

Administrator, der hinlänglich viele Systemprivilegien erhalten hat, dadurch implizit auch über Zugriffsberechtigungen für viele oder gar alle Tabellen (Objektprivilegien) verfügt. Nun besteht das Problem nicht darin, dass ein Administrator überhaupt auf Daten zugreifen kann, sondern dass die Zugriffsberechtigungen implizit, also oft ungewollt und unkontrolliert vergeben werden. Weiterhin sollte man sich daran erinnern, dass Datenverschlüsselung in einer solchen Situation wirkungslos ist. Wenn ein privilegierter Benutzer sich erfolgreich angemeldet hat, wird das Datenbank-System die verschlüsselten Daten entschlüsseln, weil es die Abfrage für legitim hält.

Die Lösung, die Oracle mit Database Vault anbietet, basiert demnach nicht auf Verschlüsselung, ist aber damit kombinierbar. Beim Einsatz von Database Vault wird eine neuartige Privilegienverwaltung implementiert, die strikt zwischen System- und Objektprivilegien trennt. Zudem ermöglicht sie den Aufbau sehr viel differenzierterer Zugriffsregeln als beim traditionellen Ansatz, der über einfache Objekt-Benutzer-Zuordnungen nicht hinauskommt. So ist es etwa möglich, Zugriffsrechte an bestimmte IP-Adressen, Uhrzeiten oder Applikationen zu binden oder die Zusammenarbeit mehrerer Personen (Vier-Augen-Prinzip) zu verlangen (siehe Abbildung 3).

Database Vault ist ein Werkzeugkasten, mit dem man sich Regelwerke, die zu den eigenen Applikationen und Anforderungen passen, bauen kann, aber auch selbst bauen muss. Das ist auch nicht anders möglich, wenn der Kunde eigene Applikationen entwickelt hat. Für Standard-Applikationen, die von vielen Kunden eingesetzt werden, liefert Oracle aber zusätzlich eine Default-Policy. Dies gilt auch für SAP-Applikationen. „Oracle Database Vault for SAP“ besteht aus einer Default-Policy, die typischerweise 70 bis 90 Prozent der Kundenanforderungen abdeckt, sowie dem Werkzeugkasten, um die vorgefertigte Policy bei Bedarf zu ändern oder zu erweitern. Ergänzt werden diese Komponenten durch eine umfangreiche Audit- und Reporting-Funktionalität, die der Überwachung des sicherheitsrelevanten Geschehens in der Datenbank dient.

Weitere Informationen

Ein ausführlicherer Überblick über Oracle-Datenbanksicherheit im SAP-Umfeld steht unter <http://www.oracle.com/us/products/database/n120-database-security-396167.pdf>. Technische Details zum Einsatz von Oracle Advanced Security sind in den SAP-Notes 973450, 974876 und 1324684, zum Einsatz von Oracle Database Vault in den SAP-Notes 1355140, 1597194 sowie 1502374 zu finden.

Christoph Kersten
Oracle Database for
SAP Global Technology Center
christoph.kersten@oracle.com

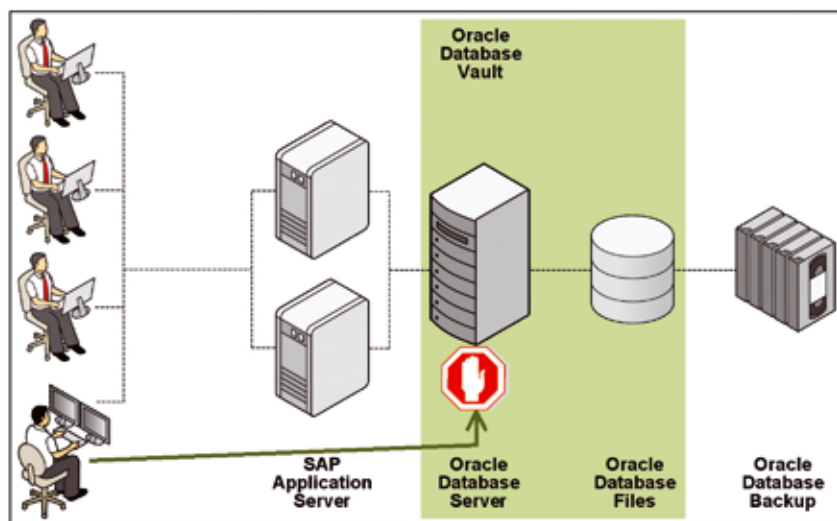


Abbildung 3: Schutz der Daten in der produktiven Datenbank durch Database Vault

Unsere Inserenten

Biotronik www.biotronik.de	Seite 41
DB Concepts www.dbconcepts.at	Seite 57
esentri consulting GmbH www.esentri.com	Seite 47
Herrmann & Lenz Services GmbH www.hl-services.de	Seite 63
Hunkler GmbH & Co. KG www.hunkler.de	Seite 3
KeepTool GmbH www.keeptool.com	Seite 15
Libelle AG www.libelle.com	Seite 33
MuniQsoft GmbH www.muniqsoft.de	Seite 19
OPITZ CONSULTING GmbH www.opitz-consulting.de	U 2
ORACLE Deutschland B.V. & Co. KG www.oracle.com	U 3
PITSS GmbH www.pitss.com	Seite 23
PROMATIS software GmbH www.promatis.de	Seite 9
Team GmbH www.team-pb.de	Seite 37
Trivadis GmbH www.trivadis.com	U 4