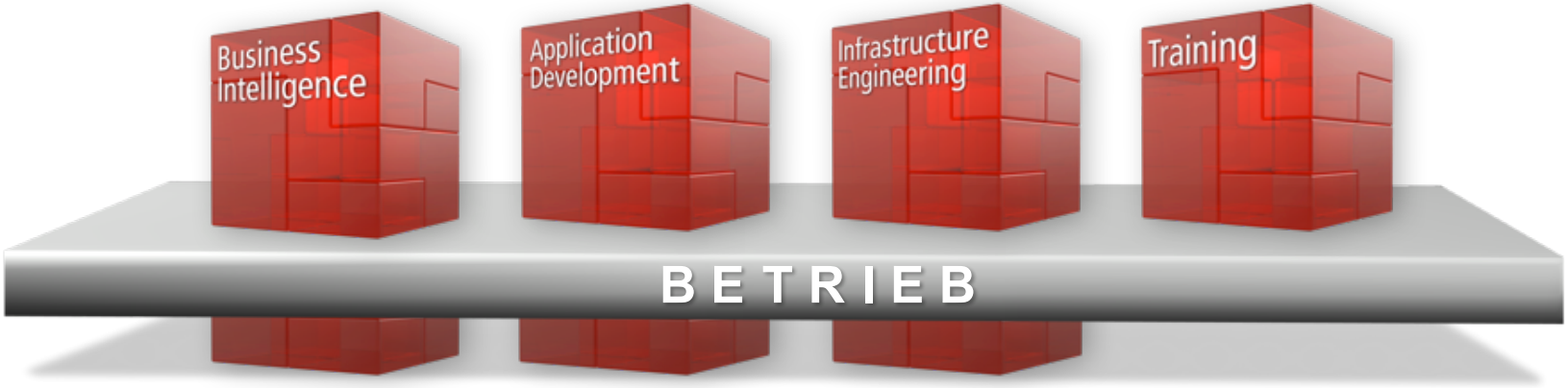
Oracle Database Security –

Wieviel darf es sein?

Stefan Oehrli

Unser Unternehmen.

Trivadis ist führend bei der IT-Beratung, der Systemintegration, dem Solution Engineering und der Erbringung von IT-Services mit Fokussierung auf ORACLE - und Microsoft -Technologien in der Schweiz, Deutschland, Österreich und Dänemark. Trivadis erbringt ihre Leistungen aus den strategischen Geschäftsfeldern:



Trivadis Services übernimmt den korrespondierenden Betrieb Ihrer IT Systeme.

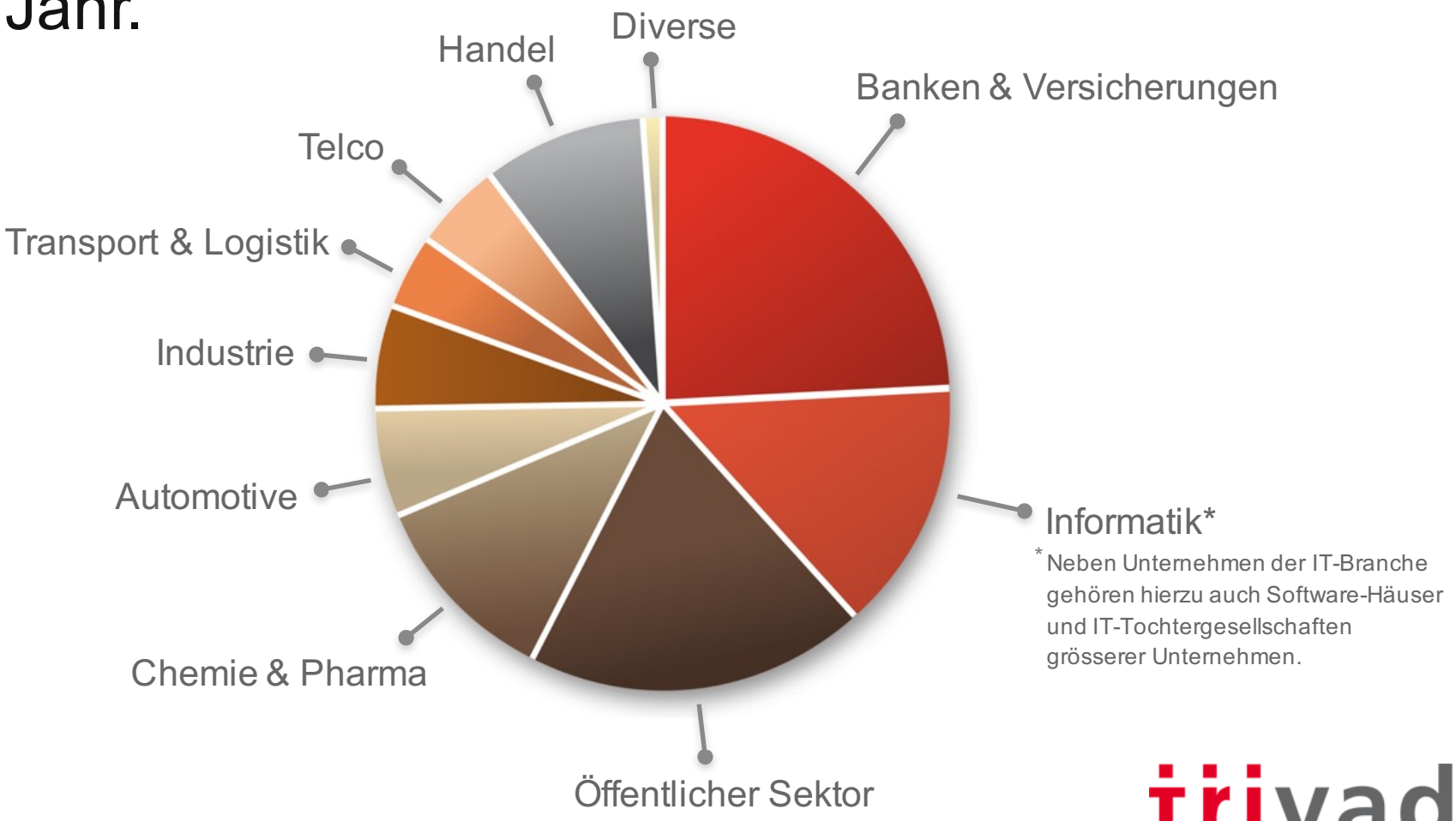
trivadis
makes IT easier.

Mit über 600 IT- und Fachexperten bei Ihnen vor Ort.

- 14 Trivadis Niederlassungen mit über 600 Mitarbeitenden.
- Über 200 Service Level Agreements.
- Mehr als 4'000 Trainingsteilnehmer.
- Forschungs- und Entwicklungsbudget: CHF 5.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

trivadis
makes IT easier.

Unsere Fachkompetenz aus über 1'900 Projekten pro Jahr.



* Neben Unternehmen der IT-Branche gehören hierzu auch Software-Häuser und IT-Tochtergesellschaften grösserer Unternehmen.

trivadis
makes IT easier.

Stefan Oehrli

Solution Manager BDS SEC

- Seit 1997 IT-Bereich tätig
- Seit 2008 bei der Trivadis AG
- Seit 2010 Disziplin Manager SEC INFR
- Seit 2014 Solution Manager BDS Security

IT Erfahrung

- DB Administration und DB Security Lösungen
- Administration komplexer, heterogenen Umgebungen
- Datenbank Teamleiter

Spezialgebiet

- Datenbank Sicherheit Security und Betrieb
- Security Konzepte
- Security Reviews
- Oracle Backup & Recovery

Skills

- Backup & Recovery
- Oracle Advanced Security
- Audit Vault und Database Firewall, Database Vault
- Team / Projekt Management

trivadis makes IT easier.

Technik allein bringt Sie nicht weiter.

Man muss wissen, wie man sie richtig nutzt.

trivadis
makes IT easier.

Agenda

1. Übersicht
2. Risikoanalyse und Bewertung
3. Risikomatrix und Schutzklassen
4. Risikoverminderung
5. Überprüfung
6. Fazit

trivadis
makes IT easier.

Übersicht

trivadis
makes IT easier.

Warum IT-Sicherheit?

Schutz des Unternehmens und dessen Business

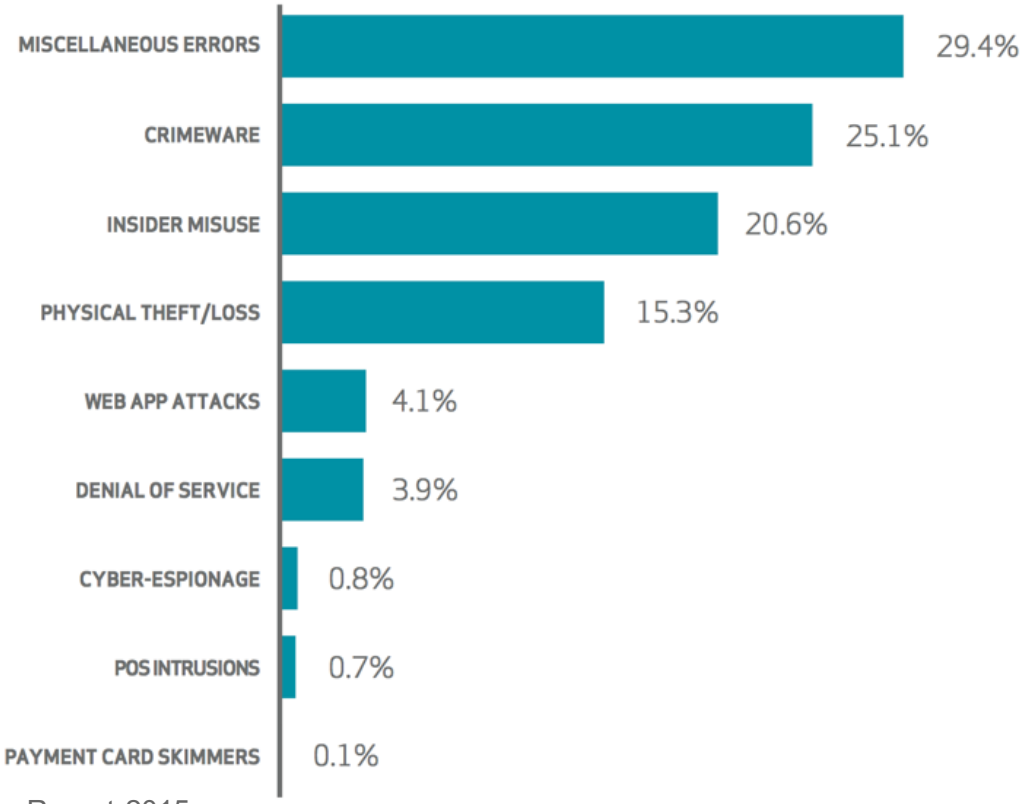
- Finanzieller Schaden
- Image Verlust
- Wettbewerbsfähigkeit
- Strafrechtliche Folgen
- Existenzbedrohung

Schutz der Mitarbeiter, Kunden und anderen Personen

- Privatsphäre
- Erwerbstätigkeit
- Verfolgung
- Strafrechtliche Folgen

trivadis
makes IT easier.

Sicherheitsrisiken

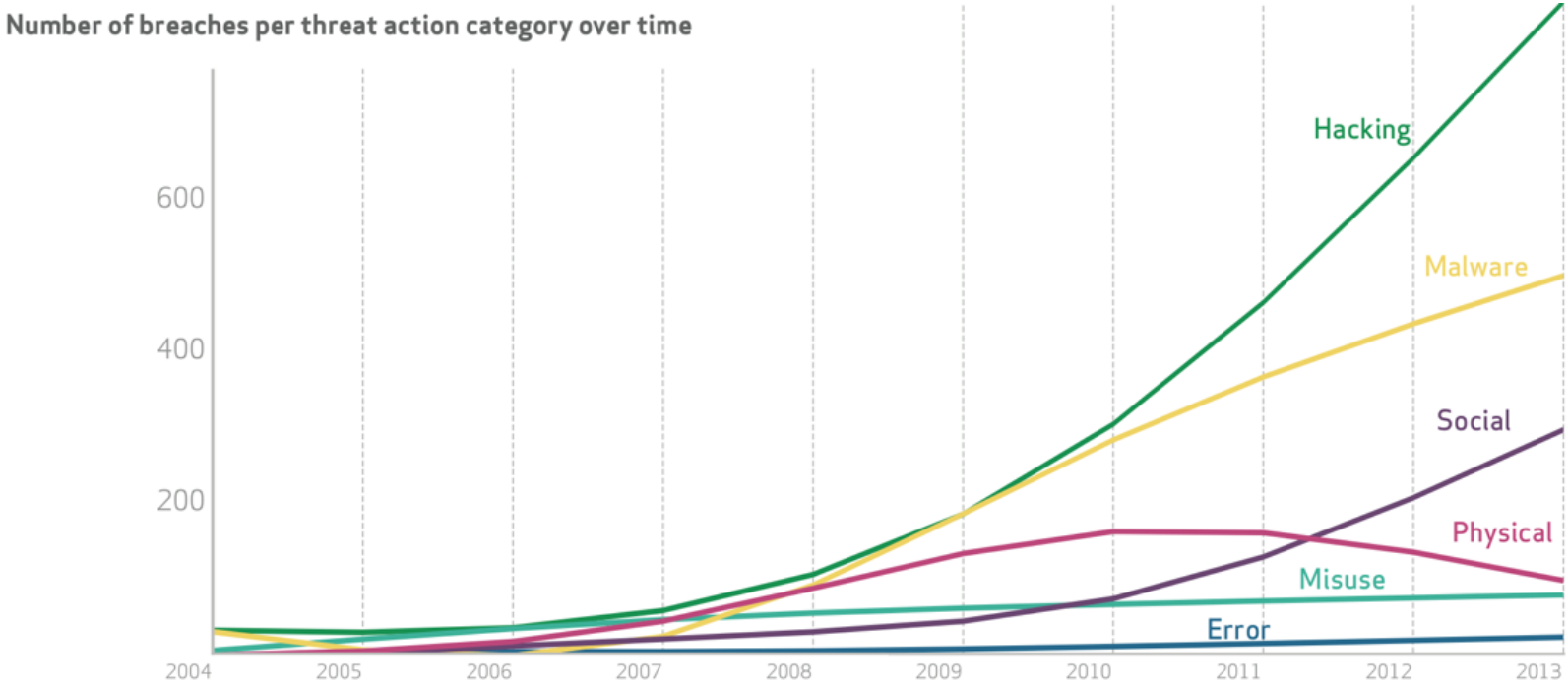


Verizon Data Breach Investigation Report 2015

trivadis makes IT easier.

Sicherheitsrisiken

Entwicklung der Sicherheitsvorfälle nach Gefahrenkategorie 2004 - 2013



Verizon Data Breach Investigation Report 2014

trivadis makes IT easier.

Rechtliche Aspekte

Strafrecht
StGB, SCC-CH,…

Schutz der:

Vertraulichkeit

Integrität

Verfügbarkeit

IT-Sicherheit
Schutz der Daten

Datenschutz
Schutz der Personen (-Daten)

Compliance / Zivielrechtliche Aspekte
GeBüV, SOX, Basel 2, PCI-DSS, …

trivadis
makes IT easier.

Angriffsvektoren

Figure 4. Compromised assets by percent of breaches involving Intellectual Property theft*

Type	Category	
Database server	Servers	48%
File server	Servers	32%
Finance/Accounting staff	People	29%
Human resources staff	People	29%
Documents	Offline Data	28%
Regular employee/end-user	People	28%
Web/application server	Servers	25%
Mail server	Servers	12%
Directory server (LDAP, AD)	Servers	6%
Executive/Upper Management	People	6%
Desktop/Workstation	User Devices	5%

*Assets involved in less than 1% of breaches are not shown

Verizon intellectual Property Theft – Data Breach Investigation Report
http://www.verizonenterprise.com/solutions/security/

trivadis makes IT easier.

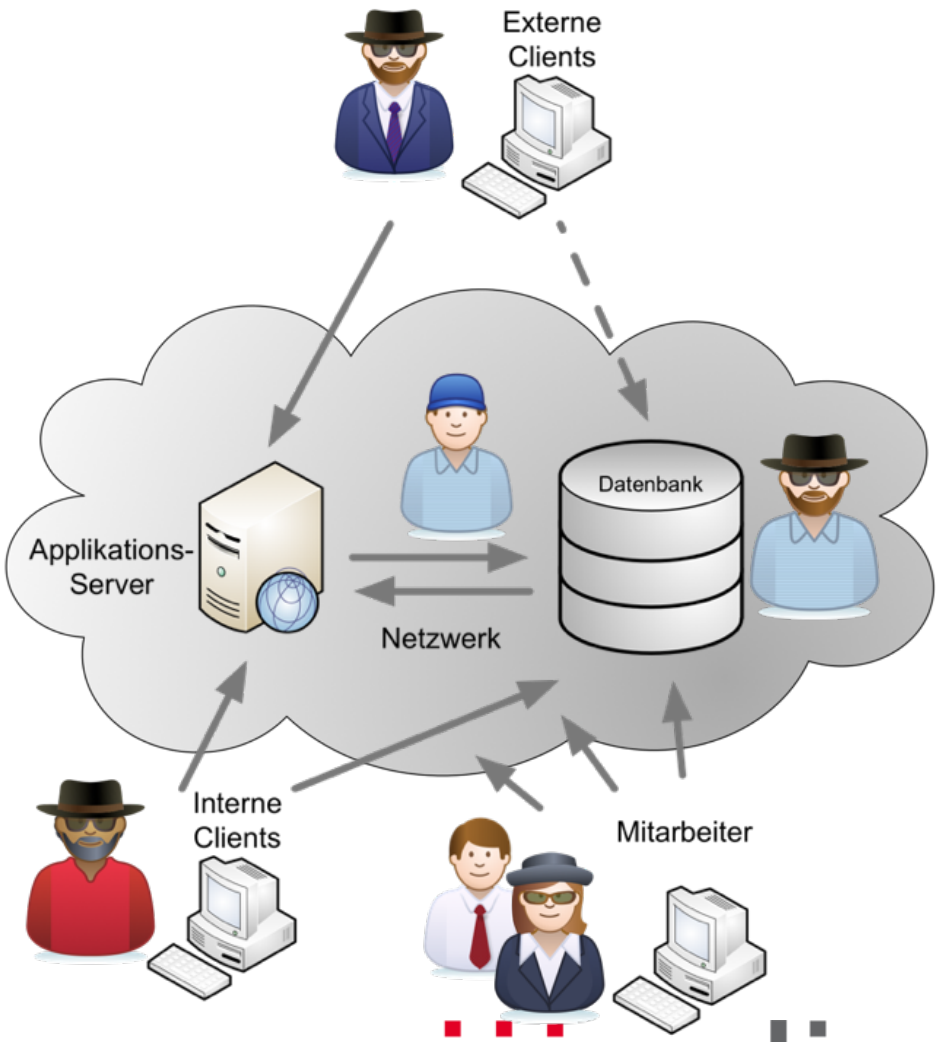
Angriffsvektoren – Top 10 - Gefahren für Datenbanken

1. Exzessive und nicht benötigte Userberechtigungen
2. Missbrauch von Rechten
3. Input Injection / SQL Injection
4. Malware
5. Schwaches Audit
6. Offenlegung / Zugang zum Speichermedium
7. Schwachstellen und Fehlkonfiguration
8. Nicht überwachte sensitive Daten
9. Denial of Service
10. Unzureichendes Sicherheitsfachwissen / Schulung

trivadis
makes IT easier.

Angriffsvektoren

- Web / Applikation / DB Server
  - Schwachstellen
  - Authentifizierung
  - Autorisierung
- Interne / Externe Clients
  - Infiziert (Malware)
  - Eingenommen (Hacked / Botnet)
- Netzwerk / Server / Storage / Cloud
  - Abhören
  - Modifizieren
- Mitarbeiter
  - Spionage
  - Unwissenheit



trivadis
makes IT easier.

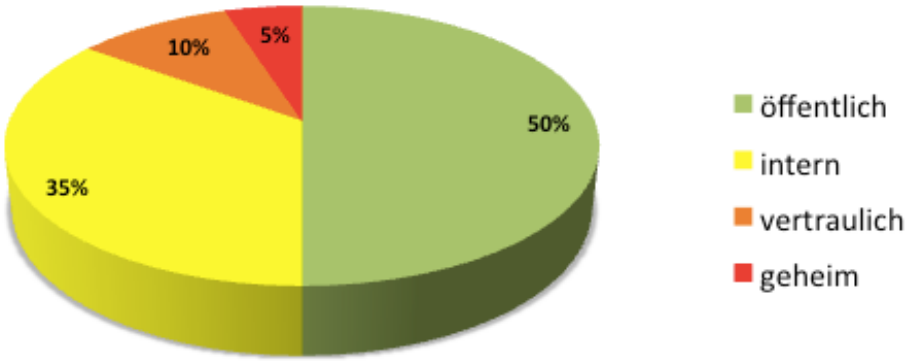
Was brauche ich?

- Oracle bietet innerhalb der Datenbank diverse Features, um die Datensicherheit zu gewährleisten. Als zusätzliche Option oder Teil der Enterprise Edition
  - EUS, VPD, ASO, TDE, DBV, AVDF, ... ☺
- Außerdem gibt es von Oracle weitere, externe Produkte
- Und natürlich auch Lösungen von Drittthersteller...
- Zusätzliche Massnahmen führen zwangsläufig immer zu Mehrkosten
  - Implementierungs- und Betriebskosten
  - Lizenzkosten
- Was brauche ich davon aber in meiner Datenbank?
- Und wenn ich viele (unterschiedliche) Datenbanken habe?

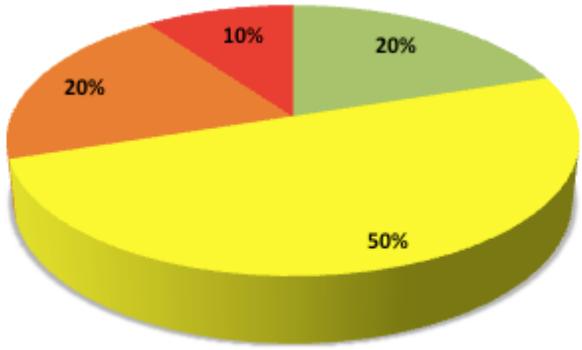
trivadis
makes IT easier.

Einleitung – Fragen

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

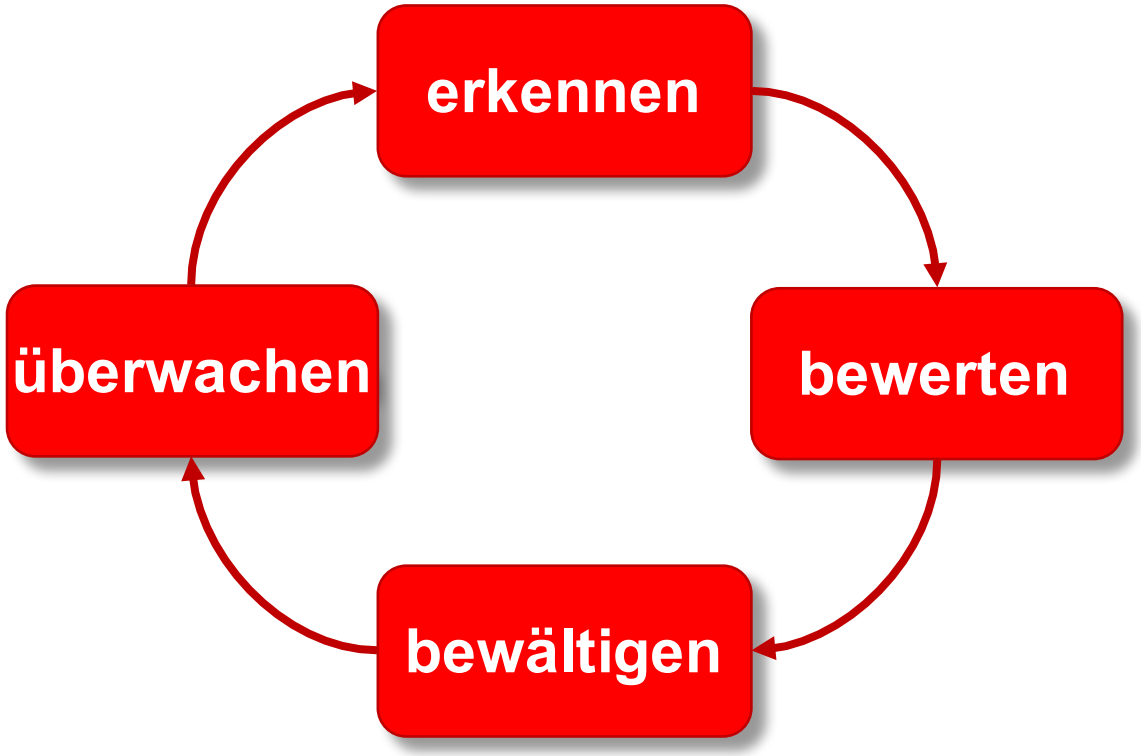


- oder eher so?



trivadis makes IT easier.

Risikomanagement



Grundstrategien der Risikosteuerung:

- Risikovermeidung
- Risikoverminderung
- Risikobegrenzung
- Risikoüberwälzung
- Risikoakzeptanz

trivadis makes IT easier.

Risikoanalyse und Bewertung

trivadis
makes IT easier.

Risikoanalyse

- Gefahren und Risiken für ein bestimmtes Umfeld müssen Bekannt sein
  - On Premise vs. Cloud
  - Überschneidung mit den Themen Disaster Recovery und Hochverfügbarkeit
  - Katalog der Risiken und Gefahren
- Besitzer der Daten bzw. der Applikation muss die Sensitivität seiner Daten definieren
  - uns somit die Konsequenzen für deren Schutz
- Das ist nicht immer ganz einfach, da jeder davon ausgeht, seine Daten sind die wichtigsten, kritischsten, ...

trivadis
makes IT easier.

Risikoanalyse

Korrekte und angepasste Risikoanalyse

trivadis makes IT easier.

Risikoanalyse

- Mehrere Ansätze
  - Katalog der Risiken und Gefahren mit Bewertung und Lösungsmethoden zur Bewältigung der Risiken
  - First Cut 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

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

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)	☐	☒	☐	

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
		☐ ☐ ☐ 1t
		☐ ☐ ☐ 3t
		☐ ☐ ☐ 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) ▪ .....

trivadis makes IT easier.

Risikomatrix

Zugang zum Speichermedium		Art der Eintretens Wahrscheinlichkeit				
		häufig	regel-mässig	gelegent-lich	selten	unwahr-scheinlich
Art der Konsequenz	Katastrophal	E	E	H	H	M
	Kritisch	E	H	H	M	S
	Marginal	H	M	M	S	S
	Vernachlässigbar	M	S	S	S	S
Aussage	Dritte haben direkten Zugang / Zugriff zum Speichermedium					
Erkenntnis	Direkte Manipulation und/oder Abzug der Daten möglich					
Konsequenzen	Verschlüsselung der Daten at Rest Einschränkung und Überwachung des Zugriffes auf OS Ebende					

1

trivadis makes IT easier.

Klassifizierung

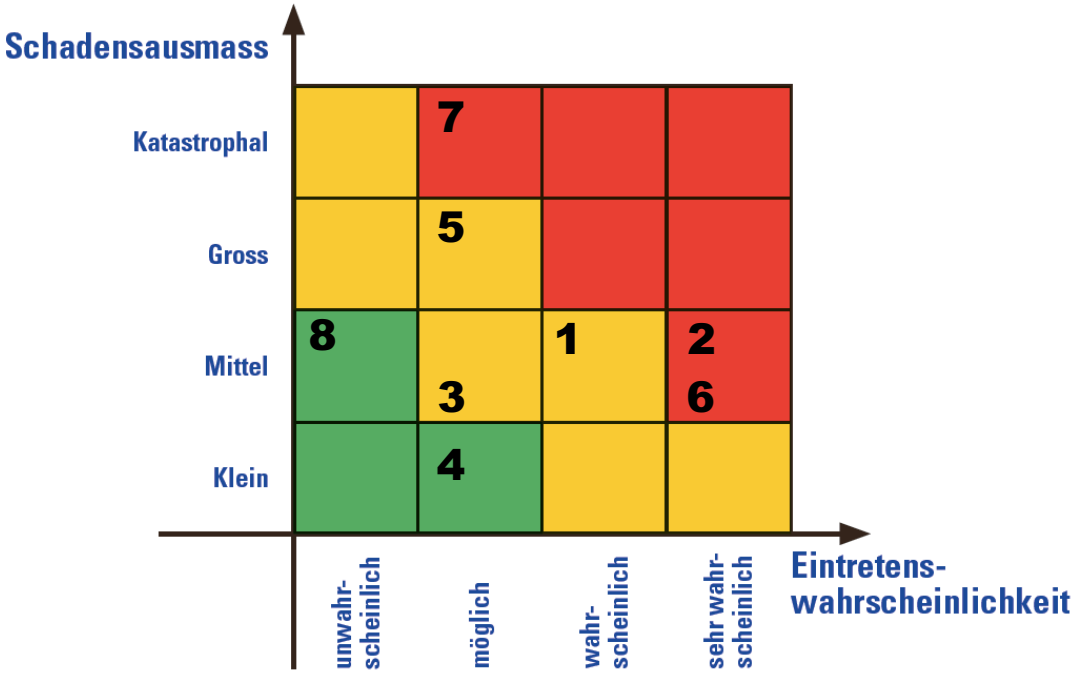
- Durch die Risikoanalyse erfolgt die Einteilung der Daten(-banken) in Sicherheitsklassen
- Typischerweise benutzt man folgende Klassen:
  - Öffentlich (Daten sind z.B. im Internet sichtbar – dürfen dort aber sicherlich nicht manipuliert werden)
  - Intern (Daten dürfen von allen Mitarbeitern gesehen 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)

trivadis
makes IT easier.

Risikomatrix und Schutzklassen

trivadis
makes IT easier.

Risikomatrix – Applikation XYZ

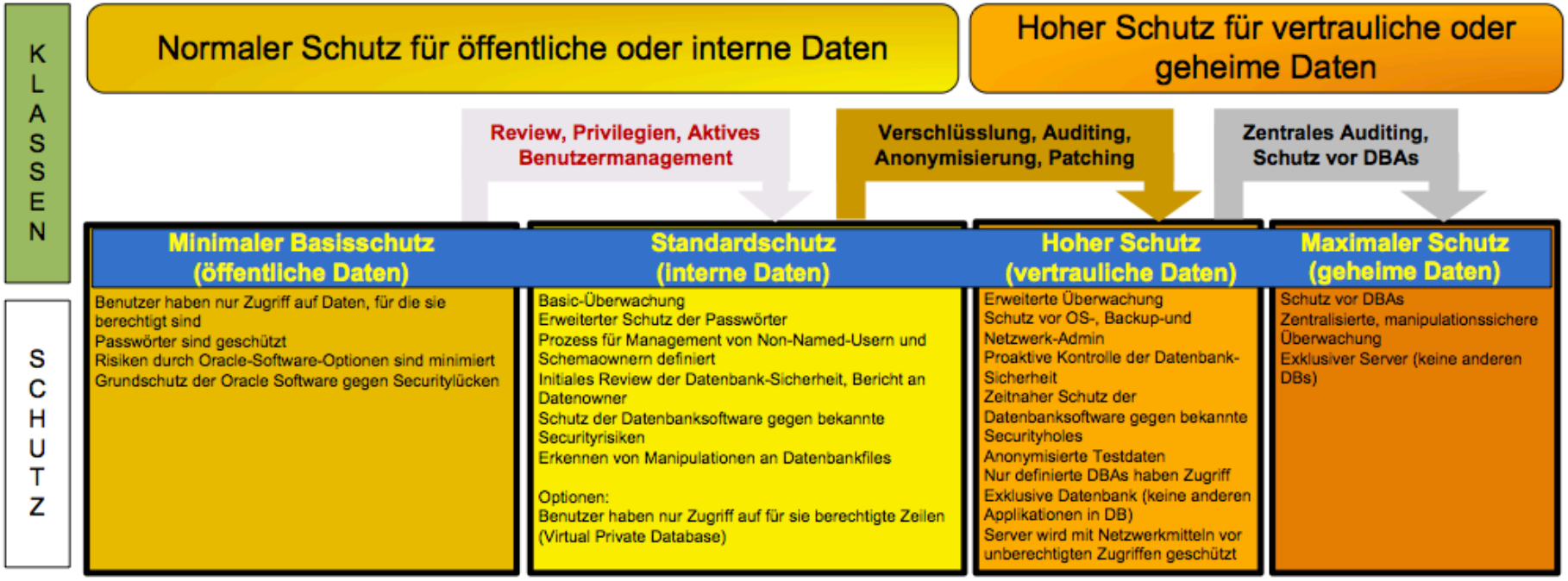


1. Exzessive und nicht benötigte Userberechtigungen
2. Missbrauch von Rechten
3. Input Injection / SQL Injection
4. Malware
5. Offenlegung / Zugang zum Speichermedium
6. Schwachstellen und Fehlkonfiguration
7. Nicht überwachte sensitive Daten
8. Denial of Service

trivadis makes IT easier.

Schutzklassen (1)

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



trivadis
makes IT easier.

Schutzklassen (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)	

trivadis makes IT easier.

Schutzklassen (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

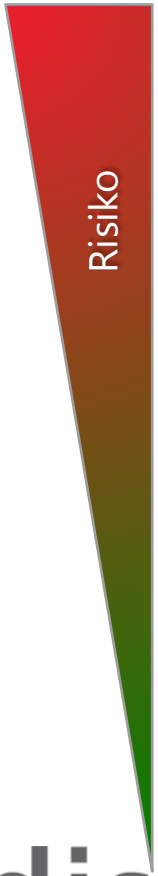
trivadis makes IT easier.

Risikoverminderung

trivadis
makes IT easier.

Authentifizierung

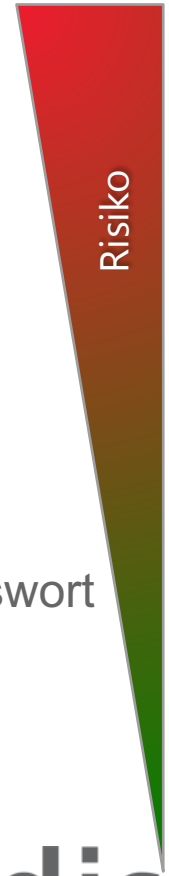
- Benutzer melden sich mit nur einem Sammelbenutzer an
- Jeder Benutzer hat seinen eigenen, persönlichen Benutzer
  - Sowohl in der Datenbank als auch auf OS Ebene
- Es existiert eine zentrale Benutzerverwaltung
  - Verwaltung in einem zentralen Verzeichnis
  - Anmeldung über dieses Verzeichnis
    - 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!**



trivadis
makes IT easier.

Passwörter

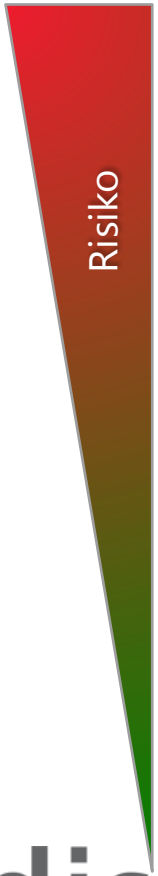
- Es existieren keine Passwortregeln
- Passwörter unterliegen Komplexitätsregeln
  - Minimale Länge
  - Benutzer von numerischen Zeichen, Sonderzeichen, ...
  - Keine gebräuchlichen Wörter
- **Alle** Passwörter müssen regelmäßig geändert werden
  - Dürfen nicht wiederbenutzt werden
  - Müssen sich auf 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



trivadis
makes IT easier.

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)



trivadis
makes IT easier.

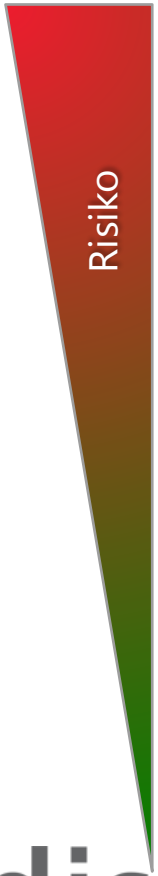
Datenzugriff - Bemerkungen

- 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

trivadis makes IT easier.

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



trivadis
makes IT easier.

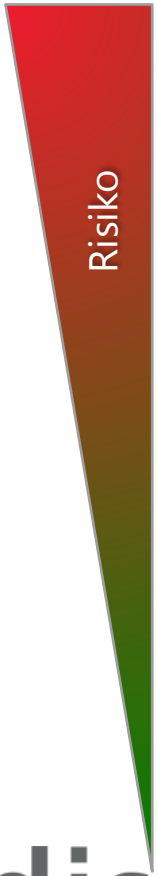
Auditing - Bemerkung

- 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

trivadis
makes IT easier.

Patching

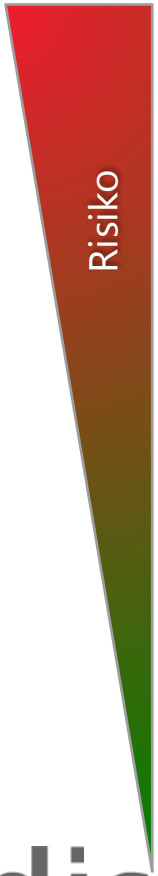
- Kein Einspielen von Security-Paches und Patch-Sets
- Regelmäßiges Einspielen der Patch-Sets (11.2.0.**3**)
- Regelmäßiges Einspielen von CPUs oder PSUs
- Zeitnahes Einspielen jedes CPUs bzw. PSUs
  - Z.B. max. ein Monat nach Erscheinen des CPUs
- Virtuelles Patching
  - McAfee Database Activity Monitoring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



trivadis
makes IT easier.

Oracle Software & Optionen

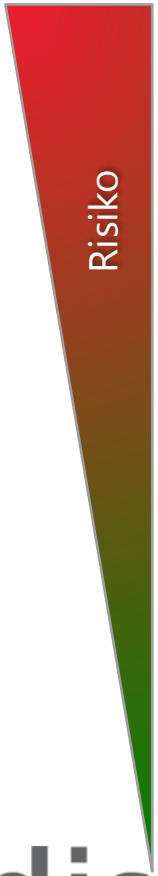
- Beliebige Software und Optionen sind installiert
- Nur benötigte Optionen sind in der Datenbank installiert
  - Kritsch z.B. Java, XDB, ...
- Nur benötige Software ist im Oracle Home installiert
- Die benötigten Optionen werden gehärtet
  - Keine Grants an Public (wie es standardmäßig häufig der Fall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



trivadis
makes IT easier.

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**



trivadis
makes IT easier.

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

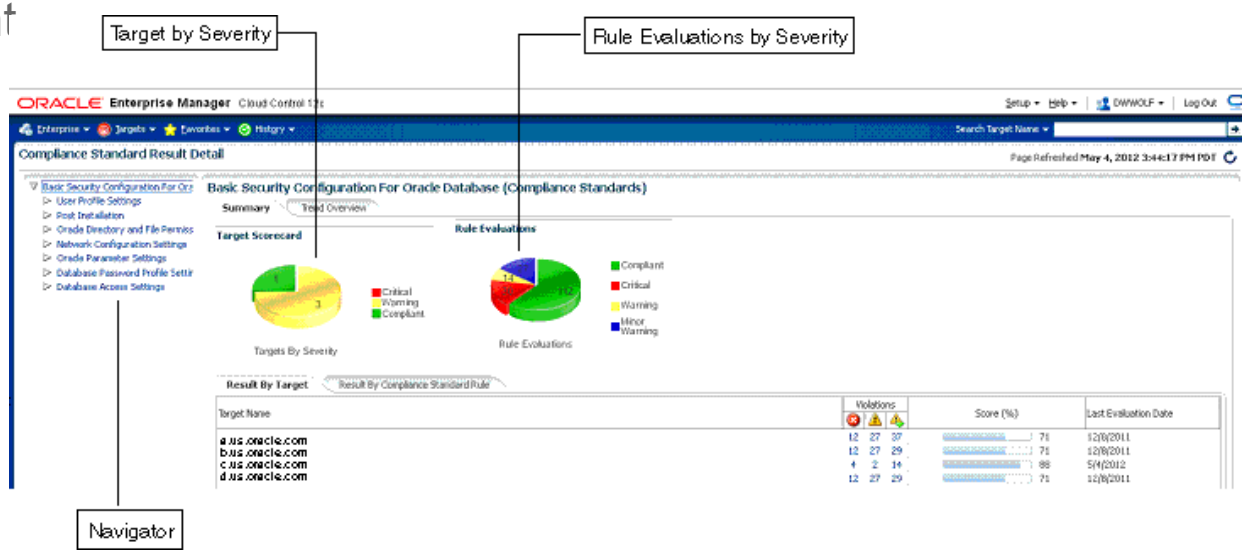
trivadis
makes IT easier.

Überprüfung

trivadis
makes IT easier.

Überprüfung der Massnahmen

- Die Einhaltung dieser Massnahmen sind regelmässig und möglichst automatisch zu überprüfen
- Verwendung von Oracle Enterprise Manager Cloud Control
  - Configuration Management
  - Compliance Framework
- Unterschiedliche Tools von Drittherstellern



trivadis makes IT easier.

Überprüfen dieser Massnahmen

- 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.

trivadis makes IT easier.

Fazit

- Security muss ganzheitlich an vielen Stellen durchgesetzt werden.
- Es ist wichtig zu wissen, was ich brauche.
  - Was ist möglich vs wieviel ist nötig
- Aber wir unterstützen Sie gern

trivadis makes IT easier.

Stefan Oehrli
Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55
stefan.oehrli@trivadis.com

http://www.trivadis.com/security
http://www.oradba.ch

trivadis
makes IT easier.