Database is een open boek

Beveiliging laat vaak te wensen over

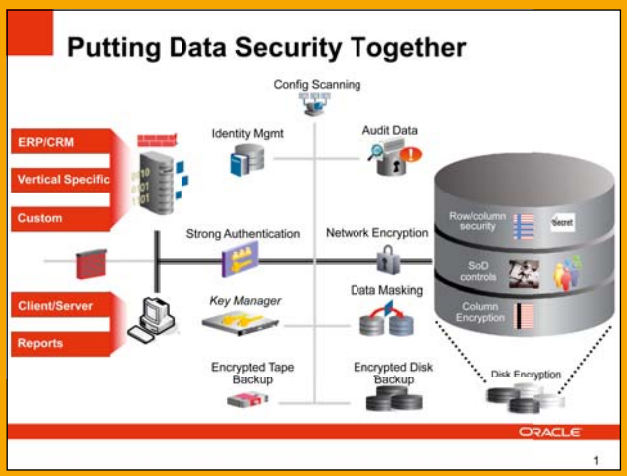
'Security inside out' is het motto, waarmee Oracle een nieuw tijdperk van IT-risico's binnentreedt. De cloud, virtualisatie, sterk groeiende en in aantallen toenemende databases maken beveiliging tot een belangrijk item in de IT. De International Oracle User Group bevestigt dit in haar meest recente 'Data Security Survey'. In 2010 zijn in 43% van de ondervraagde bedrijven de uitgaven voor beveiliging verhoogd. En 84% geeft – al dan niet vrijwillig - binnen de IT zeer hoge prioriteit aan beveiliging.

Dat beveiliging lang niet altijd optioneel is heeft te maken met wetgeving. Van de door de IOUG ondervraagde bedrijven moet ruim de helft voldoen aan de Sarbanes-Oxley Act (SOX), bijna een kwart aan de eisen van de creditcard-industrie (PCI), eenderde aan lokale wetgeving en nog eens eenderde aan Hipaa/Hitech. Maar heel regelmatig blijkt de beveiliging tekort te schieten. Niet alleen door aanvallen van buitenaf overigens. Bijna de helft van alle beveiligingslekken komen uit de eigen organisatie en kunnen variëren van pure onwetendheid tot bewust en met kwade bedoelingen gekopieerde of gestolen informatie.

Oracle zet met de 11g fusion middleware in op service oriented security, waarbij de complete stack kan worden beveiligd. 'Security inside out' bestaat uit Identity Management, Database Security en Infrastructure Security. Onder identity management zijn begrepen directory services (storage), access management (autorisatie en single sign-on) en identity administration.

Identity Management 11g is een pakket dat service-oriented beveiliging biedt. In plaats van een set technologieën in silo's, waaruit je toegangscontrole, permissies en beveiliging van directories stopt, heeft Oracle ervoor gekozen om deze mogelijkheden als services aan te bieden. Zij zijn gebaseerd op de Oracle standaarden en worden volledig geïntegreerd in de business applications. Alles wordt geconcentreerd in een enkele user interface. Als je bijvoorbeeld de expiratie van de wachtwoorden in Oracle Access Management wilt koppelen aan de wachtwoord reset-mogelijkheden van Identity management, dan kan dat.

Er is een nieuwe grafische interface gebouwd op basis van het Application Development Framework (ADF) met een navigator van waar uit de beveiliging kan worden aangestuurd. De architectuur is gebaseerd op shared services en de workflow op BPEL. De access manager is overigens omgebouwd op Java; voorheen was deze in C gecodeerd. Nieuw is een 'Adaptive Acces Manager 11g', bedoeld voor fraudepreventie.
Aan de overname van Sun heeft Oracle ook op beveiligingsgebied een aantal nieuwe producten overgehouden, waaronder Oracle Identity Analytics, OpenSSO STS (Security Token Service) en OpenSSO Fedlet voor authenticatie en autorisatie.



Zo ziet Oracle het complete beveiligingsplaatje voor de database.

Database

Op beveiligingsgebied is Oracle erg actief rond de database. Verwonderlijk is dat niet, want daar staan de gevoelige data. Bovendien hoef je geen applicaties te veranderen of de organisatie

overhoop te gooien. De meeste veiligheidsbreuken (90%) vinden ook plaats in de database, vertelt John Abrahams van Oracle tijdens een door Oracle georganiseerde bijeenkomst.

De database security omvat een audit vault, label security, database vault en een database firewall. Oracle heeft hiervoor een strategie ontwikkeld met verschillende beveiligingslagen:
- Encryption en masking
- Access Control
- Auditing en tracking
- Monitoring en blocking

Veel mensen in de organisatie kunnen bij de opgeslagen data. Daar kan dus ook makkelijk misbruik van worden gemaakt; er zijn voorbeelden te over van gekopieerde of gestolen database-gegevens. Abrahams snapt mede daarom niet zo goed waarom in minder dan een kwart van de bedrijven de data versleuteld wordt opgeslagen. Encryptie is namelijk heel eenvoudig te realiseren, het verhoogt het cpu-gebruik maar met enkele procenten, je hoeft er niets voor aan de applicaties te veranderen en het heeft geen invloed op de performance. Met Oracle advanced security is het een kwestie van een enkel vinkje zetten, waardoor de potentiële misbruiker niets meer aan de data heeft. De key zit uiteraard niet in de database.

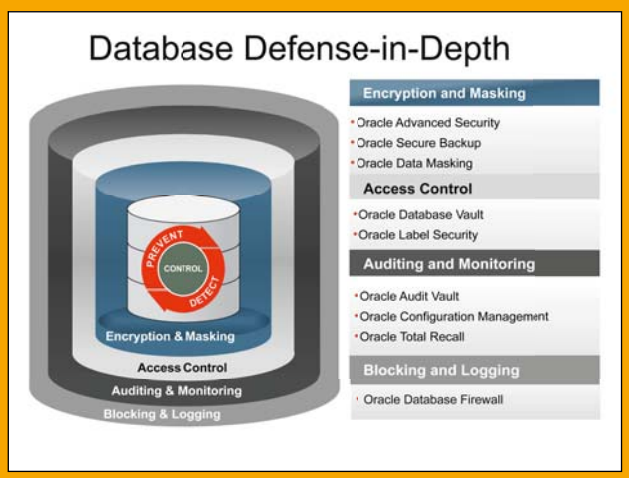
Een andere mogelijkheid om te voorkomen dat bepaalde geprivilegieerde gebruikers gevoelige data kunnen lezen of kopiëren is de Database Vault. Deze sluit de toegang tot gevoelige data af, terwijl de DBA wel zijn werk kan blijven doen. Oracle Label Security classificeert data en gebruikers, waardoor de access control kan worden geautomatiseerd. Er worden drie soorten rollen toegekend: public, confidential en sensitive. De gebruiker krijgt via identity management een sessielabel, waarmee hij voor een of meerdere rollen kan inloggen.

Monitoren

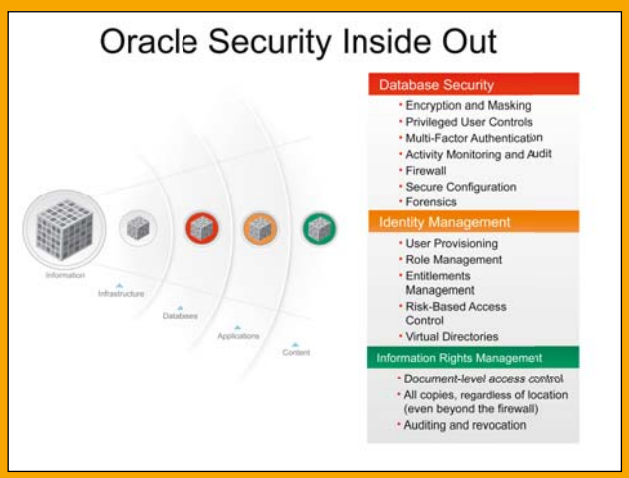
Slechts een kwart van de bedrijven gebruikt tools om de database activiteit te monitoren. De overige driekwart doet niet aan auditing of heeft hier geen controle op. Oracle heeft hiervoor de real time werkende 'Audit Vault'. Daarnaast kan met 'Total Recall' de wijziging van gevoelige data worden bijgehouden en gelogd. Eventuele onrechtmatigheden kunnen met deze tool ook snel worden teruggevonden.

Om het klonen van databases voor testdoeleinden te beveiligen heeft Oracle 'Data Masking'. Dit zorgt ervoor dat de data niet meer te identificeren zijn, terwijl zij in de testomgeving wel de juiste waarden teruggeven.

Om het gevaar van SQL injection (een techniek om de response van de database te achterhalen) tegen te gaan heeft Oracle de Database Firewall. Deze is niet zelf ontwikkeld, maar een erfenis uit de overname van het Britse Secerno in mei 2010. Tot het moment van overname was Secerno voorloper bij de ontwikkeling van actieve database controle. Bijzonder aan de systematiek is dat deze firewall werkt met op SQL gebaseerde analyse en niet – zoals de meeste firewalls – op patroonherkenning. Dit maakt onder meer dat deze firewall geen false-positives afgeeft. De firewall ondersteunt Oracle, Microsoft en Sybase. Binnenkort komen daar DB2 en MySQL bij. De firewall werkt nog niet samen met encryptie.



Met deze schillen om de database wordt die vrijwel onaantastbaar.



De maatregelen om de gehele informatiestroom te beveiligen.

Robert de Ruiter is hoofdredacteur van Optimize.