Und dann kam der Datenschutz

Stephan La Rocca
PITSS GmbH
Bielefeld

Schlüsselworte
Oracle Datenbank, Security, Firewall, Advanced Security, Data Masking

Einleitung
Geänderte Gesetzgebungen, eine deutlich gesteigerte öffentliche Wahrnehmung oder einfach die Tatsache, das der Kunde tatsächlich Opfer von Datendiebstahl geworden ist, führen mehr und mehr dazu, dass das Thema Datenschutz an Bedeutung in der IT-Abteilung gewinnt.
Gerade ältere, vom Datenmodell und den Software-Komponenten gesetzte Applikationen, stehen dann vor der Bewertung, wie hier nachträglich Anforderungen des Datenschutz umgesetzt werden können. Natürlich ohne komplettes Redesign.

Das große Ganze
Die Produktpalette von Oracle ist umfangreich, wenn es um das Thema Security geht. Was zum einen erfreulich für die Wahrnehmung des brisanten Themas ist, erschwert auf der anderen Seite die Auswahl des richtigen Produkts. Für eine erste Gliederung können wir zwischen Sicherheitsmechanismen innerhalb und außerhalb der Datentank unterscheiden. Außerhalb der Datenbank sind vor allem zwei Angriffspunkte relevant: Zum einen der unbefugte Versuch eines Zugriffs und die Angriffspunkte Festplatte und Netzwerk. Dafür positioniert Oracle das Produkt Database Firewall/Audit Fault und Verfahren wie z.B. Secure Backup/Export sowie Network Encryption.
Ist der eigentliche Zugriff zur Datenbank erlaubt, aber nur bestimmte Dateninhalte zu schützen, ist die erste Wahl Advanced Security. Abgedeckt sind weitreichende Methoden zum Verschlüsseln und Freigeben von Daten. Damit aber der DBA nicht an den Security-Einstellungen vorbeikommt, ist Database Vault das passende Tool.

Sollen die Daten nicht nur verschlüsselt, sondern komplett für die Applikation ausgeblendet werden, sind die Produkte Label Security und das darauf basierende Konzept der Virtual Private Database gedacht.

Häufig vergessen wird in dem ganzen Kontext die eigene IT-Abteilung, die zwar nicht zwingend DBA-Rechte hat, aber zumindest eine Testdatenbank für die Applikationsentwicklung benötigt. In diesen Fällen ist Data Masking der passende Ansatz.

Firewall
Der erste Schritt um die sensible Datenbank für unberechtigten Zugriff zu schützen ist das Oracle Produkt „Audit Vault and Database Firewall“.

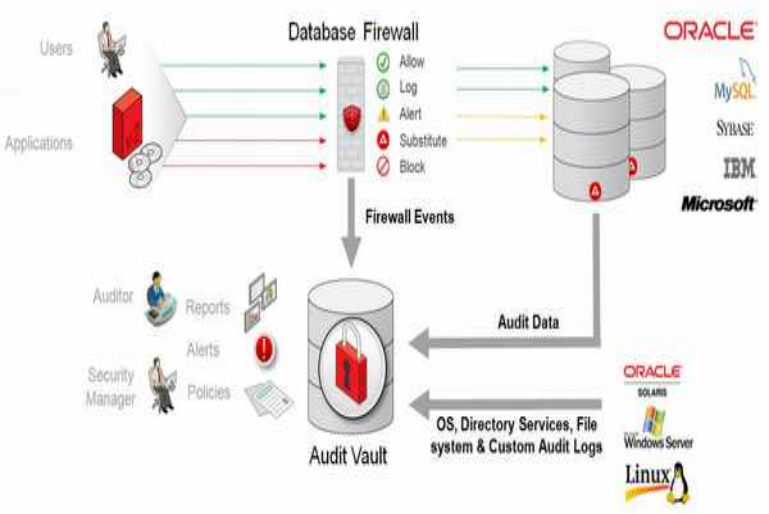

Abb. 1: Oracle Audit Vault und Database Firewall

Wie bei einer herkömmlichen Firewall protokolliert dieses Produkt jeglichen Traffic von Anwendungen und Prozessen mit der Datenbank. Dabei sind Sie nicht ausschließlich auf eine Oracle Datenbank im Backend angewiesen. Andere Datenbanken und selbst die Betriebssysteme können ebenfalls die Audit-Daten in den gemeinsamen „Tresor“ schreiben um darauf Recherchen nach unzulässigen Zugriff zu ermöglichen.
Die Firewall ist in der Lage, SQL Statements zu parsen und z.B. SQL-Injektions zu verhindern. Dazu werden Black-lists, Whitelists und Exception lists in der gleichen Art und Weise wie bei einer HTTP-Firewall genutzt. Die UI-Komponente ermöglicht daraus eine Vielzahl von Reports und Auswertungen.

Eine kleine Variante dieser Firewall, wenn wir Sie nur in der passiven Variante betrachten. d.h. es wird nur protokolliert und nichts verhindert, ist das Verfahren des Fine Grained auditing.
Hier legen Sie Audit Regeln fest, die dafür sorgen, dass alle Tabellenzugriffe mit Datum, User und Statement in eigene Audittabellen gespeichert werden. So können Angriffe und der Versuch Daten abzugreifen festgestellt werden.

Noch auf systemtechnischer Ebene und außerhalb der Datenbank befinden sich Sicherheitsmechanismen, die den Versuch die Netzwerkpakete zu analysieren, verhindern sollen. Mit Network Encryption können Sie verhindern, dass SQL-Statements und die Ergebnisse dazu im Klartext mit dem SQLNet-Protokoll über das Netz geschickt werden.

Im Filesystem, so werden wir gleich erkennen, gibt es innerhalb der Advanced Security die Möglichkeit, gesamte TableSpaces zu verschlüsseln und auch im Bereich Backup und Dataexport für ein automatisches Verschlüsseln der Daten zu sorgen.

Innerhalb der Datenbank
Eine umfassende Möglichkeit, Daten zu verschlüsseln, bietet Oracle mit dem Produkt „Advanced Security“ an.

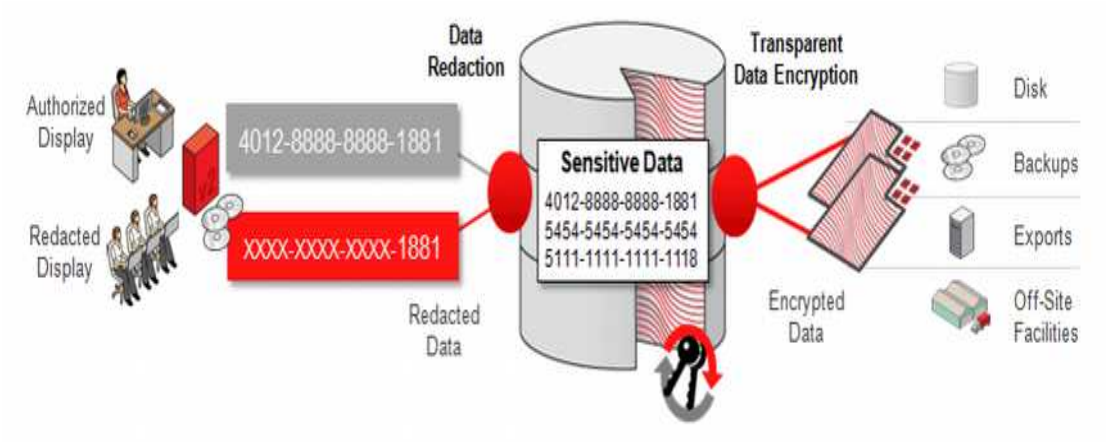

Abb. 2: Prinzip von Advanced Security

Sensitive Daten werden innerhalb der Datenbank verschlüsselt und für die Ausgabe kann entschieden werden, welche User die Daten komplett erkennen können und welche User nur „maskierte Daten“ zu sehen bekommen. Bei der Auswahl der Daten können Sie einzelne Spalten einer Tabelle oder auf der anderen Seite auch ganze Tablespaces verschlüsseln. Das notwendige Key-Management (incl. Wallet, Rotation, Master-Key-Management und Built-In Funktionalitäten wird ausschließlich in der Datenbank durchgeführt und kann über den Enterprise Manager eingestellt werden.
Der Vorteil für die Anwendungen liegt auf der Hand, denn es sind keine Änderungen an bestehenden Applikationen durchzuführen.
Für eine sinnvolle Darstellung der Daten für unberechtigte User kann aus einer Reihe von Redaction-Featuren ausgewählt werden.

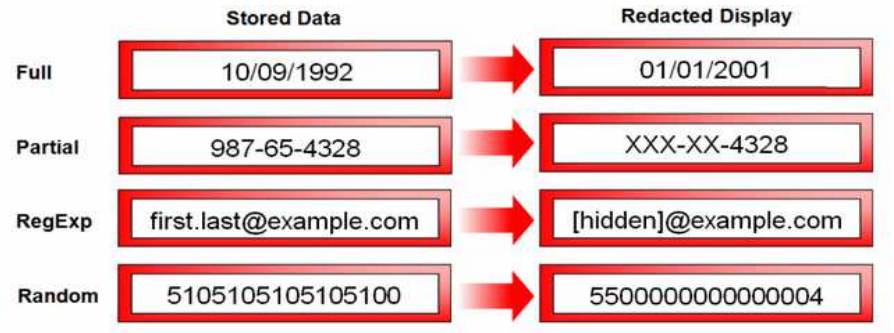

Abb. 3: Data-Masking

Die Verschlüsselung zieht sich über die primären Speicher hinaus auch auf Backups und Exports.

Sollen sensitive Daten auf der Datenbankseite nicht verschlüsselt werden, aber im UI für unberechtigte User nur maskiert werden, kann getrennt nur das Data-Masking eingesetzt werden. Dieses Verfahren

ist auch hilfreich, wenn Daten für eine Testdatenbank aufgesetzt werden soll, oder für Testzwecke das eigene Haus verlassen.

Soll nicht die lizenzpflichtige Option von Oracle zum Einsatz kommen, kann natürlich auch mit der Datenbank Package DBMS_CRYPTO gearbeitet werden. Je nach dem, wie umfangreich sie es implementieren möchten, können beliebig viele Spalten so verschlüsselt werden. Der eigentliche Aufwand steckt aber in der Schlüsselverwaltung, da sie den Schlüssel sicherlich nicht im Sourcecode verdrahten werden. So beginnen Sie eigene Rotationen und Stores dafür zu konzipieren.
Ganz zu schweigen, dass Ihnen die Optionen fehlen, über Datamasking die Daten „hübsch“ für die Ausgabe vorzubereiten.

Datenschutz auf Satzebene
Ist die Aufgabe, nicht einzelne Attribute einer Spalte dem nichtautorisierten Anwender zu verbergen, sondern ganze Datensätze an Hand der Berechtigung nicht sichtbar zu machen, ist der Einsatz von „Virtual Private Database“ VPD geeignet.
VPD kann vereinfacht dargestellt, als Möglichkeit verstanden werden, zu jedem Select (egal über welches Tool sie auf die Daten zugreifen) eine Where-Bedingung anzufügen. Dabei wird diese Where Bedingung über PL/SQL erstellt und kann den User Kontext oder den Global Kontext der Datenbank nutzen.
Basierend auf der VPD-Technologie hat Oracle die „fertige Lösung“ „Label Security“ implementiert, bei der Daten mit sogenannten Labels versehen werden und nur User, die über die entsprechenden Labels (Policies) verfügen, können die Datensätze hinter den Labels sehen.
Für beide Verfahren gilt, dass auch hier die Sicherheitsmechanismen transparent für die Applikation sind. Beachten Sie allerdings nur, dass Sie einen genauen Blick auf Ihre Indizes werfen.

Bleibt noch der DBA
In vielen Fällen wird bei solchen Konzepten der DBA mit seinen umfassenden Rechten gerne außen vor gelassen mit der Worten „einem müssen wir ja trauen“.
Um diesen Freifahrtschein nicht ungesehen unterschreiben zu müssen, eignet sich das Produkt „Oracle Database Vault“. Damit können Sie Sicherheitsmechanismen einführen, die auch durch DBA-Rechte oder ein klassisches „grant select any table“ nicht ausheben lassen.
Neben den Zugriffen auf sensitive Daten können Sie auch einschränken, wer sich wann von welchem Rechner wie mit der Datenbank verbinden darf.
Auch hinter Oracle Database Vault befindet sich ein umfangreiches Audit-Verfahren, welches umfangreich analysiert werden kann, um so auch Beweispflichten nachzukommen.

Und was kostet das Ganze
Aus dem Vortrag sollte deutlich werden, dass Oracle mit 5 verschiedenen Produkten an das Thema Sicherheit in und um die Datenbank herantritt. Die Preise verstehen sich als Listenpreise mit einer Gültigkeit zum Zeitpunkt des Schreibens des Abstracts. Diese Preise können dann in der Präsentation auf Grund einer aktuellen Preisliste abweichen:
Audit Vault und Database Firewall: 4.736€ pro CPU (nur Prozessorlizenz möglich)
Advanced Security: 237€/NUP
Database Vault: 182€/NUP
Label Security: 182€/NUP
Data Masking: 182€/NUP

Alle Produkte mit Ausnahme der Firewall sind in der gleichen Metrik zu lizenzieren, wie auch die zu schützende Datenbank lizenziert ist.

Botschaft
Sicherheit ist nicht teuer – keine Sicherheit kann schnell sehr teuer werden.

Kontaktadresse:
Stephan La Rocca
PITSS GmbH
Otto-Brenner-Str. 209
D-33604 Bielefeld

Telefon: +49 (0) 521-54679500
E-Mail slarocca@pitss.de
Internet: www.pitss.de