Trends in beveiliging

Oracle en Security (7)

Het nieuwe jaar leent zich ervoor om te kijken naar de algemene veiligheid op het gebied van de ICT. In hun '9e jaarlijkse onderzoek over de inzet en het gebruik van ICT' geeft Ernst & Young een aantal interessante cijfers over computerbeveiliging. Zo wordt geconstateerd dat bijna veertig procent van de ondervraagden denkt dat ze in 2005 meer aan ICT-beveiliging zullen uitgeven.

Ook wordt geconstateerd dat directieleden en topmanagers zich steeds meer bewust zijn van de bedreigingen die door het eigen personeel worden veroorzaakt. Tegelijkertijd geeft meer dan zeventig procent van de organisaties die aan het onderzoek hebben meegedaan, aan dat het beveiligingsbewustzijn van medewerkers geen topprioriteit is. Het is een opzienbarende constatering, dat er weinig bewustwording is - terwijl hier al een hoop bereikt kan worden zonder investering - , terwijl er tegelijkertijd wel de bereidheid bestaat om geld te investeren in beveiliging. Een laatste constatering uit dit onderzoek is dat teveel organisaties informatiebeveiliging niet van belang vinden als er geen zichtbare aanval is, terwijl de meeste aanvallen de openbaarheid niet halen. Interne incidenten worden meestal verzwegen. Tot het afgelopen jaar was het voor mij slechts een aanname dat er zich wel degelijk incidenten op dit vlak afspelen. Doordat ik het afgelopen jaar veel met allerlei mensen uit allerlei branches over dit issue heb gesproken, hoor ik steeds vaker dat iets dergelijks zich ook bij mijn gesprekspartner op het werk heeft voorgedaan. Vaak betreft het stelen van informatie bij het overstappen naar een andere baan. En altijd wordt erbij verteld dat het incident binnenskamer is gehouden.

Trends

Hoe vertaalt zich dit naar het gebruik van Oracle databases in Nederland? Waar schort het aan en wat zijn de algemene trends? Omdat Motiv zich nu al meer dan een jaar bezig houdt met het uitvoeren van security scans op de Oracle database, is het mogelijk wat algemene trends te ontdekken:

Toegangsbeveiliging

In zijn algemeenheid is de toegangsbeveiliging zwaar onvoldoende. Tot aan de komst van Oracle 10g (en die zien we eigenlijk nog niet in productiesystemen) kost het veel beheersinspanning om ervoor te zorgen dat er geen standaard accounts open staan met een default wachtwoord. Het grote probleem hiervan is dat hiermee een eventuele kwaadwillige bij een default-installatie de beschikking krijgt over een lijst met alle gebruikersnamen (de view ALL_USERS). Meestal blijkt er hiermee een gebruiker te vinden te zijn met een zwak wachtwoord en genoeg privileges om bij de view DBA_USERS te kunnen. Met de informatie die hierin staat is het mogelijk om rustig, thuis te onderzoeken of er bij nog meer accounts ingebroken kan worden. Dit blijkt meestal mogelijk.

Patches

Oracle is de afgelopen jaren steeds meer security minded geworden. Dit blijkt enerzijds uit de grote aantallen certificaten die Oracle op het gebied van security de laatste jaren heeft gehaald. Anderzijds blijkt het ook uit het grote aantal nieuwe features op het gebied van security in de laatste nieuwe versies van de Oracle database. Als laatste blijkt het ook uit de steeds frequenter uitkomende security patches. Sinds medio vorig jaar is Oracle er toe over gegaan om niet meer ad hoc, maar periodiek security patches uit te brengen. De aangegeven reden hiervoor is dat het op deze manier voor beheerders beter in te plannen wordt. Vele Oracle sites houden zich echter nog

Bijna veertig procent van de ondervraagden denkt dat ze in 2005 meer aan ICT-beveiliging zullen uitgeven

helemaal niet bezig met security patches. Voor degenen die dit wel doen, blijken er een aantal problemen te zijn, die verhinderen dat ze hiermee bij blijven:

- Er zitten nog te vaak fouten in de door Oracle uitgebrachte security patches.
- Er is veel tijd nodig om een test van een patch door de hele ontwikkelstraat te loodsen.
- Er wordt veelal met een beschikbaarheid van 24 x 7 gedraaid.
- Er wordt door Oracle niet aangegeven welke problemen er door een security patch worden opgelost. Dit maakt een prioriteitsbepaling lastig, zo niet onmogelijk. Deze informatie is overigens bij goed zoeken wel te verkrijgen. Onze eigen security scan bijvoorbeeld geeft deze informatie.

Gevoeligheid voor DoS aanvallen

De term 'Denial of Service'-aanvallen heeft een hoog 'hacker' gehalte. En klink als zodanig erg 'ver van mijn bed' voor de gemiddelde DBA. Toch is bijvoorbeeld het op illegale wijze stoppen van de listener voldoende om ervoor te zorgen dat alle databases op die machine onbereikbaar zijn geworden. En in hacker termen heet dat een Denial of Service attack. Eigenlijk zijn alle databases die wij onderzoeken, door gebruikers met meer dan normale kennis - maar zonder bijzondere privileges vanuit het interne netwerk - onbereikbaar te maken. Eigenlijk is er in Nederland nog niet het besef, dat de meeste aanvallen van "hackers" van binnenuit, dus vanaf het eigen netwerk, plaatsvinden. De cijfers hierover uit verschillende bronnen lopen wel iets uiteen, maar er wordt toch meestal gesproken over dat zeventig tot tachtig procent van de aanvallen van binnenuit plaatsvinden. In de VS zijn al een aantal ontslagen medewerkers veroordeeld vanwege het hacken van hun oude werkgevers. Veel van de geconstateerde beveiligingslekken zijn op een eenvoudige en vrijwel kostenloze manier te dichten. Een voorbeeld hiervan is de file-permissies van files die gebruikt worden in een database-omgeving, variërend van executables tot database files. Het kost niets, zowel in geld als in gebruiksgemak, om deze zo dicht mogelijk te zetten, en kan tegelijkertijd wel een hoop problemen voorkomen.

Beveiliging

Nog steeds worden applicaties over het algemeen ontwikkeld zonder speciale aandacht voor de security aspecten. Een gevolg hiervan is dat vele eindgebruikers nog steeds standaard de rollen CONNECT en RESOURCE krijgen, die sinds versie 7 alleen nog maar aanwezig zijn vanwege backwards compatibility. Ook wordt meestal bij oplevering van een nieuwe applicatie aangegeven dat de schema-eigenaar DBA-rechten moet hebben. Meestal blijkt dat onzin te zijn. Dit geldt zowel voor intern ontwikkelde als aangekochte applicaties. Zeker voor kleine organisaties waar geen specifieke Oracle-beheerder aanwezig is, leidt dit tot slecht beveiligde applicaties. Een ander probleem is de zelf geschreven autorisatie modules. Veelal blijkt dat deze modules misschien zelf wel complex genoeg zijn om voldoende beveiliging te bieden, maar dat het relatief eenvoudig is om de module te misbruiken, zonder dat de noodzaak bestaat om te doorgronden hoe hij precies werkt.

Functiescheiding

In de praktijk van afgelopen jaar blijkt dat het begrip functiescheiding met name belangrijk wordt ervaren bij uitbesteding. Van verschillende kanten is ons gevraagd of er niet voor kan worden gezorgd, dat DBA functies (zoals back-up) kunnen worden uitgevoerd door gebruikers die geen leesrechten hebben op de data in een database. Dit omdat er enerzijds privacygevoelige informatie is opgeslagen in de database terwijl anderzijds het beheer inclusief DBA-taken is uitbesteed.

Nog steeds worden applicaties over het algemeen ontwikkeld zonder speciale aandacht voor de security aspecten

Mijns inziens is beveiligingsbewustheid het grootste probleem. Voor veel van de bovengenoemde problemen is een eenvoudige en kosteneffectieve oplossing mogelijk, indien er maar voldoende bij wordt stil gestaan. Bij de bouw van nieuwe applicaties hoeft beveiliging niet tot grote extra kostenposten te leiden, mits er maar vooraf over nagedacht wordt.

Gerard Uiterwaal is Oracle- en security expert en werkzaam bij Motiv. 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.