Oracle Database Security: Wie viel darf es denn sein?

Oracle Database Security Seminar

Stefan Oehrli
Senior Consultant
Discipline Manager
Trivadis AG

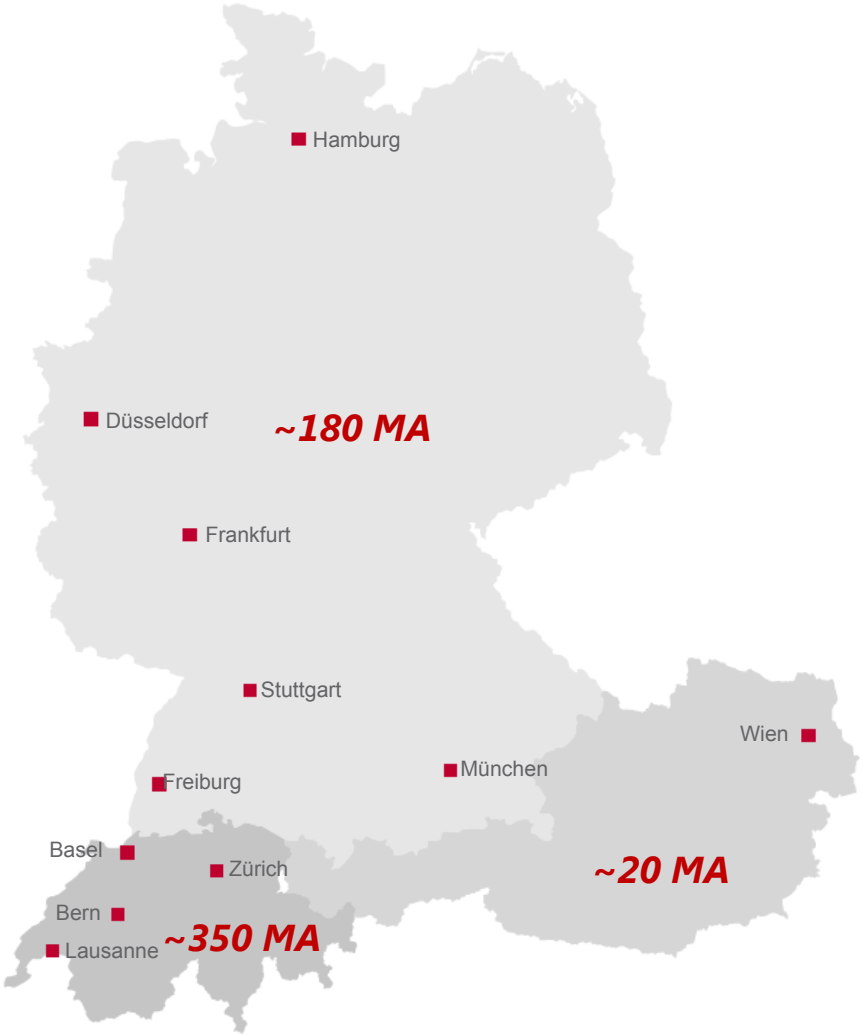
08 / 09 Februar 2012,
Düsseldorf + Berlin

BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

2011 © Trivadis

trivadis
makes IT easier.

Trivadis Facts & Figures



11 Trivadis Niederlassungen mit über 550 Mitarbeitern

Finanziell unabhängig und nachhaltig profitabel

Kennzahlen 2010

- Umsatz CHF 101 / EUR 73 Mio.
- Dienstleistungen für über 700 Kunden in mehr als 1‘800 Projekten
- Über 170 Service Level Agreements
- Mehr als 5'000 Trainingsteilnehmer
- Forschungs- und Entwicklungs-budget: CHF 5.0 / EUR 3.6 Mio.

2011 © Trivadis

trivadis
makes IT easier.

Das Besondere

Kundenindividuelle Lösungskompetenz und Herstellerunabhängigkeit	▪ bietet fundierte Methodenkenntnisse und eigenentwickelte Vorgehensweisen ▪ garantiert wiederholbare Qualität und Realisierungssicherheit
Technologiekompetenz	▪ hat über 17 Jahre Expertise in Oracle und Microsoft ▪ verfügt über ein eigenes Technology Center und setzt auf technologische Exzellenz
Lösungs- und Integrations-Know-how	▪ hat eine breite, branchenübergreifende Kundenbasis und jährlich über 1800 Projekte ▪ verbindet technologisches Spezialisten Wissen mit dem Verständnis für die Business-Spezifika des Kunden
Begleitung über den gesamten IT-Projekt-Lifecycle	▪ begleitet den gesamten IT-Projekt-Lifecycle mit einem modularen Dienstleistungsportfolio ▪ bietet für jeden „Reifegrad" die passende Dienstleistungs- und Lösungskombination

2011 © Trivadis

trivadis
makes IT easier.

AGENDA

1. Übersicht
2. Risikoanalyse und Kategorisierung
3. Risikomatrix
4. Risikominimierung
5. Überprüfung

2011 © Trivadis

trivadis
makes IT easier.

Einleitung – Fragen

- Oracle bietet innerhalb der Datenbank diverse Features, um die Datensicherheit zu gewährleisten
  - VPD, ASO, TDE, DBV, AV, … ☺
- Ein Teil ist nur in der Enterprise Edition vorhanden, ein Teil ist zusätzlich lizenzpflichtig
- Außerdem gibt es von Oracle noch weitere, externe Produkte
- Und natürlich auch Lösungen von Drittthersteller…

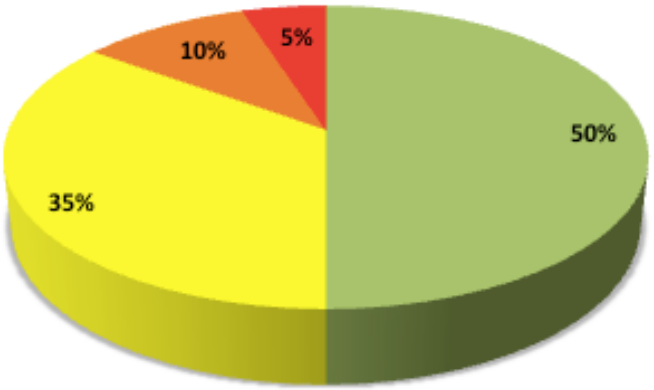
- Was brauche ich davon aber in meiner Datenbank?
- Und wenn ich viele (unterschiedliche) Datenbanken habe?

2011 © Trivadis

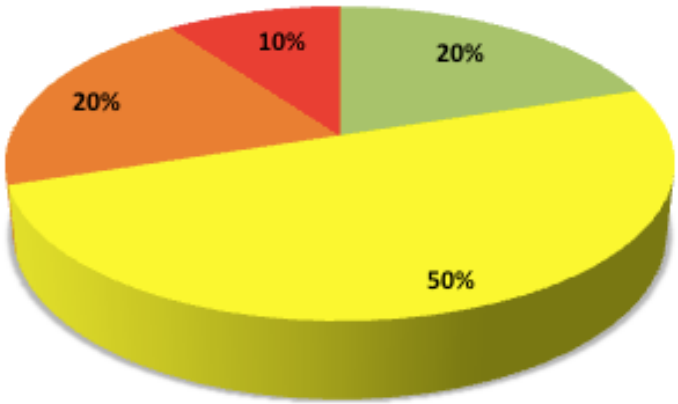
trivadis
makes IT easier.

Einleitung – Fragen

- Kennen Sie Ihre Daten?
- Beziehungsweise deren Sensitivität?
- Wie ist der Anteil von öffentlichen, vertraulichen, internen, geheimen, … Daten
- So?



- oder eher so?



2011 © Trivadis

trivadis
makes IT easier.

AGENDA

1. Übersicht
2. Risikoanalyse und Kategorisierung
3. Risikomatrix
4. Risikominimierung
5. Überprüfung

2011 © Trivadis

trivadis
makes IT easier.

Risikoanalyse

- Der Besitzer der Daten (bzw. der Applikation) muss die Sensitivität seiner Daten definieren
- Das ist nicht immer ganz einfach, da jeder davon ausgeht, seine Daten sind die wichtigsten, kritischsten, ...
- Deshalb empfiehlt sich die Durchführung einer Risikoanalyse
- 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

2011 © Trivadis

trivadis
makes IT easier.

First Cut Risikoanalyse - Inhalt

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

2011 © Trivadis

trivadis
makes IT easier.

First Cut Risikoanalyse – Analyse

D) Impact Analyse

Vertraulichkeit

	Schadenszenarien	Schadensausmass A	Schadensausmass B	Schadensausmass 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)	☐	☒	☐	

2011 © Trivadis

trivadis
makes IT easier.

First Cut Risikoanalyse - Konsolidierung

E) Konsolidierte Einschätzung

Übertrag aus Impact Analyse

Vertraulichkeit	Integrität	Verfügbarkeit
A ☐ B ☐ C ☐	A ☐ B ☐ C ☐	A ☐ B ☐ C ☐ 4h A ☐ B ☐ C ☐ 1t A ☐ B ☐ C ☐ 3t A ☐ B ☐ C ☐ 7t

Welcher Schutzbedarf hat diese Applikation/System? (Daraus werden die Sicherheitsmassnahmen abgeleitet. Der höchste Wert (A= Hoch, B=Mittel, C=Normal) der Vertraulichkeit oder der Integrität bestimmt den Schutzbedarf)	Hoch ☐ Mittel ☐ Normal ☐
Welche Sicherheitsmassnahmen werden zur Risikoreduzierung eingeführt? (ev. Referenz zu Sicherheitskonzept)	☒ Grundschutz (obligatorisch für alle produktiven Systeme) ☐ Weitere Massnahmen (bitte beschreiben) ▪ .....

2011 © Trivadis

trivadis makes IT easier.

Klassifizierung

- Durch die Risikoanalyse erfolgt die Einteilung der Daten(-banken) in Sicherheitsklassen
- 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)

2011 © Trivadis

trivadis
makes IT easier.

AGENDA

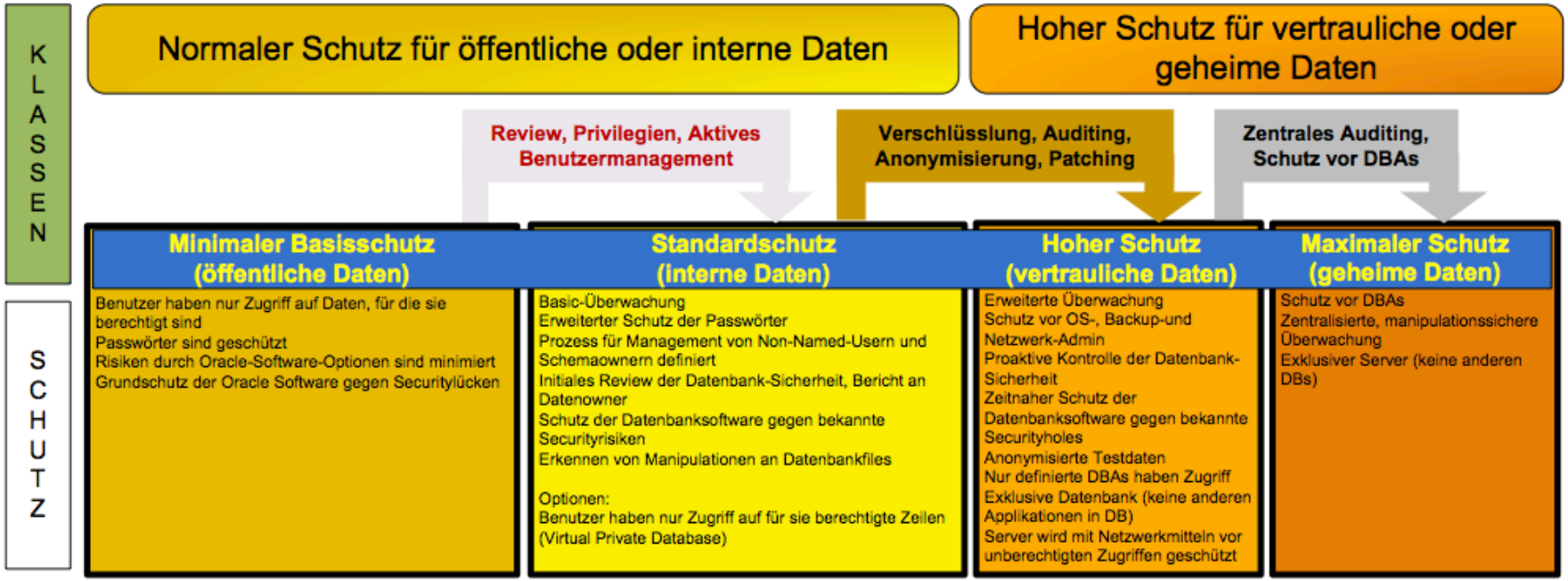
1. Übersicht
2. Risikoanalyse und Kategorisierung
3. Risikomatrix
4. Risikominimierung
5. Überprüfung

2011 © Trivadis

trivadis
makes IT easier.

Risikomatrix (1)

- Der Kopf der Matrix definiert die Klassen und die zu reduzierenden Risiken:



2011 © Trivadis

trivadis
makes IT easier.

Risikomatrix (2)

- Im weiteren werden dann die Maßnahmen definiert, mit denen die definierten Risiken reduziert werden sollen:

MASSNAHMEN				
	• Rollenkonzept • Einfache Passwortprofiles (Länge 6 Zeichen, min. 1 Sonderzeichen) • Oracle Standardpasswörter werden geändert • Löschen nicht benötigter Oracle Optionen • Locken nicht interaktiv benötigter Oracle-Accounts	Komplexere Passwortprofile (min. 10 Stellen) Definiertes Benutzer-, Rollen- und Privilegienkonzept Shared User (non named user) werden nicht benutzt, jeder Endbenutzer hat seinen eigenen Account mit seinen minimal benötigten Berechtigungen Anmeldung mit Schema-Owner nur für Release-Prozess möglich (durch DBA) ANY-Privilegien werden nicht benutzt (oder Benutzung ist genehmigt) PUPLIC-Privilegien werden nicht benutzt (oder Benutzung ist genehmigt) Public-Privilegien werden von kritischen Packages entfernt siehe Privilegierte Packages Datenbank-Parameter gesetzt entsprechend „Datenbank-Parameter"	Verschlüsslung der Datenfiles, Backups und Netzwerks durch Advanced Security Option Anonymisierung des Testsystems (z.B. Data Masking) Anonymisierung der Exports für Softwarelieferenten Personalisierte Accounts für OS und DB	Database Vault
	Auditing	**Auditing** Standardauditing, Optionen siehe "Empfohlene Audit-Optionen (intern)" Aufbewahrung: 6 Monate	**Auditing** Standardauditing auf kritische Tabellen/Transaktionen, Privilegien und Benutzermanagement siehe "Empfohlene Audit-Optionen Vertraulich" Aufbewahrung min. 2 Jahre	**Auditing** Audit Vault (oder anderes Tools wie z.B. Sentrigo Hedgehog) Aufbewahrung: 7 Jahre
	Patching Einspielen von Patchsets max. 3 Monate nach erscheinen	**Patching** 2x pro Jahr Einspielen von CPUs/PSUs bzw. von Patchsets (wenn verfügbar)	**Patching** Einspielen von CPUs/PSUs max. 1 Monat nach Erscheinen	
		Review Initialer Review, Bericht über Security-relevante Parameter, Any-Privilegien, ...	**Review** halbjährliches Review der DB, unterstützt durch Software (z.B. Tvd-SecAudit)	

2011 © Trivadis

trivadis
makes IT easier.

Risikomatrix (3)

- Wichtig ist, auch die Konsequenzen (und Kosten) zu definieren:

KONSEQUENZEN				
		Anforderungen an Data-Owner: Benutzer-, Rollen- und Privilegienkonzept muss zusammen mit Data-Owner definiert werden	**Anforderungen:** Kritische Tabellen müssen definiert werden	**Anforderungen:** Prozesse müssen geändert werden (z.B. Benutzer-management liegt beim Kunden)
	Kosten **(jeweils unverhandelt pro Prozessor)**	**Kosten:** Diskplatz (minimal)	**Kosten:** Diskplatz (mittel) ASO: 13k Data Masking Pack: 13k RepView: 1k pro DB	**Kosten:** Diskplatz (hoch) AV-Agent: 4k AV-Server: 66k Database Vault: 26k

2011 © Trivadis

trivadis
makes IT easier.

AGENDA

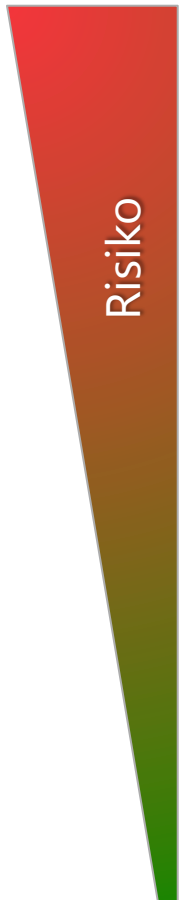
1. Übersicht
2. Risikoanalyse und Kategorisierung
3. Risikomatrix
4. Risikominimierung
5. Überprüfung

2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung - Authentifizierung

- Benutzer melden sich mit nur einem Sammelbenutzer an
- 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)



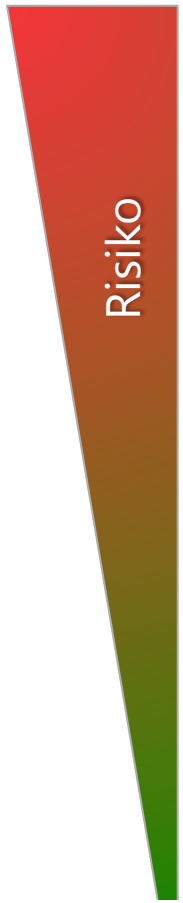
- **Achtung: Authentifizierung ist die Grundlage für alles weitere!**

2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung - Passwörter

- Es existieren keine Passwortregeln
- Passwörter unterliegen Komplexitätsregeln
  - Minimale Länge
  - Benutzer von numerischen Zeichen, Sonderzeichen, ...
  - Keine gebräuchlichen Wörter
- **Alle** 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

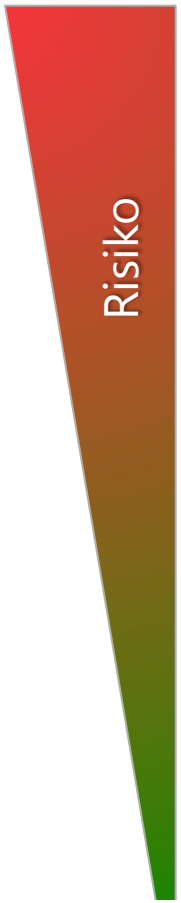


2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung - Datenzugriff

- Benutzer können alle Daten lesen/ändern
- 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 Verschlüsselungslösungen wie z.B. von Safenet)
  - Tokenization



2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung - Datenzugriff - Bemerkungen

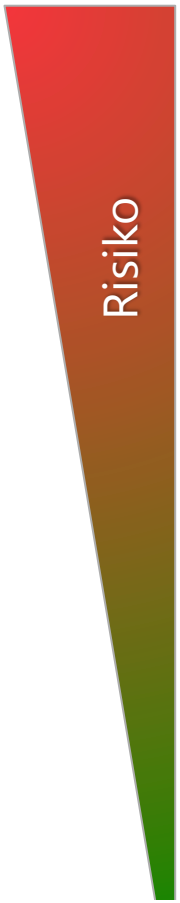
- Wichtig dabei ist zu erkennen, auf welche Art jemand Zugriff auf Daten erlangen kann:
  - Owner der Tabelle
  - Direkter Grant auf die Tabelle
  - Über eine (geschachtelte) Rolle
  - Public-Berechtigung
  - Über eine View oder ein Package
  - Über ein Systemprivileg (select any table)
  - Über hoch privilegierte Rollen (dba, sysdba)
- An Rollenwechsel denken (Praktikanten haben die meisten Rechte...)
- Tools für die Analyse benutzen wie z.B. Oracle Identity Analytics

2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung - Auditing

- Auditing ausgeschaltet
- Nur 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
  - SYSLOG Auditing
  - McAfee Database Activity Monitoring



2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung - Auditing - Bemerkung

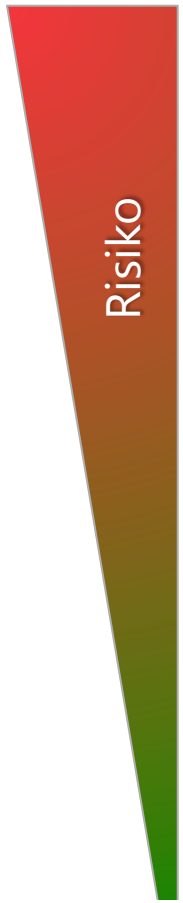
- Häufig will man den Zugriff auf Tabellen nur bei bestimmten Bedingungen überwachen
  - Einsatz von Fine Grained Auditing (FGA)
- Daten müssen regelmäßig ausgewertet
  - Reporting Funktionen bei einem Zentralen Auditing mit Oracle Audit Vault
  - Auswertung / Tools bei einem SYSLOG Server
  - Manuelles Reporting in der Datenbank
  - Alarmierung bei Problemen / Verstößen!
- Und wie lange sollen diese Aufbewahrt werden?
  - Definition der Aufbewahrungszeiten für Rohdaten und Reports.
  - Automatisiertes Housekeeping
  - Archivierung

2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung - Patching

- Kein Einspielen von Security-Paches und Patch-Sets
- Regelmäßiges Einspielen der Patch-Sets (11.2.0.**3**)
- Regelmäßiges Einspielen von CPUs oder PSUs
- Zeitnahes Einspielen jedes CPUs bzw. PSUs
  - Z.B. max. ein Monat nach Erscheinen des CPUs
- Virtuelles Patching
  - McAfee Database Activity Monitoring (zusätzlicher Schutz zum CPU/PSU)

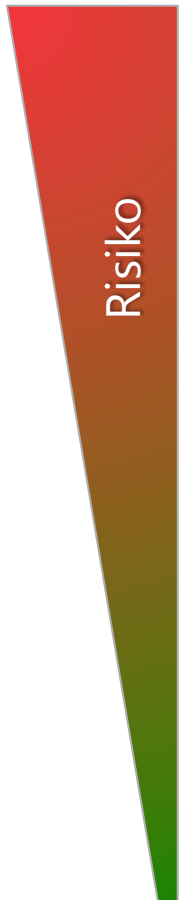


2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung – Oracle Software & Optionen

- Beliebige Software und Optionen sind installiert
- Nur benötigte Optionen sind in der Datenbank installiert
  - Kritsch z.B. Java, XDB, ...
- Nur benötige Software ist im Oracle Home installiert
- Die benötigten Optionen werden gehärtet
  - Keine Grants an Public (wie es standardmäßig häufig der Fall ist)
  - Rollenkonzept, nur Berechtigungen an Benutzer, die Funktionalität brauchen
  - Network Callouts (Mail, TCP, ...) werden eingeschränkt

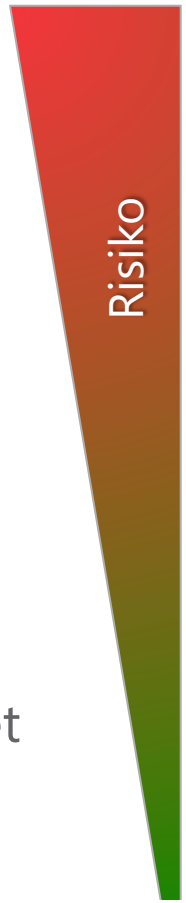


2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung – Parameter

- Initialisierungsparameter stehen beliebig
- Definition einer Baseline für sicherheitskritische Parameter, z.B.
  - 07_DICTIONARY_ACCESSIBILITY
  - AUDIT_SYS_OPERATIONS, AUDIT_TRAIL
  - DB_BLOCK_CHECKING
  - REMOTE_OS_AUTHENT
  - REMOTE_OS_ROLES
  - UTL_FILE_DIR
- Durchsetzen der Baseline
- Ausnahmen (eventuell durch Applikation gefordert) sind begründet und **dokumentiert**



2011 © Trivadis

trivadis
makes IT easier.

Risikominimierung – weitere Möglichkeiten

- Netzwerk:
  - Database Firewall (Oracle, Imperva)
  - Verschlüsselung (Advanced Security Option)
  - Zonenkonzept
- Release Management:
  - Wer hat wann Zugriff auf Schema Owner (die ja gelockt sein sollen)
  - Dokumentation der Prozesse
- Anonymisierung von Testdaten (Oracle Data Masking)
- Schutz von Datenfiles, Exports, Dump's, Backups durch Verschlüsselung

2011 © Trivadis

trivadis
makes IT easier.

AGENDA

1. Übersicht
2. Risikoanalyse und Kategorisierung
3. Risikomatrix
4. Risikominimierung
5. Überprüfung

2011 © Trivadis

trivadis
makes IT easier.

Überprüfen dieser Massnahmen

- Die Einhaltung dieser Massnahmen sollte regelmässig und möglichst automatisch überprüft werden
- Dazu bietet sich das Trivadis Tool Tvd-SecAudit© an

1. Oracle Software and Options

Test	Passed	Prio	Results	Description
1.1. Check Oracle software and patches				
1.1.1. Installed Patchsets	Passed	▲	Next patchset (11.2.0.3) isn't available yet	*[sof100]* Regelmaessiges Einspielen von Patchsets erhoeht die Sicherheit der Datenbank erheblich. Ausserdem werden dadurch auch diverse andere Bugs behoben. Spaetestens 6 Monate nach Erscheinen eines Patchsets sollte dies eingespielt sein.
1.1.2. Installed PSUs	Failed	▲	PSU Jun2011: not installed PSU Apr2011: not installed PSU Jan2011: not installed	*[sof120]* Regelmaessiges Einspielen von Patch Set Updates (PPU) erhoeht die Sicherheit der Datenbank erheblich. Spaetestens nach 6 Monaten muss der PSU eingespielt sein.
1.1.3. Installed CPUs	Partial	▲	CPUApr2011: not installed No CPU installed in the last 6 month. *First cpu for 11.2.0.2 younger than 6 months.*	*[sof140]* Regelmaessiges Einspielen von Critical Patch Updates (CPU) erhoeht die Sicherheit der Datenbank erheblich. Spaetestens nach 6 Monaten muss der CPU eingespielt sein.
1.2. Check Oracle options				
1.2.1. Installed options: XDB	Failed	▲	Oracle XML Database is installed. But not in use! Usage count: 0 (in 2 samples)	*[sof300]* Oracle XML Database sollte nur installiert werden, wenn wirklich mit XML-Files innerhalb der Datenbank gearbeitet wird.

- http://www.trivadis.com/produkte/datenbank-tools/tvd-secauditm.html

2011 © Trivadis

trivadis
makes IT easier.

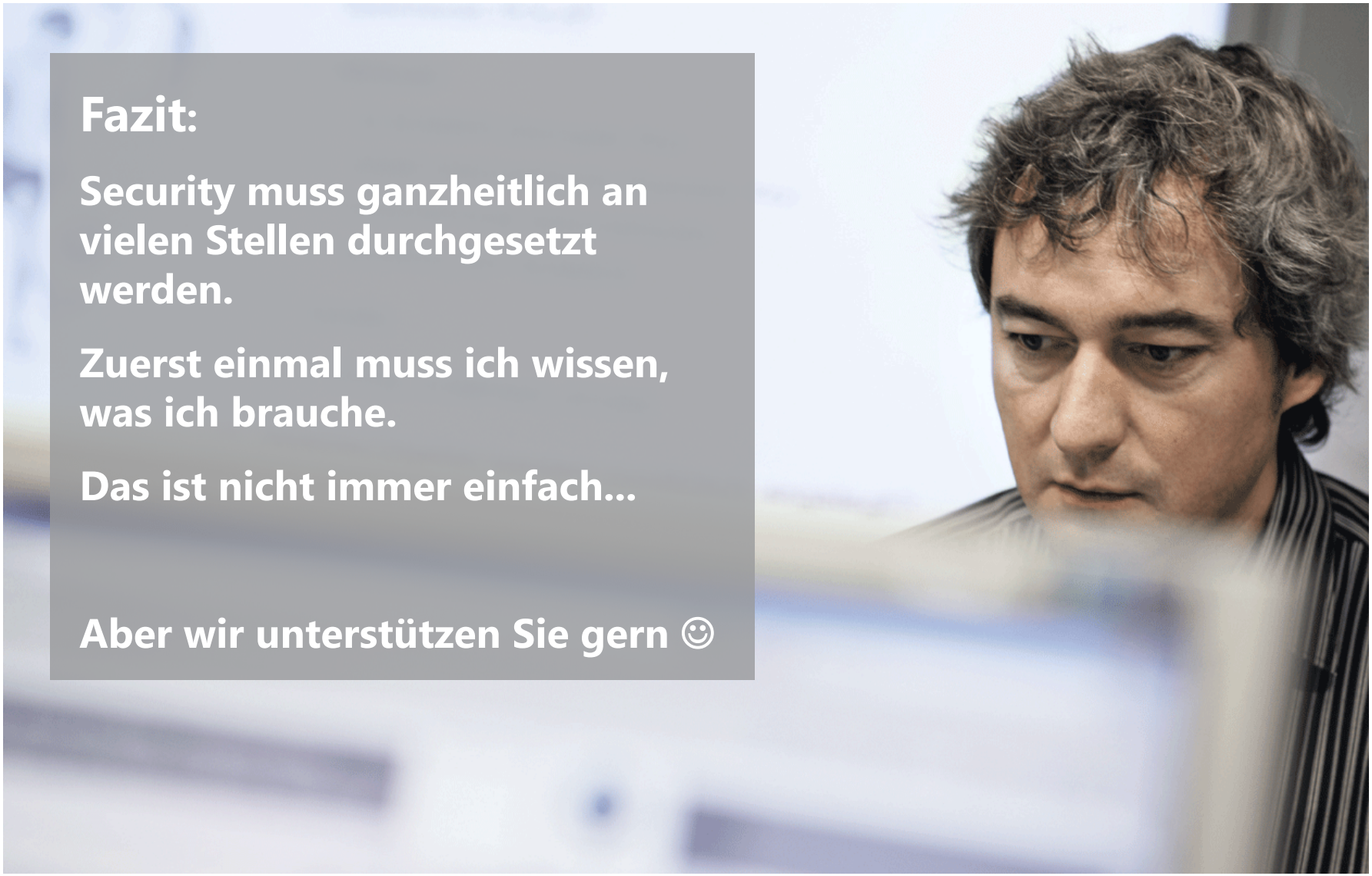
Fazit:

Security muss ganzheitlich an vielen Stellen durchgesetzt werden.

Zuerst einmal muss ich wissen, was ich brauche.

Das ist nicht immer einfach...

Aber wir unterstützen Sie gern ☺



2011 © Trivadis

trivadis
makes IT easier.

?

Fragen ?

2011 © Trivadis

trivadis
makes IT easier.

VIELEN DANK.

Trivadis AG

Stefan Oehrli

Europa-Strasse 5
CH-8152 Glattbrugg

Tel. +41 44 808 70 20

stefan.oehrli@trivadis.com
www.trivadis.com
www.oradba.ch

BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

2011 © Trivadis

trivadis
makes IT easier.