Oracle en Security (2)

Beveiliging gescheiden van applicaties

Ook vroeger al was het zinnig om, voordat een applicatie daadwerkelijk ontworpen werd, onderzoek te doen naar wie wat met welke gegevens mag doen. Van oudsher leren de informaticadeskundigen ons dat je een security model moet maken op het moment dat je bezig bent met de informatie analyse. Wat deze deskundigen ons eigenlijk zeggen is dat toegang tot informatie onafhankelijk is van de applicaties die gebruik maken van deze informatie.

Een van de meer recente toevoegingen aan het security pallet van de Oracle database is een implementatie van de 'Virtual Private Database' (VPD). Het doel van de VPD is dat iedere gebruiker zijn eigen beeld heeft op de database. Dat klinkt precies hetzelfde als de aloude definitie van views, en wanneer je gaat kijken naar de onderliggende techniek heeft het hier ook veel weg van. Kort gezegd komt het erop neer, dat een extra deel aan de where-clausule wordt toegevoegd, waardoor je, afhankelijk van wie je bent en eventueel waar je bent, andere gegevens te zien krijgt en deze wel of niet kunt bewerken. Met bijvoorbeeld views kun je dit ook zelf bouwen. Het mooie van de VPD is echter dat de security regels rechtstreeks bij de brongegevens (de tabellen) worden vastgelegd in de vorm van security policy's. Vervolgens maakt het niet meer uit op welke manier deze gegevens geraadpleegd of bewerkt worden. Er kan met ad hoc tools gekeken worden. Tevens kunnen er meerdere verschillende applicaties van dezelfde brongegevens gebruik maken. De security policy voor elk stuk informatie is eenduidig vastgelegd en wordt centraal afgedwongen. Een niet te onderschatten voordeel van de VPD is dat de informatie over wie er wat mag met welke tabel gemakkelijk is terug te vinden in de dictionary van de Oracle database. In de views DBA_POLICIES / ALL_POLICIES kan van elke tabel in een oogopslag worden vastgesteld wie er überhaupt select, insert, update en/of delete mogelijkheden hebben. Voor het precies vaststellen wie er bij welke rijen mag komen, staat hierin ook de naam vermeld van de procedure die dit regelt.

> ***De Morris-worm was de eerste worm die op grote schaal servers, verbonden met Internet, aanviel***

De VPD bestaat uit een aantal onderdelen:
- Database logon trigger
- Contexts
- Security Policies

Functioneel gezien doet de VPD het volgende: bij het inloggen van een gebruiker gaat de database logon trigger af. Hierin wordt voor elke gebruiker de context gezet. Alle informatie die van een gebruiker bekend is bij het inloggen aan de database kan in deze context verwerkt worden. Dit kan van alles zijn, bijvoorbeeld of er is ingelogd via internet of juist direct lokaal op de server, de manier waarop de identiteit van de gebruiker bepaald is (database, network, proxy, ...) et cetera. Bij het benaderen van gegevens van een tabel wordt in een security policy bepaald wat gebruikers met een bepaalde context mogen doen met die gegevens.

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 in deze rubriek telkens een security-onderdeel toe.

Zoals uit bovenstaande blijkt is de security op deze manier volledig gescheiden van de applicaties. Ook wordt bij een tabel direct vastgelegd wat welke soort gebruiker met gegevens uit deze tabel mag doen. Indien er op enig moment views worden aangemaakt gelden hier automatisch de security policies van de onderliggende tabel(len). Als een nieuwe applicatie gebruik gaat maken van een al bestaande tabel geldt wederom automatisch de al bestaande security policy. Indien nodig kan deze wel worden aangepast of uitgebreid zonder dat hiervoor de reeds bestaande applicaties moeten worden aangepast.

Voor diegenen die de beschikking hebben over een Oracle 9i database heeft Oracle een voorbeeld ter beschikking gesteld van de VPD. Met behulp van een aantal meegeleverde scripts bouw je je eigen VPD. De URL hiervoor is: http://otn.oracle.com/obe/obe9ir2/obe-sec/vpd/vpd.htm.

Security Alerts

Evenals vorige keer zullen we in deze rubriek weer één van de Oracle security alerts wat beter bekijken. De Oracle security alerts kunnen op vele manieren gecategoriseerd worden. De categorie van deze keer is de 'niet Oracle specifieke' alert. In zijn algemeenheid maakt Oracle gebruik van vele externe standaarden en producten. Als in één hiervan een security lek ontdekt wordt, is het waarschijnlijk dat ook de Oracle implementatie gevaar loopt. Security alert #62 is een voorbeeld hiervan. Het algemene product is hier het netwerk protocol 'Secure Socket Layer' ofwel SSL, een protocol dat veel gebruikt wordt om gegevens beveiligd over een openbaar netwerk te transporteren. Vanuit het Oracle alert wordt enerzijds de oplossing voor de Oracle software aangegeven (welke versies hebben last van dit lek en wat is de patch waarmee het probleem opgelost kan worden). Anderzijds wordt er verwezen naar een centrale instantie (CERT) waar het algemene probleem is aangemeld.

Een bewuste aanval van hackers is waarschijnlijk gericht op de producten die zij het beste kennen

CERT

Deze centrale instantie (CERT) is speciaal opgericht voor het registreren van security alerts. Ze is opgericht naar aanleiding van de Morris worm in november 1988. De Morris-worm was de eerste worm (virus) die op grote schaal servers verbonden met het internet aanviel. De schatting is dat binnen een paar dagen de Morris-worm zo'n tien procent van de toenmalige servers heeft platgelegd (6.000 van de 60.000). Niemand wist toen hoe hiermee om te gaan, zodat het - zelfs nadat bekend

Security Alert #62	
Algemeen alert	CERT Advisory CA-2003-26
Datum	Ontstaan: 4 december 2003 Aangepast: -
Ernst	1
Gevaar	OpenSSL handelt standaard een aantal situaties niet goed af. (o.a. te grote getallen en geheugen deallocatie)
Risico	Hierdoor kan een 'denial of service' aanval worden gedaan, tevens is het mogelijk dat niet bedoelde code kan worden uitgevoerd
Producten en versies	Oracle9i Database Server Release 1 en 2 (9.0.1 en 9.2.0)
	Oracle8i Database Server Release 3 (8.1.7)
	Oracle9i Application Server (9.0.2 en 9.0.3)
	Oracle9i Application Server Release 1 (1.0.2.2 en 1.0.2.1s)
	Oracle HTTP Server (8.1.7 , 9.2.0 en 9.0.1)
Platforms	MS Windows NT/2000/XP
	Unix[1]
	Linux[1]
Randvoorwaarden	-
Oplossing	Voer patch voor security alert #62 uit.

[1] Voor exacte versies zie metalink document 249034.1

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

was geworden hoe de worm bestreden moest worden - nog de nodige tijd en moeite gekost heeft om dit bij elke aangetaste server te implementeren. Nu, vijftien jaar later, is er geen zichzelf respecterende grote site meer, die (via servers waarop Unix en Windows draait, verbonden met Internet) niet 'onmiddellijk' de relevante patches aanbevolen door het CERT op zijn systemen zet. Tevens is het een belangrijk onderdeel van het vak van systeembeheerders geworden om te weten hoe besmetting met virussen te voorkomen is en hoe virussen weer op te ruimen zijn, indien een systeem toch besmet raakt.

Security Alert #62

Een bewuste aanval van hackers is waarschijnlijk gericht op producten die zij het beste kennen (met name Windows, Unix en Linux). De volgende anekdote geeft misschien nog enig stof tot nadenken:
Eén van mijn vroegere collega's met een huis op het platteland van Friesland en een klein flatje in Amsterdam heeft alles in het werk gesteld om een autoradio met afneembaar frontje te krijgen van de leasemaatschappij, vanwege het grote aantal autoinbraken in Amsterdam. De autoradio (met frontje er nog op) is uiteindelijk uit zijn auto gestolen voor zijn huis in Friesland.

Het is zeker de moeite waard om de onvermijdelijke regelmatige tests uit te voeren op de patches in de eigen omgeving, om niet degene te zijn die last heeft van hackers op het relatieve platteland van Oracle.

Er is geen zichzelf respecterende grote site meer, die niet 'onmiddellijk' de relevante patches aanbevolen door het CERT op zijn systemen zet.

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, kunt u dit aangeven via e-mail: gerard.uiterwaal@motiv.nl . De auteur streeft ernaar zoveel mogelijk vragen te beantwoorden.

NIEUWS

MKB in Europa wil competitiever worden

Het omlaag brengen van kosten blijft de belangrijkste focus voor het midden- en kleinbedrijf in Europa. Dit blijkt uit een nieuw onderzoek uitgevoerd door Datamonitor in opdracht van Oracle. Meer dan de helft van de respondenten (53%) geeft aan dat hun eerste prioriteit is om hun concurrentiepositie te verbeteren, terwijl slechts 17% het verhogen van de verkopen of het marktaandeel als belangrijkste doel noemt. Maar het onderzoek laat zien dat het standaardiseren van de IT-omgeving en technologieplatforms hoog op hun prioriteitenlijstje staat en dat er als eerste weer in deze zaken geïnvesteerd gaat worden als daar ruimte voor komt. Het onderzoek, *"SME business issues in a re-emergent market"*, is gebaseerd op telefonische diepte-interviews met 4.480 senior executives bij bedrijven in 19 landen in Europa en het Midden-Oosten.
De wens om hun concurrentiepositie te verbeteren door kostenreductie was duidelijk de top prioriteit voor het MKB en kwam aanzienlijk hoger uit dan de twee daarop volgende doelstellingen - de behoeften aan een consistente IT-omgeving en betere interne samenwerking - die ieder 34% scoorden. Hoewel er financieel betere tijden in het verschiet liggen laat het rapport toch zien dat nieuwe investeringen "waarschijnlijk nog een half jaar tot een jaar op zich laten wachten".
Volgens Datamonitor verschilt de behoefte aan IT consistentie per sector. De productiesector en de overheid zijn er het meest in geïnteresseerd en retail, de groothandel en engineering het minst. De behoefte aan meer en betere managementinformatie staat met 24% op de vierde plaats op het prioriteitenlijst van het MKB in Europa. Andere prioriteiten die de respondenten noemen zijn verbetering van de samenwerking met externe partijen (18%), het verhogen van de verkopen en het marktaandeel (17%) en het voldoen aan standaarden en wetgeving die gelden binnen de sector (13%).

Datamonitor concludeert dat IT-budgetten die binnen drie tot zes maanden drastisch gereduceerd zijn mogelijk wel 18 maanden nodig hebben om terug op het oude niveau te komen. De meest waarschijnlijke volgende stappen binnen het MKB zijn het doorvoeren van meer kostenreducerende maatregelen, interne herstructurering, het plannen van groeiscenario's en het ontwikkelen van een roadmap voor de benodigde IT en andere middelen.