# De oracle database en system security

## *Beveiliging op niveau van besturingssysteem*

***De aandacht voor veiligheid van IT is de laatste jaren in een stroomversnelling gekomen. In 'Oracle land' is dit merkbaar door een toename aan controles op informatie-beveiliging zoals onder andere Sarbanes-Oxley (alias 'SOX'), HIPAA en ISO-27001. Voor de database, en daarmee databasebeheerders, is dit merkbaar door (nieuwe) Oracle producten die op deze ontwikkelingen inspelen.***

De opties en features gerelateerd aan security zijn meestal van toepassing op zaken in de database. Er is echter weinig aandacht voor security van de database op het niveau van het besturingssysteem. Kijken we naar security op operating systeemniveau, dan zien we dat de wijze waarop de database wordt geïnstalleerd meestal sterk is geïnspireerd op de installatiehandleiding van Oracle zelf. Deze handleiding beschrijft de Operating System User 'Oracle', en tenminste een tweetal groepen: 'oinstall' en 'dba'. Dit werkt uitstekend. Daarom wordt het in 90% van de gevallen toegepast. Er kleven echter een aantal bezwaren aan deze manier van installeren.
De standaardmethode om de database te beheren gaat uit van het 'oracle' account. Dit betekent dat alle beheerders hetzelfde account gebruiken. Met als gevolg dat het netwerkadres (IP-adres) van het systeem waar de beheerder op ingelogd is, de enige is op de databaseserver. Alleen met dat IP-adres is de beheerder te identificeren. Het mag duidelijk zijn dat een IP-adres geen ideale manier is om een persoon te identificeren. Denk daarnaast aan wat dit betekent met dynamische IP-adressen (DHCP) of gedeelde machines zoals beheerportals.

Het gebruik van het 'oracle' account betekent dat er onbeperkt toegang is tot alle Oracle-elementen op besturingssysteemniveau. Natuurlijk is er vertouwen in de beheerders, maar het is niet verstandig om ze allemaal toegang te verlenen terwijl dit meestal niet nodig is. Niet voor niets wordt op besturingssysteemniveau in Linux/Unix-systemen het gebruik van 'root' teruggedrongen of verboden en in deeltaken gedelegeerd naar persoonlijke beheeraccounts. Waarom dan niet hetzelfde met de database?

De database houdt altijd audit/log gegevens bij van stop, start en SYSDBA-toegang. Dit zijn typische taken die een beheerder met het 'oracle' account uitvoert. De betrouwbaarheid van deze logging is vanzelfsprekend laag als het account, dat geaudit wordt, deze gegevens kan wijzigen of verwijderen.
Door de toevoeging van een extra groep ('oracle') en het terugdringen van de defaulttoegang op de Oracle software en database, is het relatief eenvoudig een database-installatie en - gebruik auditable te maken. Oracle heeft de operating system databasesecurity geïmplementeerd door gebruik te maken van groepen.
Door een andere groep (niet 'oinstall' (voor toegang tot de inventory), en 'dba' (voor database SYSDBA toegang) als primaire groep van het 'oracle' account op te geven, , wordt dit de hoofdgroep van alle Oracle bestanden. Hiermee kan toegang tot de Oracle databasesoftware en andere files expliciet worden uitgedeeld.
De 'DBA'-groep (opgegeven tijdens installatie van de Oracle database software) is de groep die DBA-taken (stop, start en SYSDBA-toegang) mag uitvoeren. Een ander account dan 'oracle' kan aan de 'DBA'-groep toegevoegd worden. Indien dit account toegang tot de Oracle home en de executables heeft, kan dit account deze taken uitvoeren.
Naast het stoppen en starten van de database zijn er diverse andere taken die een databasebeheerder uitvoert. Om vanuit een ander (persoonlijk) account dan 'oracle' toch zaken onder oracle uit te voeren (denk aan manipuleren van de listener, het aanmaken van een database of het wijzigen van (netwerk) configuratiefiles) kan sudo gebruikt worden.

Beheertoegang tot een databaseserver met een gedeeld account/het 'oracle' account is begrijpelijk vanuit historisch perspectief en vanwege de documentatie van Oracle. Toch is dergelijk gebruik onacceptabel in het licht van informatie beveiligingsregelgevingen van moderne beheerstechnieken op besturingssysteemniveau.

**Frits Hoogland** is werkzaam bij VX Company.