Oracle Database Security:
Wie viel darf es denn sein?

Sven Vetter
Trivadis AG
Glattbrugg, Schweiz

Schlüsselworte:

Database Security, Risikoanalyse, Kategorisierung, Securityklassen, Database Hardening, Authentifizierung, Autorisierung, Oracle Optionen, Database Vault, Audit Vault, McAfee Database Activity Monitoring

Einleitung

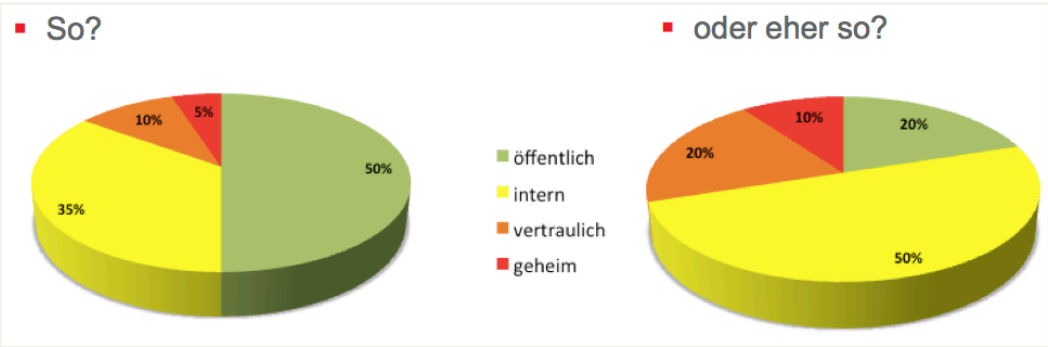
Oracle bietet innerhalb der Datenbank diverse Features, um die Datensicherheit zu gewährleisten:

- VPD, RLS, ASO, TDE, DBV, AV, ...

Ein Teil ist nur in der Enterprise Edition vorhanden, ein Teil zusätzlich lizenzpflichtig. Außerdem gibt es von Oracle noch weitere, externe Produkte. Und natürlich gibt es auch noch Dritthersteller...

Was brauche ich davon aber in meiner Datenbank?
Und wenn ich viele (unterschiedliche) Datenbanken habe – was dann?

Wie ist der Anteil von öffentlichen, vertraulichen, internen, geheimen, ... Daten?



Risikoanalyse und Kategorisierung

Um diese Fragen beantworten zu können, bedarf es in einem ersten Schritt einer Risikoanalyse. Der Besitzer der Daten (bzw. der Applikation) muss die Sensitivität seiner Daten definieren. Das ist nicht immer ganz einfach, da jeder davon ausgeht, dass seine Daten die wichtigsten, kritischsten, ... sind.
Wir benutzen dazu die Trivadis First Cut Risikoanalyse:

- Einfach durchzuführen
- In "Business-Sprache"
- Gefährdungen werden schnell erkannt
- Geht nicht in die (technische) Tiefe, aber danach ist bekannt, vorauf man sich konzentrieren muss

Abgefragt werden (u.a.):

- Werden Personendaten oder sogar besonders schützenswerte Personendaten (Gesundheit, Religion, Strafmaßnahmen, ...) verarbeitet?
- Was geschieht bei Verlust der Vertraulichkeit? (Wettbewerbsnachteile, Geschäftsschädigung, Störung des öffentliches Vertrauens, Haftung, ...)?
- Was geschieht bei Verlust der Integrität? (falsche Management Entscheide, zusätzliche Kosten, Geschäftsunterbruch)?
- Was geschieht bei Verlust der Verfügbarkeit (Wiederherherstellung, ...)?

Der Datenowner bewertet alle diese Punkte in einer 3stufigen Skala (von nicht kritisch über kritisch bis geschäftskritisch). Hier können auch Werte für den materiellen Schaden hinterlegt werden, dies hilft häufig für die Einschätzung.

D) Impact Analyse

Vertraulichkeit

	Schadenszenarien	Schadensausmass A B C	Beschreibung
1	**Wettbewerbsnachteile** Wie schädlich sind die Auswirkungen, wenn der Konkurrenz Daten offen gelegt würden?	☐ ☒ ☐	
2	**Direkte Geschäftsschädigung** Wie hoch wäre der direkte Schaden durch die Offenlegung von Informationen bzw. in welchem Ausmass könnten dadurch Geschäfte verloren gehen?	☐ ☐ ☒	
3	**Öffentliches Vertrauen** In welchem Ausmass können durch die Offenlegung von Informationen das Vertrauen der Kunden, das öffentliche Image und der gute Ruf oder das Vertrauen der Aktionäre und Lieferanten gestört werden?	☐ ☐ ☒	
4	**Zusätzliche Kosten** Wie hoch sind die entstehenden Zusatzkosten, wenn Informationen öffentlich werden?	☐ ☒ ☐	
5	**Gesetzliche Haftung** Welche Auswirkungen hat die Offenlegung von Informationen auf gesetzliche oder vertragliche Verpflichtungen?	☐ ☒ ☐	
6	**Betrug** Wie schädlich wäre ein Betrug, der durch Offenlegung von Informationen begangen wird?	☐ ☐ ☒	
	Höchste Schadenstufe (Maximum der oben stehenden Einschätzungen)	☐ ☒ ☐	

Abb. 1: Auszug aus der First Cut Risikoanalyse

Durch die Risikoanalyse erfolgt die Einteilung der Daten(-banken) in Securityklassen. Typischerweise benutzt man folgende Klassen:

- Öffentlich (Daten sind z.B. im Internet sichtbar – dürfen dort aber sicherlich nicht manipuliert werden)
- Intern (Daten dürfen von allen Mitarbeitern gesehen werden)
- Vertraulich (Daten dürfen nur von einem definierten Kreis von Mitarbeitern gesehen werden)
- Geheim (Wenn diese Daten verloren gehen, ist die Existenz der Firma gefährdet, z.B. das Rezept von Coca Cola)

Risikomatrix

Im zweiten Schritt definiert man eine Risikomatrix:

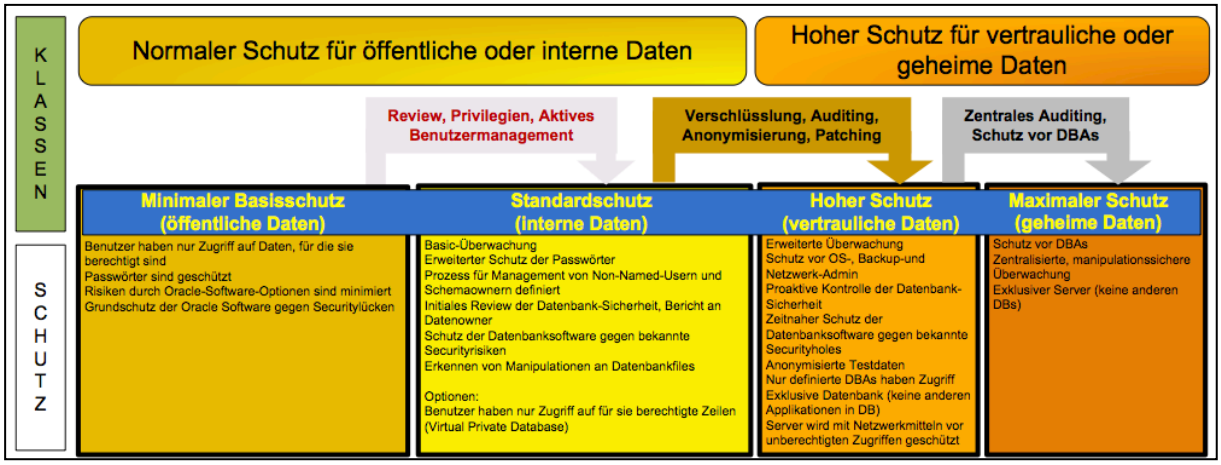


Abb. 2: Risikomatrix: Klassen und zu reduzierende Risiken

Pro Klasse werden dann die Maßnahmen definiert, welche die Risiken minimieren. Auch anfallende Kosten können hier aufgeführt werden:

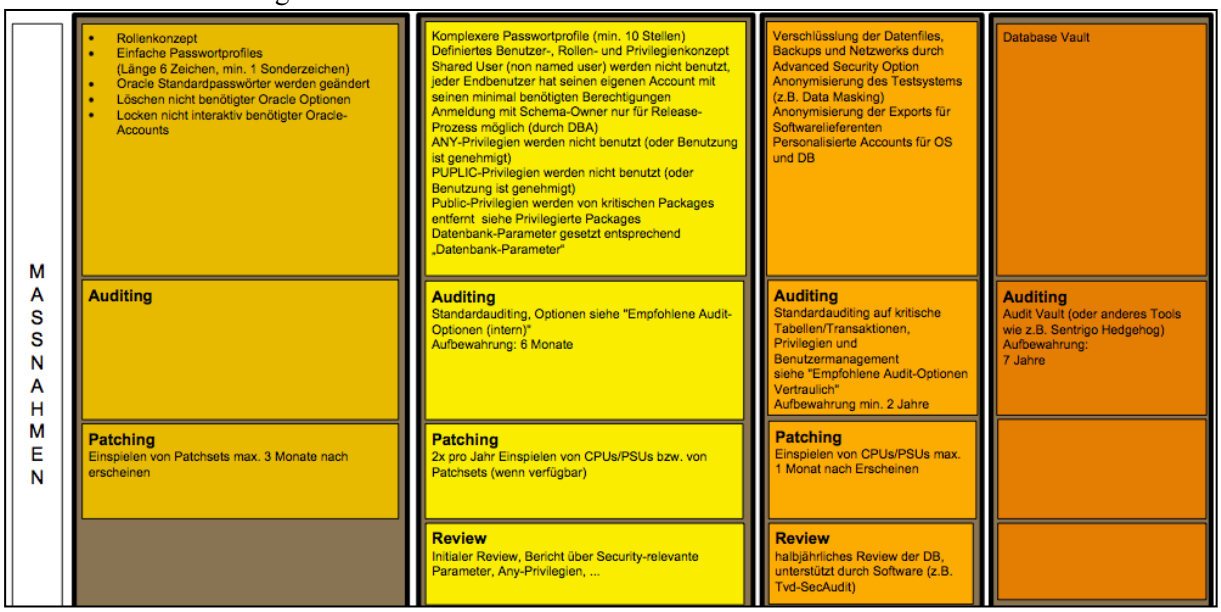


Abb. 3: Risikomatrix: Maßnahmen

Welche Maßnahmen in welcher Klasse umgesetzt werden, ist firmenspezifisch. Zu den typischen Angriffspunkten hier einige mögliche Abwehraktionen:

Authentifizierung:

- Jeder Benutzer hat seinen eigenen, persönlichen Benutzer
  - Sowohl in der Datenbank als auch auf OS Ebene
- Es existiert eine zentrale Benutzerverwaltung
  - Verwaltung in einem zentralen Verzeichnis
  - Anmeldung über dieses Verzeichnis
    - z.B. Enterprise Users
  - oder Provisionierung der Benutzer in die Datenbanken
    - z.B. CUA4DB (Centralized User Administration for Database
- Starke Authentifizierung (mehr als nur Benutzername und Passwort)

Passwörter:

- Passwörter unterliegen Komplexitätsregeln
  - Minimale Länge
  - Benutzer von numerischen Zeichen, Sonderzeichen, ...
  - Keine gebräuchlichen Wörter
- Passwörter müssen regelmässig geändert werden
  - Dürfen nicht wiederbenutzt werden
  - Müssen sich auf definierte Art vom alten Passwort unterscheiden
- Nicht interaktiv benötigte Accounts werden gelockt (oder auf unmögliches Passwort gesetzt)
  - Gilt auch (oder gerade) für Oracle Default Schemata

Datenzugriff:

- Benutzer haben nur Zugriff auf Daten, für die sie Berechtigungen haben (auf Tabellenebene):
  - Rollenkonzept
  - Keine Public Grants
- Benutzer haben nur Zugriff auf Daten, für die sie Berechtigungen haben (auf Zeilenebene):
  - Virtual Private Database (Security Policies)
  - Label Security
- Auch Administratoren haben nur Zugriff auf berechtigte Daten
  - Database Vault
  - Verschlüsselung vor der Datenbank (durch die Applikation oder Verschlüsselungs-lösungen wie z.B. von Safenet)
  - Tokenization

Auditing:

- Grundlegende Operationen werden auditiert (z.B. Connect)
- Kritische Operationen werden auditiert
  - Benutzung von ANY Privilegien
  - Benutzer- und Berechtigungsmanagement
  - Operationen von SYSDBAs
- Zugriffe auf kritische Objekte werden auditiert
  - Definition der kritischen Objekte
  - Definition der Regeln, wann ein Zugriff auditiert werden soll
- Zentrales Auditing
  - Oracle Audit Vault
  - McAfee Database Activity Monitoring
  - ...

Weitere Möglichkeiten:

- Installation nur von benötigten Optionen
- Patching der Oracle Software (Patchsets, CPUs, PSUs)
- Setzen von Initialisierungsparametern (Definition einer Baseline)
- Netzwerk
    - Database Firewall (Oracle, Imperva)
    - Verschlüsselung (Advanced Security Option)
    - Zonenkonzept
- Release Management
    - Wer hat wann Zugriff auf Schemaowner (die ja gelockt sein sollen)
    - Dokumentation der Prozesse
- Anonymisierung von Testdaten
- Schutz von Datenfiles, Exports, Dumps, Backups durch Verschlüsselung

Fazit

Die Definition, welches Risiko durch welche Maßnahme reduziert werden kann, ist nicht einfach. Außerdem sollte noch regelmäßig überwacht werden, ob die Maßnahmen auch umgesetzt wurden – und nicht durch irgendwelche Eingriffe (z.B. Installation neuer Applikationen) zurückgesetzt wurden.

Trotz allem lohnt sich dieser Aufwand, da nicht für jede Datenbank alle Optionen eingesetzt werden müssen – also an Lizenzkosten gespart werden kann.

Wir unterstützen Sie selbstverständlich gern bei der Ausarbeitung einer individuellen Matrix für Sie – und natürlich auch bei der Umsetzung.

Kontaktadresse:

Sven Vetter
Trivadis AG
Europa-Strasse 5
CH-8152 Glattbrugg (Zürich)

Telefon: +41-44-808 70 20
E-Mail Sven.Vetter@trivadis.com
Internet: www.trivadis.com