Eine zunehmende Zahl von Kunden, die SAP-Systeme auf der Basis von Oracle-Datenbanken betreiben, möchte ihre Daten besser vor unbefugten Zugriffen schützen. Aber welche der von Oracle angebotenen Sicherheitsoptionen sind von SAP unterstützt? Wann lohnt es sich, sie einzusetzen? Und gibt es spezielle Oracle-Angebote für SAP-Kunden? Der Artikel beantwortet diese Fragen für die Oracle Database 11*g* R2.

Oracle-Datenbanksicherheit in SAP-Umgebungen

Christoph Kersten, Oracle Database for SAP Global Technology Center

Wenn Datenbanken in SAP-Umgebungen auf Schwachstellen und Optimierungsmöglichkeiten hin untersucht wurden, ging es in der Vergangenheit meist um Performance und Verfügbarkeit. In neuerer Zeit sind mit der Effizienz der Datenspeicherung (Komprimierung, Partitionierung) und dem bestmöglichen Schutz der Daten vor unbefugtem Zugriff zwei weitere wichtige Aspekte hinzugekommen. Der Hintergrund ist in beiden Fällen gleich: Die Konsolidierung vieler dezentraler Systeme brachte nicht nur Datenbanken unbekannter Größe, sondern führte auch zu weitaus dramatischeren Folgen eines einzigen gelungenen Datendiebstahls. Durch neue organisatorische Lösungen wie Outsourcing oder Hosting waren die anfallenden Gesamtkosten sehr stark vom verbrauchten Plattenplatz bestimmt, und Personen, die gar nicht oder nur lose in das Unternehmen eingebunden sind, erhielten Zugang zu sensitiven Daten.

Oracle stellt mit „Advanced Security" und „Database Vault" optionale Zusatzfunktionalitäten zum Oracle-Datenbank-Server bereit, die das Risiko des Datendiebstahls erheblich minimieren. Beide Pakete können auch in SAP-Umgebungen eingesetzt werden. Nutzen und Unterschiede lassen sich am besten anhand verschiedener Zugriffsszenarien erläutern.

Szenario 1: Zugriff über SAP-Applikationen

In der Regel soll und wird der Zugriff auf die von SAP-Applikationen generierten und in Oracle-Datenbanken abgelegten Daten von SAP-Anwendern ausgehen und über SAP-Applikationen erfolgen. Ein solcher Normalzugriff ist aus Oracle-Sicht unproblematisch, weil die SAP-Funktionalität über eine eigene, von der Datenbank völlig unabhängige Benutzer- und Privilegienverwaltung verfügt. Aus diesem Sachverhalt ergeben sich drei wichtige Schlussfolgerungen für das Verhältnis von Applikations- und Datenbanksicherheit:

- In allen Fällen, in denen der Zugriff regulär über SAP-Applikationen stattfindet, ist die SAP-Funktionalität für den Schutz der Benutzerdaten verantwortlich. Der Oracle-Datenbank-Server mischt sich in die applikationsinternen Vorgänge nicht ein. Das heißt auch: Wenn das Verhalten der SAP-Applikation im Hinblick auf einzelne Sicherheitsaspekte nicht den Erwartungen entspricht, sollte man als Kunde nicht versuchen, dieses Verhalten mit Oracle-Mitteln zu korrigieren, sondern sich an SAP wenden.
- Auf der anderen Seite ist die SAP-Funktionalität völlig chancenlos, wenn es darum geht, potenziell illegale Datenzugriffe abzuwehren, die unter Umgehung der SAP-Applikationen erfolgen. In diesem Fall kann einzig und allein die Oracle-Funktionalität helfen.
- Die von SAP und von Oracle zur Verfügung gestellten Sicherheitsmechanismen konkurrieren nicht miteinander, sie ergänzen sich vielmehr. Deshalb sollte man sie gemeinsam – und selbstverständlich zusammen mit allgemeinen Maßnahmen wie der Kontrolle des Zugangs zum Firmennetzwerk oder zu Datensicherungen – implementieren, um den größtmöglichen Schutz der Daten zu erreichen.

Szenario 2: Zugriff auf Daten im Netzwerk

Eine Möglichkeit, anders als auf dem regulären Weg über die SAP-Applikationen Zugriff auf die Daten zu bekommen, besteht darin, das Netzwerk abzuhören. Bei diesem Verfahren können die Daten, die gerade im Netzwerk unterwegs sind (data in transit), entweder nur gelesen oder aber zusätzlich noch manipuliert werden. Um dies zu verhindern, bietet Oracle im Rahmen des Zusatzpakets „Advanced Security" die Funktionalität „Network Encryption" an. Diese verschlüsselt Daten vor dem Versenden über das Netzwerk und entschlüsselt sie auf der Empfängerseite wieder. Der Administrator kann zwischen verschiedenen Schlüssellängen und Verschlüsselungsverfahren wählen. Zusätzlich können Prüfsummen generiert werden, die es dem Empfänger erlauben, Datenmanipulationen zu entdecken (siehe Abbildung 1).

Dabei ist zu beachten, dass die Oracle Network Encryption nur den Datenaustausch zwischen SAP-Application-Server-Instanzen und Oracle-Datenbank-Server-Instanzen schützen kann. Die Verschlüsselung erfolgt durch Oracle-Software, die zwar auf al-

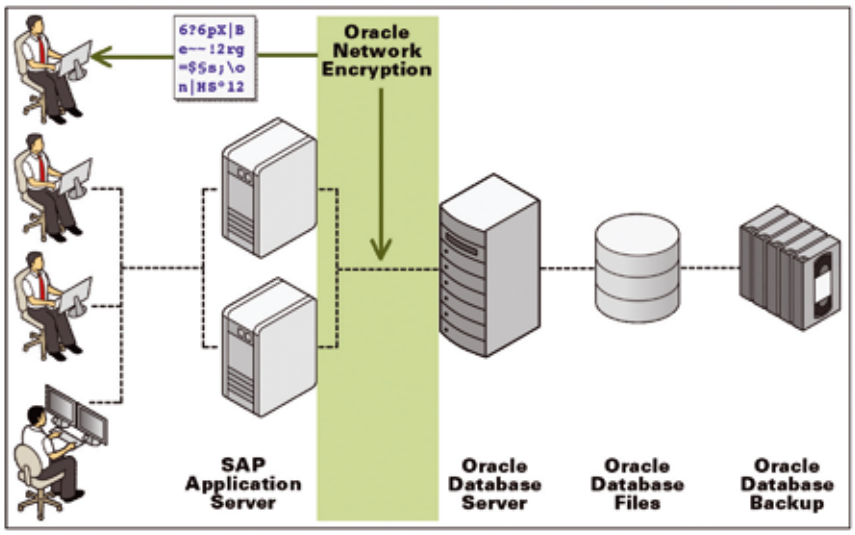

Abbildung 1: Schutz der Netzwerkkommunikation durch Network Encryption

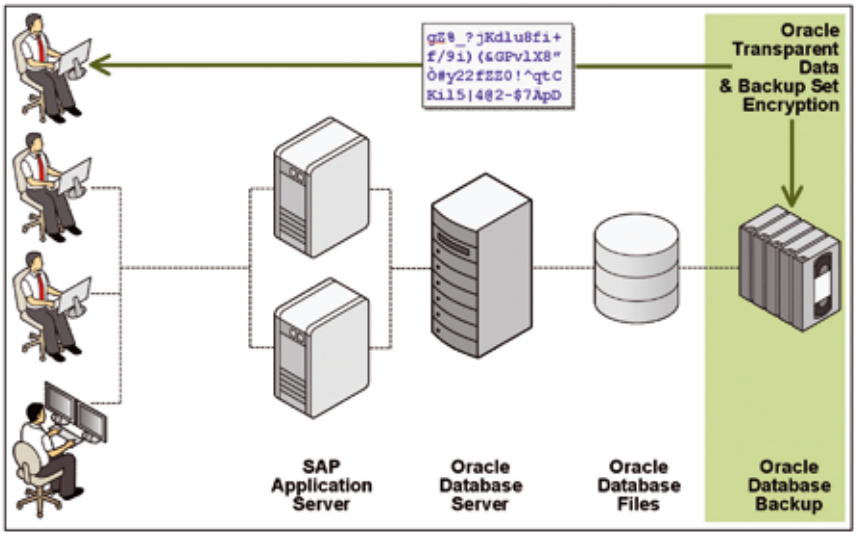

Abbildung 2: Schutz der Datenbankdateien durch Transparent Data Encryption und Backup Set Encryption

len Rechnern installiert ist, auf denen Oracle-Datenbank-Server oder SAP-Application-Server laufen, nicht aber auf den Endgeräten der SAP-Anwender. Die zwischen SAP-Anwendern und SAP-Application-Servern ausgetauschten Daten sind daher mit anderen Mitteln zu verschlüsseln.

Szenario 3: Zugriff auf Datenbank-Dateien

Eine zweite Möglichkeit des illegalen Datenzugriffs besteht darin, sich Kopien der Datenbank-Dateien (beispielsweise eine Datensicherung) zu besorgen und die Datei-Inhalte auszulesen. Diese Strategie erfordert zwar umfangreiches Wissen und ein hohes Maß an krimineller Energie, unmöglich ist sie aber nicht. Man kann allerdings auch hier die Hürden für potenzielle Angreifer erheblich erhöhen, indem man die in der Datenbank abgelegten Daten (data at rest) verschlüsselt. Ebenfalls im Rahmen des Zusatzpakets „Advanced Security" stellt Oracle zu diesem Zweck die Funktionalitäten „Transparent Data Encryption (TDE)" sowie „Backup Set Encryption" zur Verfügung (siehe Abbildung 2).

„Transparent Data Encryption" gibt es schon seit einigen Jahren, jedoch wies die Funktion bis einschließlich Database 10*g* einige Einschränkungen auf, die ihre Implementierung im SAP-Umfeld sehr erschwerten. Vor allem stellte der Ansatz, nur einige wenige Tabellenspalten zu verschlüsseln (column encryption), SAP-Anwender vor ein nahezu unlösbares Problem, da das SAP-Datenmodell nicht nur äußerst komplex, sondern zudem nicht offengelegt ist. Hier schafft Database 11*g* Abhilfe mit dem neuartigen Ansatz, ganze Tablespaces zu verschlüsseln (tablespace encryption). Mit dieser Datenbank-Version ist es also möglich, sich die komplizierte Suche nach zu verschlüsselnden Spalten zu sparen und einfach sämtliche Tablespaces zu verschlüsseln, die SAP-Nutzdaten enthalten. Kundenerfahrungen zeigen, dass dies selbst für Multi-Terabyte-Datenbanken eine realistische Strategie ist.

Zusätzlich zur Verschlüsselung der Daten in der produktiven Datenbank bietet „Backup Set Encryption" die Möglichkeit, mit dem Oracle Recovery Manager (RMAN) erstellte Datensicherungen komplett zu verschlüsseln. Dies ist insbesondere dann ein zusätzlicher Schutz, wenn man sich entschlossen hat, einen Teil der in der Produktiv-Datenbank abgelegten Daten unverschlüsselt zu lassen.

Szenario 4: Direktzugriff auf Daten in der Datenbank

Der dritte Schleichweg zu den von SAP-Applikationen generierten und in der Oracle-Datenbank abgelegten Daten führt über Standard-Datenbank-Werkzeuge wie SQL*Plus. Mithilfe einer direkten Verbindung zur Datenbank lassen sich sämtliche SAP-Schutzmechanismen aushebeln. Das stellt insbesondere dann eine potenzielle Gefahr dar, wenn privilegierte Benutzer (Datenbank-Administratoren) diesen Weg ausnutzen.

Um das Problem und die von Oracle angebotene Lösung zu verstehen, sollte man sich zunächst einmal an eine Unschärfe der Privilegienverwaltung in Datenbanksystemen erinnern. Beim herkömmlichen Verfahren wird zwar zwischen System- und Objektprivilegien unterschieden, die Umsetzung führt dann aber meist dazu, dass ein

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/nl20-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.

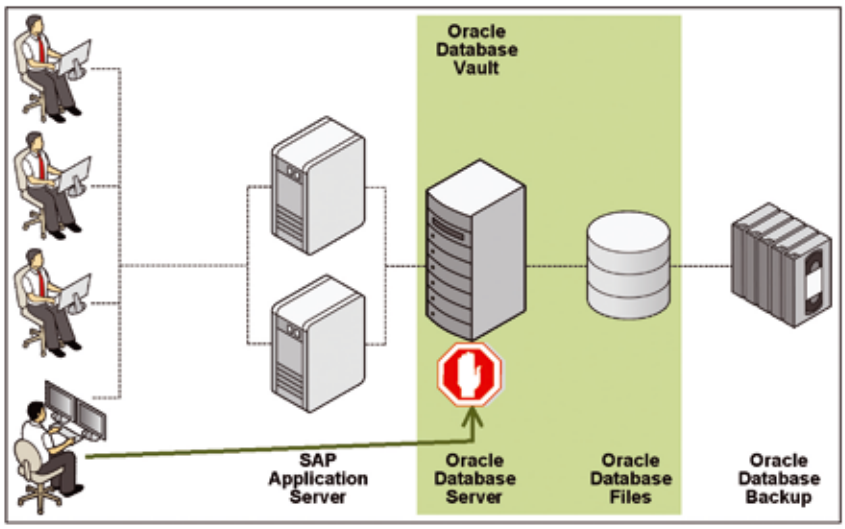

Abbildung 3: Schutz der Daten in der produktiven Datenbank durch Database Vault

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