Schon einfache Maßnahmen wie entsprechende Konfigurationseinstellungen können Sicherheitslücken weitestgehend verhindern. Richtig konfiguriert und gehandhabt stellt die Datenbank ein überschaubares Risiko dar.

Sicherheitsrisiko Oracle-Datenbank?

Christian Wischki und Kyle Krüsi

Sensible Datenbanken liegen meist in den innersten Kreisen der Firmen-Netzwerke und sind somit in der Regel allein schon durch mehrere demilitarisierte Zonen gegen Sicherheitsrisiken von außen abgesichert. Die in der Praxis aber überwiegenden Versuche von unbefugten Personen, an die in der Datenbank enthaltenen Daten zu gelangen, erfolgen jedoch nicht von außen, sondern von innen – auch durch die Mitarbeiter des eigenen Unternehmens.

Wie viel Sicherheit braucht ein Unternehmen?

Das Security-Management für Oracle-Datenbanken kann im Grunde abstrakt betrachtet und wie folgt definiert werden: die Gewährleistung der Daten im vorgegebenen Umfang, bezogen auf die Vertraulichkeit (Schutz vor unautorisiertem Zugriff auf die Datenbank), Integrität (Vollständigkeit und Korrektheit der Daten), inhaltliche Verfügbarkeit (berechtigte Personen und Systeme können im jeweils definierten Umfang bei Bedarf auf die Datenbank zugreifen) sowie die Rückverfolgbarkeit und Nachvollziehbarkeit (Protokollierung der Aktivitäten innerhalb der Datenbank).

So einfach das auf den ersten Blick erscheint, in der Praxis kann das Security-Management für Oracle-Datenbanken durchaus sehr schnell zu einer sehr komplexen und aufwändigen Angelegenheit werden – vor allem wenn es gleich zu Beginn alle mögli-

chen oder bekannten Richtlinien wie beispielsweise diverse Compliance-Vorgaben zu realisieren gilt. Deshalb sollte am Anfang eines jeden Security-Managements immer die Identifikation der Risiken stehen – im Grunde die Beantwortung der Frage: „Was bedeutet es für mein Unternehmen, wenn die Sicherheit einer Datenbank vernachlässigt wird?“ Jedes Unternehmen muss für sich selbst klären, welche Schäden es in Kauf nehmen will und welche nicht.

Aus Sicht der Datenbank sollten Unternehmen für die Erfassung möglicher Schäden folgende Fragen zwingend beantworten:

- Was geschieht, wenn die Datenbank nicht mehr verfügbar ist?
- Wie lange kommen wir ohne die darin befindlichen Daten und Funktionalitäten aus?
- Was kann geschehen, wenn Unbefugte an diese Daten gelangen?

In engem Zusammenhang mit dem Security-Management steht der Begriff „Compliance“. Darunter versteht man die Erfüllung von und die Übereinstimmung mit rechtlichen, regulativen und normativen Vorgaben – was aber nicht bedeutet, dass man „frei von Risiken“ oder gar „sicher“ ist. Compliance-Anforderungen definieren in der Regel lediglich einen Grundschutz oder ein erforderliches Minimum an Maßnahmen. Compliance-Vorgaben lassen sich wie folgt unterteilen:

- *Rechtliche Vorgaben*
  Unternehmen, Organisationen und Personen sind verpflichtet, die jeweils geltenden Gesetze und behördlichen Verordnungen einzuhalten, wie beispielsweise Sarbanes-Oxley Act (SOX), Eurosox, Datenschutzgesetz, Obligationenrecht etc.
- *Regulative Vorgaben*
  Anforderungen, die sich unter anderem aus dem „Code of Best Practice“ von Branchen oder sonstigen Fertigungsrichtlinien ergeben, wie beispielsweise GMP (Good Manufacturing Practice), Basel II & III, PCI (Payment Card Industry Data Security Standard) etc.
- *Normative Vorgaben*
  Anforderungen der nationalen und internationalen Normen wie Zertifizierung nach ISO 20000, Zertifizierung nach ISO 27001, Zertifizierung nach ISO 9001 etc.

Die hier genannten Vorgaben müssen immer nach den aufgeführten Gesetzestexten, ISO-Normen und eigenen Anforderungen (Richtlinien) für das eigene Unternehmen umgesetzt sein, um diese auch für das jeweilige Unternehmen messbar und transparent prüfen zu können.

Umsetzung der Informationssicherheits-Gesetze und -Richtlinien

Datenbanken besitzen die Besonderheit, dass sie in ihrem Lebenszyklus ständigen Einflüssen wie Upgrades, Application Changes, Tuning-Maßnahmen oder Veränderungen von Parametern unterliegen. So können sich beispielsweise durch einen applikationsbedingten Remote Function Call (RFC) die Sicherheitsparameter der Datenbank verändern, indem etwa neue Rollen oder Privilegien vergeben werden. Für eine kontinuierliche Einhaltung der Sicherheitsrichtlinien müssen beispielsweise folgende grundsätzliche Punkte zwingend umgesetzt sein:

- Installation der Oracle-Software und Aufsetzen der Datenbanken nach den Sicherheits-Standards, die das Security-Management vorgibt und die sich in der Configuration Policy wiederfinden
- Regelmäßige Überprüfung auf Einhaltung der Sicherheits-Richtlinien – insbesondere nach Upgrades
- Implementierung von Changes ausschließlich über RFCs und auch nur nach den im Change Management definierten Prozessen, in welchen auch ein Post Implementation Review (PIR) in Bezug auf die Einhaltung der entsprechenden Sicherheitsrichtlinien erfolgt
- Durchführung von regelmäßigen Datenbank-Audits
- Informationen von Sicherheitsverletzungen an Application Owner und Data Owner
- Zeitnahes Einspielen von aktuellen Sicherheits-Patches von Oracle

Integrität der Daten

Datenintegrität bedeutet im Grunde, dass die Daten in der Datenbank über einen bestimmten Zeitraum vollständig und unverändert bleiben. Es geht also um den Schutz vor Verlust und Fälschung der Daten. Oracle bietet folgende Optionen an, um dieses Ziel zu unterstützen:

- Bei jedem Schreiben vom Memory-Bereich auf Disk erfolgt eine Kontrolle der Datenbank-Blöcke. Damit kann man die Änderung von außen zwar nicht verhindern, jedoch zumindest erkennen. Mit einem Recovery dieses Datenblocks lässt sich diese Attacke rückgängig machen.
- In Bezug auf das zugrundeliegende Daten-Netzwerk kann Oracle über die Advanced-Security-Option (ASO) eine Integritätsprüfung durchführen. Diese erkennt Daten-Modifikation sowie das Löschen und Hinzufügen von Datenpaketen (zum Beispiel Replay Attacks). Der Schutz jedes Datenpakets ist durch eine Vergabe von Sequenz-Nummern, sicheren Prüfsummen (Hashwerte) sowie die Berechnung der Sequenz-Nummern und Prüfsummen mittels eines Master-Session-Keys gewährleistet.

Vertraulichkeit der Daten

Die Vertraulichkeit der Daten innerhalb einer Oracle-Datenbank realisiert man in der Praxis mit der Authentisierung, Autorisierung, Verschlüsselung und bei Bedarf auch durch die Rückverfolgbarkeit und das Auditing der Daten.

Die Authentisierung innerhalb der Oracle-Datenbank-Systeme ist sehr wichtig, da nur der Benutzername die Privilegien der Benutzer bestimmt. Derzeit unterstützt Oracle Authentifizierungsmethoden wie die Datenbank-Authentifizierung, die Betriebssystem-Authentifizierung (davon wird aus Sicherheitsgründen abgeraten), das Single Sign-on (etwa per OID und Ker-

beros), das Advanced Security (ASO) und die Secure Sockets Layer (SSL) sowie eine Proxy-Authentifizierung. Hierbei gilt es jedoch zu beachten, dass zunächst keine Passwort-Richtlinien aktiv sind. Dies bedeutet, dass ein Benutzer beispielsweise niemals verpflichtet ist, sein Passwort zu ändern. Außerdem sind keine Komplexitätsregeln festgelegt, sodass der Nutzer ein beliebig einfaches Passwort (beliebiger Länge, beliebigen Schwierigkeitsgrads) verwenden kann. Er kann auch beliebig oft versuchen, sich mit einem falschen Passwort anzumelden, ohne dass der Account jemals gesperrt wird. Diese Sicherheitslücken lassen sich jedoch mittels sogenannter „Password-Profiles" unterbinden. Dabei sollten mindestens folgende Kriterien erfüllt sein:

- Das Passwort soll den vom Kunden bestimmten Komplexitätsregeln entsprechen
- Im Passwort müssen numerische und/oder Sonderzeichen vorkommen
- Das Passwort muss automatisch nach einem bestimmten Zeitintervall seitens des Benutzers geändert werden
- Das Passwort darf erst nach einer bestimmten Zeit wieder verwendet werden
- Bei einer definierten Anzahl falscher Anmeldungen wird das Benutzerkonto automatisch seitens des Systems gesperrt

Mit der Autorisierung erhalten die Benutzer und Benutzergruppen ihre jeweiligen Privilegien. Seitens Oracle können Berechtigungen auf verschiedenen Ebenen vergeben werden wie Systemprivilegien (zum Beispiel „create session"), Objektprivilegien (zum Beispiel „select", „insert" oder „update" auf Tabellen und dediziert auf das Ausführen von PL/SQL-Code), Berechtigungen auf Spaltenebene, Berechtigungen auf Zeilenebene und Berechtigungen für Netzwerk-Callouts (ab 11*g*). In der Praxis werden Privilegien meist mittels eines Rollenkonzepts geregelt und vergeben. Dieses sollte jedoch immer zweiteilig geplant werden, um so zwischen Applikationen und Datenbank-Usern unterscheiden zu können. Somit lassen sich sowohl die Bedürfnisse der Applikation als auch die der Datenbankbenutzer (Entwickler, DBA, Super-User etc.) einfach und skalierbar verwalten. Darüber hinaus gibt es auch die Möglichkeit, mit Views, Stored Procedures und Triggern die Kontrolle des Datenzugriffs auf der Datenebene durchzuführen. Damit übernimmt die Applikation die Funktion der Rechteverwaltung. Außerdem gibt es in diesem Zusammenhang noch die folgenden Optionen:

- *Virtual Private Database*
  Mit einer Virtual Private Database (VPD) ist eine individuelle und flexible Zugriffskontrolle auf die Datenbank möglich. Die Zugriffskontrolle ist wesentlich feinmaschiger als beim traditionellen Konzept und kann auf Zeilen- und Spalten-Niveau ausgedehnt werden.
- *Oracle Label Security*
  Oracle Label Security (OLS) ist eine feinmaschige Zugriffskontrolle, die Oracle für die US-Regierung entwickelt hat. Diese ist frei verfügbar, verursacht jedoch extra Lizenzkosten.
- *Database Vault*
  Database Vault wurde speziell entwickelt, um das Bedrohungsrisiko „von innen" einzuschränken, indem die Trennung von Funktionen und Aufgaben möglich ist. So kann man beispielsweise verhindern, dass der DBA die Anwendungsdaten sieht. Diese Lösung bietet flexible, transparente und sehr anpassungsfähige Sicherheitskontrollen vor allem für Client/Server- oder Web-Anwendungen, da hierbei der Applikations- beziehungsweise Anwendungscode nicht verändert werden muss.

Standardmäßig erfolgt die Authentifizierung mithilfe verschlüsselter Übertragung über das Netzwerk. Datafiles sowie Backups werden jedoch unverschlüsselt übertragen und gespeichert. Für kritische Datenbanken wird die Verschlüsselung in den Datenfiles, Backups und Exports empfohlen, da im Falle eines Diebstahls dieser oder mittels direkten Zugriffs auf diese ein zusätzlicher Schutz besteht. Das lässt sich beispielsweise mit der Transparent Data Encryption, RMAN Backup Encryption und einer Netzwerk-Verschlüsselung erreichen.

Es ist in der Praxis jedoch sicherlich nicht immer notwendig, alle Daten oder gar die ganze Datenbank zu verschlüsseln – oft reichen hierfür einige Bereiche. Da sich die Verschlüsselung der Daten vor allem negativ auf die Performance einer Datenbank auswirkt, sollte man sich immer vorab Gedanken darüber machen, welche Bereiche zwingend schützenswert sind und welche nicht.

Verfügbarkeit, Rückverfolgbarkeit und Auditing

Bei der Verfügbarkeit der Daten geht es um die Bereitstellung und den Zugriff auf die Daten. Um dies zu gewährleisten, sollte das Security-Management stets mit dem Availability- und Continuity-Management eng zusammenarbeiten. In diesem Kontext muss man auch das Thema der Autorisierung berücksichtigen, weil Datenverfügbarkeit und Datenzugang nicht dasselbe sind.
Die Rückverfolgbarkeit bedeutet im Falle von Oracle-Datenbank-Services nichts anderes als die Protokollierung der Aktivitäten innerhalb der Datenbank, wie beispielsweise „Wer macht wann ein „select", „insert", „create index" oder „alter table" auf einem Datenbank-Objekt?" oder „Wer hat wann welchen Datensatz modifiziert, was war der alte Wert des entsprechenden Attributs und was ist der neue Wert des Attributs?" Dieses lässt sich in der Praxis durch verschiedene Oracle-Datenbank-Auditing-Optionen realisieren:

- *Oracle Standard Auditing*
  Mit dem Standard Auditing von Oracle ist es beispielsweise möglich, sowohl einzelne SQL-Anweisungen oder auch bestimmte Systemprivilegien wie den Zugriff auf einzelne Objekte zu überwachen, als auch alle oder nur bestimmte Benutzer. Hier ist im Grunde ein Audit auf jeder Ebene und auch mit allen denk-

baren Kombinationen möglich, doch es gilt Folgendes zu beachten: Ein Standard-Audit sollte nur selektiv, sowohl im SYSAUX-Tablespace als auch im Filesystem, verwendet und innerhalb einer Datenbank zwingend periodisch ausgewertet werden. Die gesammelten Daten sollten – sofern nicht mehr benötigt – wieder gelöscht werden.
Folgende Protokollierungen sind für ein initiales Oracle-Standard-Auditing empfohlen:

- „create"-, „drop"- und „alter"-Operationen bei den Objekten „table", „index", „procedure", „trigger", directory", „public synonym" und „profile"
- Die Benutzung der Privilegien „force transition" und „force any transition"
- Sowohl die erfolgreichen als auch die nicht erfolgreichen „create session" (check unsuccessful attempts), „role", „profile", „grant any privilege", „grant any object privilege", „grant any role" und „exempt acess public"

- *Trigger based Auditing*
  Mit Event-Triggern kann man Informationen beispielsweise auch über „connects" oder „disconnects" einer Session gewinnen. Mit DML-Triggern lassen sich außerdem beispielsweise die Fragen „Wer hat wann welchen Datensatz modifiziert?" oder „Was war der alte Wert des Attributs und was ist der neue Wert?" beantworten.
- *Fine Grained Auditing*
  Fine Grained Auditing ermöglicht eine engmaschige Kontrolle auf Zeilen- und Spaltenebene. So kann der Zugriff auf die eigenen Personaldaten, um beispielsweise die Anschrift oder die Telefonnummer zu ändern, durchaus angebracht sein, das Ändern des Gehalts durch den Benutzer selbst dagegen weder erlaubt noch erwünscht. Es ist hier auch möglich, bei jedem Event, der die Bedingung erfüllt, eine Nachricht an den Security-Beauftragten zu senden. Zu beachten ist, dass sowohl Audit-Einträge erzeugt werden, wenn ein „rollback" durchgeführt wird (und auch die E-Mail verschickt, wenn dies in einer benutzerdefinierten Prozedur programmiert ist), als auch wenn ein „select"-Statement sicherheitsrelevante Daten lesen könnte, dies aber nicht tut, da nicht alle Records gelesen werden.
- *Auditing von DBAs*
  Mit den bisher erwähnten Auditing-Methoden konnten bis zur Version 9*i* R1 nur die normalen Benutzer, nicht aber die Operationen der Benutzer „sysdba/sysoper" überwacht beziehungsweise protokolliert werden.
- *Oracle Audit Vault*
  Audit Vault ist ein eigenständiges Produkt von Oracle, welches das Einsammeln und Analysieren der Audit-Daten mehrerer Datenbanken unterstützt, automatisiert sowie ein entsprechendes Reporting ermöglicht.
- *Auditing mit dem Oracle Enterprise Manager*
  Die Einrichtung und Verwaltung von Audit-Einstellungen kann mit dem Oracle Enterprise Manager erfolgen. Dieser zeigt beispielswiese auf der Startseite der Datenbank die Anzahl der Sicherheitsverletzungen an. Die im Oracle Enterprise Manager definierten Sicherheitsrichtlinien können aber auch über entsprechende Regeln verändert, gelöscht oder mit neuen Regeln erweitert werden. Oracle liefert hierzu auch eine Standard-Bibliothek mit vordefinierten Regeln aus.

Security-Checkliste für Oracle-Datenbank-Services

Zu diesem Thema gibt es bereits eine Vielzahl entsprechender Veröffentlichungen. In der Praxis – vor allem für Oracle-Datenbank-Services, die in kleinen oder mittelständischen Unternehmen zum Einsatz kommen – werden diese jedoch oft aufgrund ihres Umfangs nicht umgesetzt. Eine für die gelebte IT-Praxis kurze und probate Security-Checkliste, die vor allem auch von kleineren Unternehmen und Oracle-Datenbank-Services umgesetzt werden kann, sollte im Basis-Set folgende Aspekte berücksichtigen:

- *Architektur*
  Von wo aus (Internet, Intranet, DMZ) kann auf die Datenbank zugegriffen werden? Welche Ports sind offen und welche Protokolle können auf das System und die Datenbank zugreifen? Soll sich der Datenbank-Zugriff auf bestimmte Rechner beschränken? Ist die Kommunikation mit der Datenbank sicher – wird ASO und/oder SSL verwendet? Wird der „SQL*Net"-Listener geschützt? Ist nur das unbedingt Notwendige installiert? Welche Security Patches wurden eingespielt?
- *Physikalische Sicherheit*
  Wann und wie werden Datenbanksicherungen durchgeführt? Wo werden die Sicherungen verwaltet und abgelegt? Werden die Sicherungen verschlüsselt? Werden die Datenbankdateien verschlüsselt? Wie werden die Verschlüsselungs-Keys verwaltet?
- *Benutzer-Management*
  Welche Benutzer haben Zugriff auf welche Applikation? Sind die Standardbenutzer gesperrt? Setzt man Benutzer/Passwörter in Datenbank-Links ein? Werden „public" -Datenbank-Links eingesetzt? Wie verwaltet man die Benutzer?
- *Passwort-Management*
  Welche Anforderungen werden an Passwörter gestellt? Werden Default-

Newsticker

Oracle optimiert MySQL-Installer und die Hochverfügbarkeit für Windows
Der neue MySQL-Installer für Windows vereinfacht den Installationsprozess auf Windows-Plattformen und reduziert dadurch den Zeitaufwand erheblich. Um Windows-Anwender auch weiterhin zu unterstützen, hat Oracle die Zertifizierung von MySQL Enterprise Edition for Windows Server 2008 R2 Failover Clustering abgeschlossen. Auf diese Weise können auch unter Windows geschäftskritische Anwendungen eingesetzt werden, die hohe Ansprüche an die Verfügbarkeit stellen.

Passwörter verwendet? Wurden die Passwörter für Standardbenutzer geändert? Wie verwaltet man Passwörter? Wie werden die Passwörter gespeichert?

- *Privilegien und Rollen*
  Welche Privilegien werden von welchen Benutzern verwendet? Wer hat „any"-Privilegien? Werden public"-Privilegien eingesetzt? Welche Privilegien sind welchen Rollen zugeordnet?
- *Überwachung*
  Welche Benutzer und Objekte werden überwacht? Welche Audit-Daten werden gesammelt? Welche Aktionen werden aufgrund des Audits ausgelöst? Wie werden die Audit-Daten verwaltet?

Fazit

Datenbank-Sicherheit ist für jedes Unternehmen relevant, aber in welcher Dimension und mit welcher Intensität, muss jedes Unternehmen stets individuell festlegen. In diesem Zusammenhang ist stets zu beachten, dass dieses Thema laufend zusätzliche Aufwände (Budget und Zeit, da das Security-Management ein fortlaufender Prozess aufgrund der sich stetig ändernden Bedrohungen ist) nach sich zieht – sowohl in Bezug auf den organisatorischen Zusatzaufwand, als auch in Form von Performance-Einbußen und Lizenzkosten der Datenbank, die durch das Setzen diverser Konfigurationseinstellungen für Datenbanksicherheit bei den Datenbanken verursacht werden. Allein schon aus diesen Gründen sollte man bei diesem Thema keinesfalls nur die hierfür anfallenden Projektkosten betrachten, sondern vor allem auch immer die anschließend entstehenden, wiederkehrenden Betriebskosten.

Weiterführende Literatur

- *Cecchetti*, Configuration Benchmark for Oracle Database Server 11*g*
- *Haas*, Oracle Security in der Praxis
- *Wischki und Fröhlich*, ITIL & ISO20000 für Oracle Datenbanken

Christian Wischki
cw@christianwischki.com

Kyle Krüsi
kyle@zynex.ch