, ook vanuit het management. Het is nog steeds zeer gebruikelijk het volgende in een automatiseringsplan terug te lezen: *'Er dient zorg gedragen te worden voor een goede back-up en recovery procedure.'* Het komt nog weinig voor dat een concretere eis gesteld wordt zoals *'Het moet onmogelijk zijn dat er meer gegevens dan … verloren kunnen gaan.'* Een gevolg is dat back-up en recovery veelal op een technische manier worden opgezet. Er wordt dan voornamelijk naar het dagelijkse proces (back-up) en minder naar het incidentele proces (recovery) gekeken, terwijl de mogelijkheid om te kunnen recoveren toch de doelstelling is. Tevens worden technieken en hardware apart beoordeeld op hun wenselijkheid, in plaats van eisen te formuleren en te bekijken welke technieken en hardware deze eisen kunnen verwezenlijken. *'Er is budget voor een tape robot, en we hebben eigenlijk ook een stand-by database nodig voor een bedrijfskritische applicatie'.*

Een gevolg van de focus op de dagelijkse processen is dat back-up geoptimaliseerd wordt. Hoe kan ik met zo min mogelijk inspanning een juiste back-up maken van mijn essentiële data? Terwijl dit vaak grote negatieve gevolgen heeft voor de tijd die nodig is om na een catastrofe weer in de lucht te komen.

Voor een security officer komt back-up en recovery op een heel ander moment in de picture. Eén van zijn eerste acties binnen een bedrijf zal het opzetten zijn van een informatie beveiligingsbeleid. Hierin zal onder andere voor elke applicatie beschreven worden hoe belangrijk die is. Van hieruit worden eisen opgesteld waaraan de applicatie zal moeten voldoen. Daarin wordt onder meer beschreven hoelang de applicatie bij een calamiteit uit de lucht mag zijn, en hoeveel gegevens bij een calamiteit verloren mogen gaan. Dit is een veel beter uitgangpunt om te bepalen hoe back-up en recovery ingericht moet worden.

Security Alerts

Een Oracle database is een IT applicatie als elke andere. Het feit dat de leverancier van deze applicatie meer 'security conscientious' is dan gemiddeld, wil dan ook niet zeggen dat bij verkeerd of onzorgvuldig gebruik geen mogelijkheden ontstaan voor iemand met kwade bedoelingen om hier misbruik van te maken. Op de Oracle internet site OTN (http://otn.oracle.com/deploy/security/alerts.htm) staat de lijst met genummerde security alerts vanaf oktober 2001. Op dit moment (7 januari 2004) staan er 62 alerts op deze website vermeld. Dit houdt zeker niet in dat er

Security Alert #59

Datum	Ontstaan: 20 oktober 2003 Aangepast: 3 november 2003
Ernst	2
Gevaar	Het is mogelijk om zoveel gegevens aan de oracle binaries (oracle en oracleO) te geven dat hierbij een buffer overloopt.
Risico	Hierdoor is het mogelijk dat niet bedoelde code kan worden uitgevoerd
Producten en versies	Oracle 9i Database Release 2, Version 9.2.x Oracle 9i Database Release 1, Version 9.0.x
Platforms	Alle UNIX versies Alle Linux versies
Rand-voorwaarden	Gebruiker moet kunnen aanloggen op de database server
Oplossing 1	Geef privilege om oracle binaries uit te voeren slechts aan beperkte groep gebruikers
Technische invulling oplossing	# cd $ORACLE_HOME/bin # chmod o-x oracle oracleO
Oplossing 2	Voer patch voor security alert #59 uit.

Tabel 1. Voorbeeld van een security alert, zoals die op de OTN-website worden gepubliceerd.

meer dan 60 security leaks in Oracle zouden zitten. De alerts zijn publicaties die de zogenaamde 'best practices' beschrijven omtrent het omgaan met Oracle. Het grote verschil met de normale beveiliging van uw Oracle omgeving is dat deze security alerts gericht zijn om een omgeving te creëren waarin het niet mogelijk is dat kwaadwillende personen misbruik kunnen maken van deze eventuele 'security leaks'. Deze best practices beschermen tegen de volgende gevaren:

Denial of Service.
Het ervoor zorgen dat de applicatie niet gebruikt kan worden. De applicatie houdt zich zoveel met de aanvaller bezig dat ze geen tijd meer over heeft voor het normale werk, ofwel de applicatie crasht.

Execute code
Het uit de applicatie breken en op de machine uitvoeren van code die meegebracht is of al op de machine aanwezig is, maar die geen onderdeel uitmaakt van de applicatie. Met deze code wordt vervolgens onheil op de machine uitgericht.

Unauthorized access
Het benaderen van gegevens die niet via de applicatie benaderd mogen worden.

Een voorbeeld van een security alert is te zien in tabel 1. Deze security alert wijst op een veel voorkomend soort gevaar. In alle software wordt ruimte gereserveerd (een buffer) om gegevens kwijt te kunnen. Indien geprobeerd wordt om hier meer gegevens in te stoppen dan er in past, gaat er natuurlijk iets mis. Hackers proberen vaak uit of dit leidt tot de mogelijkheid om hiermee stukjes ongeautoriseerde code uit te laten voeren door de eigenaar van de software die ze aanvallen. Veelal heeft deze eigenaar meer privileges dan een normale gebruiker. Dat is ook het geval voor de eigenaar van de Oracle software.

Voor zover er naar beveiliging gekeken wordt, heeft dat vooral betrekking op technische problemen die kunnen ontstaan

Vulnerability

In dit geval kan er alleen misbruik gemaakt worden van deze vulnerability (zwakte) door gebruikers op de server waar de database draait. Bij het gebruik van een applicatieserver of een goed ingestelde firewall zullen gebruikers van buiten dit niet voor elkaar kunnen krijgen. Het eerste algemene advies wat dan ook door Oracle gegeven wordt is dan ook om zo min mogelijk gebruikers rechtstreeks op de database server toe te laten.
De eerste manier om te voorkomen dat mensen gebruik maken van de vulnerability zoals in deze alert beschreven, bestaat eruit het aantal gebruikers dat gebruik mag maken van de Oracle software drastisch te beperken. Indien voor oplossing 1 gekozen wordt kunnen alleen nog de gebruiker oracle en gebruikers in de unix groep dba rechtstreeks op de machine gebruik maken van de Oracle software. De patch van oplossing 2 zorgt ervoor dat de gereserveerde ruimte in de buffer niet meer overschreden kan worden.

Privileges

Wat zijn nu de redenen dat niet elke dba ervoor zal kiezen om één of meerdere van deze oplossingen te implementeren? Ten eerste kost de implementatie van beide oplossingen tijd. Voor de eerste oplossing moet er gekeken worden naar welke gebruikers de Oracle software rechtstreeks op de database server benaderen en dit nu niet meer kunnen. Kunnen ze misschien ook via sql*net gaan werken en wat zijn de consequenties hiervan? Moeten één of meerdere hiervan misschien worden opgenomen in de dba groep, maar dan krijgen ze veel meer privileges (ze kunnen bijvoorbeeld de database stoppen)?
Bij het gebruik maken van een gekochte applicatie is het misschien helemaal niet mogelijk om alle gebruikers via sql*net te laten werken. Aangezien al deze zaken op elke site anders zijn, zal dit eerst uitgezocht moeten worden.
De tweede oplossing is het installeren van een patch. Ook dit dient eerst uitvoerig getest te worden omdat vrijwel elke patch bijwerkingen heeft.

De security officer zal aangeven dat minstens een van beide oplossingen geïmplementeerd zal moeten worden of misschien wel beiden. De dba die een en ander moet uitvoeren zal veelal inschatten dat er geen tijd voor is in de planning, met soms alle gevolgen van dien…

Gerard Uiterwaal
is Oracle- en security-expert en werkzaam bij Motiv IT Masters. Indien u in een van de volgende uitgaven van Optimize graag een specifiek onderdeel belicht zou willen zien dan kunt u dit aangeven via e-mail: gerard.uiterwaal@motiv.nl. De auteur streeft ernaar zoveel mogelijk vragen te beantwoorden.