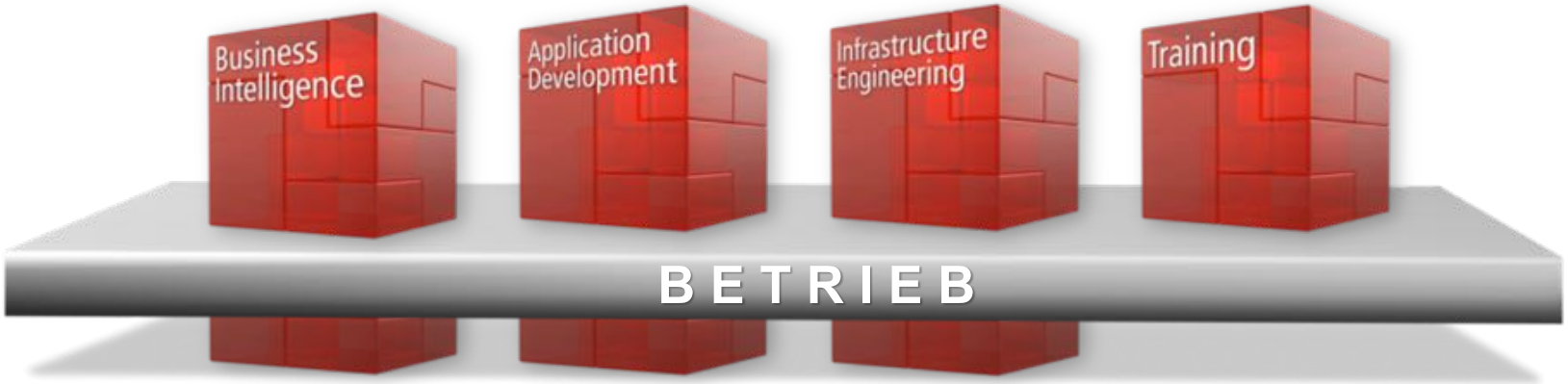
Oracle Datenbank Sicherheitsfeatures

Datensicherheits-Features im Fokus aktueller Datenschutzgesetze

Stefan Oehrli, Christian Golz

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.

Technik allein bringt Sie nicht weiter.

Man muss wissen, wie man sie richtig nutzt.

trivadis
makes IT easier.

Agenda

1. **Registrierung und Begrüssung**
2. **Willkommen bei der Trivadis**
3. **EU-Datenschutz-Grundverordnung**
   - Digitalisierung
   - Überblick zur EU DSGVO / GDPR
   - Konsequenzen für Unternehmen
4. **Kaffeepause**
5. **Oracle Datenbank Sicherheitsfeatures**
   - Risiko Analyse und Kategorisierung
   - Risiko Minimierung
   - Oracle 12c Release 2 Datenbank Sicherheitsfeatures (Auswahl)
   - Datenbank Sicherheitsfeature und GDPR / DSGVO
6. **Q&A mit anschliessendem Apéro**

trivadis makes IT easier.

EU-Datenschutz-Grundverordnung

DSGVO / GDPR – Überblick

Christian Golz

Christian Golz

Senior Consultant – IT-Security

- Since 2002 Working in the IT sector
- Since 2009 Active in IT infrstructure
- Since 2014 Increasingly in IT security
- Since 2017 Specialization Cloud Security
- Since 2017 Data Protection Officer for Trivadis GmbH

IT Experience

- IT-Infrastructure concepts & implementation for On-Premise
- Security-Reviews for On-Premise IT-Infrastructures

Special Subjects

- Security Concepts for Cloud- & On-Premise Infrastructures
- Security Reviews
- Data Protection

Skills

- Requirements Engineering
- Concepts & Reviews
- Project Management

trivadis makes IT easier.

Agenda

1. **Digitalisierung**

2. **Überblick zur EU DSGVO / GDPR**
   - Geltungsbereich
   - Ausnahmen
   - Ziel der EU GDPR / DSGVO
   - Definition „personenbezogene Daten“
   - Rechte der Betroffenen
   - Verschärfung
   - Privacy by Design

3. **Konsequenzen für Unternehmen**

trivadis makes IT easier.

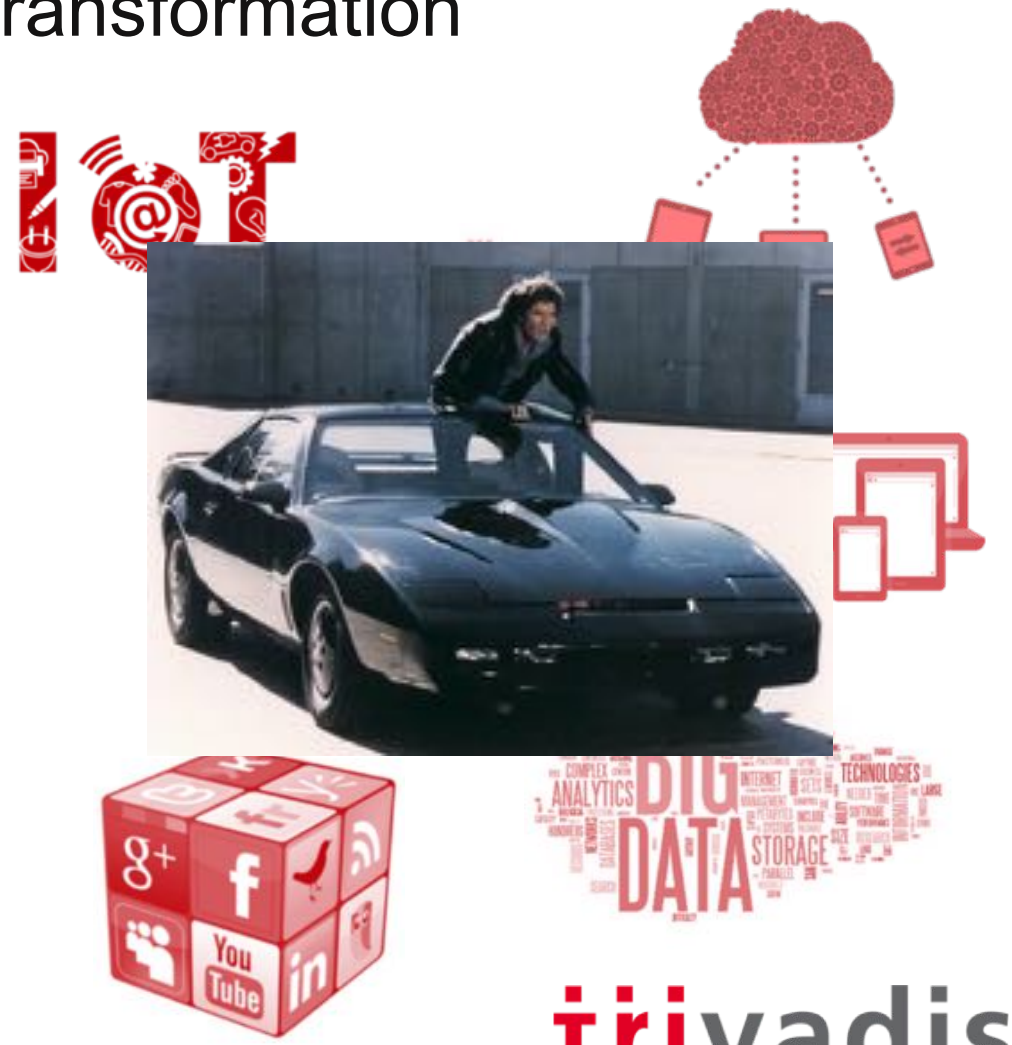
Digitalisierung

trivadis
makes IT easier.

Digitalisierung … Digitale Transformation

- Neue Technologien
- Business- und User-getrieben
- Digitalisierung forciert kürzere Markdurchdringungszeiten
- Neue Chancen und Risiken
  - Technisch, Sozial, Business, Rechtlich, Politisch …

Kodak



Picture source:www.fhnw.ch, opencliparts.org, lenovo.com

trivadis makes IT easier.

Digitalisierung … Datensicherheit

- Digitalisierung beruht auf Daten
- Daten sind …
  - In Bewegung
  - Verarbeitet von multiplen Systemen
  - Liegen in unterschiedlichen Bereichen – redundant
  - Überschreiten Firmen-, Landes- und Kontinentalgrenzen

Die Zukunft gehört den Daten = Gold des digitalen Zeitalters

trivadis makes IT easier.

Digitalisierung … Datensicherheit

Daten = Gold des digitalen Zeitalters

- Interessant für Hacker
- Erhöhte Berichterstattung
  - Neue Wahrnehmung bei Usern, Unternehmen und staatlichen Organisationen
- Neue gesetzliche Regelungen
  - Privacy Shield
  - EU GDPR / DSGVO

trivadis makes IT easier.

EU GDPR / DSGVO
Überblick

trivadis makes IT easier.

Datensicherheit vs. Datenschutz

Schutz personenbezogener Daten bekommt eine hohe Wichtigkeit

- Datensicherheit:

  Technische und organisatorische Massnahmen zum Schutz von Daten vor Verfälschung, Missbrauch, Zerstörung oder unzulässiger Weitergabe

- Datenschutz:

  Technische und organisatorische Massnahmen zum Schutz von personenbezogenen Daten (EU GDPR / DSGVO)

trivadis makes IT easier.

EU GDPR / DSGVO
Geltungsbereich

trivadis
makes IT easier.

Geltungsbereich EU GDPR / DSGVO

- Niederlassungsprinzip
- Marktortprinzip, gilt für Unternehmen, die…
  - **keine** Niederlassung in der EU besitzen
  - Waren und/oder Dienstleistungen anbieten
  - Profiling durchführen

- In der Praxis macht das die DSGVO zu einem weltweitem Gesetz.

trivadis
makes IT easier.

Geltungsbereich EU GDPR / DSGVO

Daten-verantwortlicher	Daten Verarbeiter	Daten von (Ansässigkeit)	Anwendbarkeit EU-DSGVO	Grundlage
EU	EU	EU	✔	Art. 3 Abs. 1
EU	CH	EU	✔	Art. 3 Abs. 1
EU	CH	CH	✔	Art. 3 Abs. 1
CH	EU	CH	✔	Art. 3 Abs. 1
CH	-	CH	✗*	
CH	-	EU	✔	Art. 3 Abs. 2

(*) vorbehältlich, dass Waren oder Dienstleistungen an in der EU ansässige Personen angeboten werden oder ein Verhalten beobachtet wird

trivadis makes IT easier.

EU GDPR / DSGVO
Ausnahmen

trivadis
makes IT easier.

Ausnahmen für EU GDPR / DSGVO

Unternehmen weniger als 250 Mitarbeiter beschäftigt…

- … es sei denn:
  - Verarbeitung birgt hohes Risiko für Rechte und Freiheiten der betroffenen Person
  - Verarbeitung erfolgt nicht nur gelegentlich
  - Verarbeitung bezieht sich auf besondere Kategorien personenbezogener Daten

- Beispiel:
  - Kleine Bäckerei, Handwerker, Fleischerei jeweils ohne Webshop

trivadis
makes IT easier.

EU GDPR / DSGVO

Ziele

trivadis makes IT easier.

EU GDPR / DSGVO

Wirksam ab dem **25. Mai 2018** (Art. 99 Satz 2 DSGVO) in EU

- Bis dahin müssen die Verarbeitung personenbezogener Daten und die Datenschutzprozesse umgestellt sein
- EU GDPR / DSGVO ist eine Verordnung
- Öffnungsklauseln zur Konkretisierung von Artikeln
- One-Stop-Shop – eine Aufsichtsbehörde je Mitgliedsstaat

Ziel der EU GDPR / DSGVO

- Schaffung eines einheitlichen Datenschutzniveaus in EU
- Stärkung der Rechte der Betroffenen
- Stärkere Verpflichtung der Unternehmen

- Rechtmässigkeit der Verarbeitung von personenbezogenen Daten
  - Rechenschaftspflicht
  - Transparenz
- Es sind Spielräume vorhanden

trivadis makes IT easier.

EU GDPR / DSGVO
Personenbezogene Daten

trivadis
makes IT easier.

Definition „personenbezogene Daten“

Neue, breitere Definition von **personenbezogenen Daten** (Art. 4 Abs. 1)

- Alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen
- Insbesondere mittels Zuordnung
  - Zum Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung
  - Zu besonderen Merkmalen: „Ausdruck der physischen, physiologischen, **genetischen**, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität“

trivadis makes IT easier.

Definition „personenbezogene Daten“

Beispiel:

- Tom Cruise
- David Hasselhoff
- Donald Trump
- «Madonna» Louise Veronica Ciccone

trivadis makes IT easier.

Definition „personenbezogene Daten“

Personenbezogene Daten

Geboren: 19.03.1955

In Idar Oberstein, Deutschland

Männlich

Der Älteste von 3 Geschwistern

Ist Vater von 5 Töchtern

Heutige Jobs: Sänger
Produzent
Schauspieler

Wohnort: Carneys Point Township, New Jersey, U.S.

Verheiratet mit: Emma Heming

Erster Vorname: Walter

Besondere Kategorien personenbezogener Daten

trivadis makes IT easier.

Rechte der Betroffenen

- Recht auf Auskunft
  - Recht auf Überlassung einer Kopie
- Recht auf Berichtigung
- Recht zur Löschung (Vergessenwerden)
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
  - Automatisierte Entscheidungen
- Recht auf Einschränkung der Verarbeitung
- Recht auf Berichtigung
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung

EU GDPR / DSGVO
Verschärfungen

trivadis
makes IT easier.

Bisherige Situation

- Keine Beweispflicht für Unternehmen, dass Sie das Thema Datenschutz im Griff haben
- Eintrittswahrscheinlichkeit zur Verfolgung von Sicherheitsvorfälle gering
- Geringe Strafen max. 300,000 € in DE und max. 10,000 CHF in CH

«Wo kein Kläger, da kein Richter»

trivadis makes IT easier.

Verschärfung

Bisherige Praxis:

- Inkaufnahme von Datenschutzverstößen soll sich nicht mehr lohnen

Neu: Geldbuße droht bei

- technisch-organisatorischen Verstößen gegen Vorgaben der EU GDPR/DSGVO
- Verstößen gegen die Pflicht zu datenschutzfreundlicher Technikgestaltung oder datenschutzfreundlichen Voreinstellungen
- Deutlich erhöhte Bussgeldrahmen gegen Verantwortliche oder Auftragsverarbeiter

trivadis makes IT easier.

Verschärfung

- Jede Aufsichtsbehörde stellt sicher, dass Geldbusse in jedem Einzelfall **wirksam**, **verhältnismäßig** und **abschreckend** ist (Art 83. Abs. 1)

- Kleine Verstöße:
  - Bis zu **10 Mio. €** oder bis zu 2% des weltweiten Vorjahresumsatzes (Art. 83 Abs. 4), je nachdem welcher der Beträge höher ist

- Größere Verstöße:
  - Bis zu **20 Mio. €** oder bis zu 4% des weltweiten Vorjahresumsatzes (Art. 83 Abs. 5 & Abs. 6), je nachdem welcher der Beträge höher ist

trivadis makes IT easier.

Verschärfung

- Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen (2%)
- Melde- und Benachrichtigungspflicht bei Datenschutzverletzungen (72h) (2%)
- Verzeichnis von Verarbeitungstätigkeiten (Verfahrensverzeichnis) (2%)
- Risikoanalyse (2%)
- Fehlende Datenschutzfolgeabschätzung (2%)
- Verweigerung der Bestellung eines DSB bei Pflicht (2%)
- …

trivadis makes IT easier.

Verschärfung

- Nicht Einhaltung der Weisungen von Aufsichtsbehörden (4%)
- Nachweis des Verantwortlichen das alle Datenschutzgrundsätze eingehalten wurden (4%)
  - Auch Datenverarbeiter (4%)
- Informierung des Betroffenen ob und wie seine Daten verarbeitet werden (4%)
- Informationspflicht bei Datenerhebung bei Dritten (4%)
- …

trivadis makes IT easier.

EU GDPR / DSGVO
Privacy by Design

trivadis
makes IT easier.

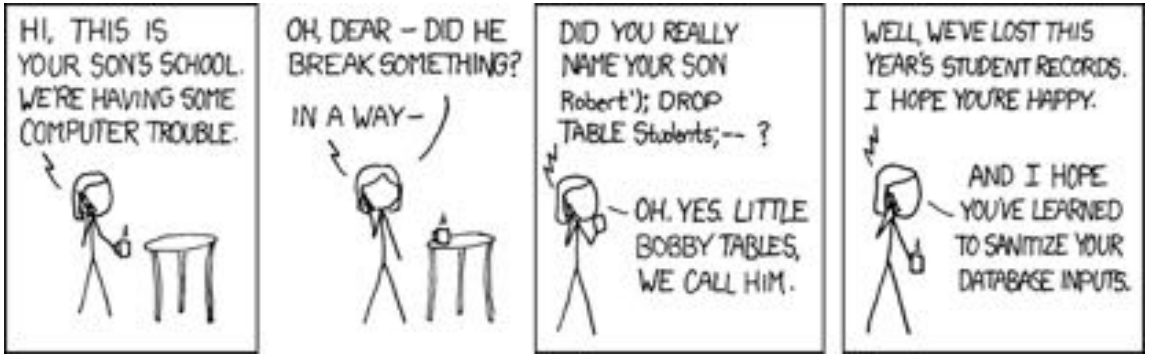
Privacy by Design

Datenschutz durch

- Datenschutzfreundliche Technikgestaltung
- Datenschutzfreundliche Voreinstellungen (Art. 25)

- Datenschutzfördernde Technologien und datenschutzfreundliche Voreinstellungen zur Verarbeitung personenbezogener Daten sollen bereits in der Design-Phase berücksichtigt werden, z.B.
  - Pseudonymisierung der Daten, Datenminimierung, Speicherfrist, Zugänglichkeit
  - Zertifizierung soll Erreichung der Privacy by Design-Ziele gewährleisten

Privacy by Design



- Sichere Programmierung
  - Ist die Applikation sicher?
  - Best Practice Umsetzung?
  - Review des Codes / Anwendung
- Ausweisung und Dokumentation der sensitiven Daten
- Anonymisierung und Maskierung der sensitiven Daten
  - In der Produktion z.B. Kreditkarten
  - Anonymisierung von Test und Entwicklungsdaten

trivadis makes IT easier.

Konsequenzen für Unternehmen

trivadis makes IT easier.

Konsequenzen für Unternehmen

- Digitalisierung = schneller Wandel auch für Datensicherheit
- Daten bekommen eine hohe Wertigkeit, die es zu schützen gilt
- Neue Risiken fordern uns heraus (nicht nur technische)
- Einhaltung der EU GDPR / DSGVO für fast alle Unternehmen erforderlich

- EU GDPR / DSGVO bringt Veränderung, die als Chance zu nutzen ist

Seien Sie Vorbereitet - Seien Sie Pro-Aktiv

trivadis makes IT easier.

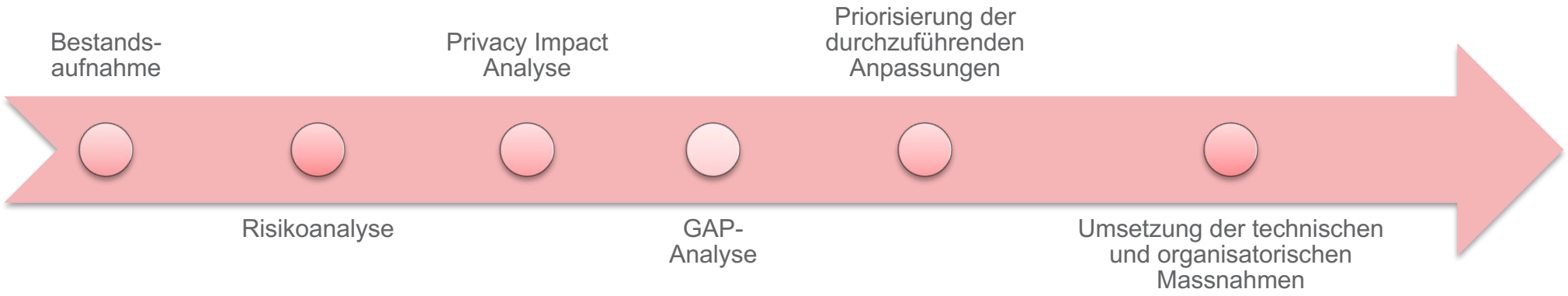
Konsequenzen für Unternehmen

Wir unterstützen Sie gerne:

- Bei Security Reviews und Risk Assessments
- Bei der Erstellung von Sicherheitskonzepten und bei deren Umsetzung
- Bei der ganzheitlichen Beratung im Bereich Datensicherheit

trivadis makes IT easier.

Konsequenzen für Unternehmen



trivadis makes IT easier.

Kaffeepause

trivadis makes IT easier.

Oracle Datenbank Sicherheitsfeatures

Technische-Organisatorische Massnahmen

Stefan Oehrli

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
- Oracle AVDF und DB Vault
- Oracle Directory Services
- Team / Projekt Management

trivadis
makes IT easier.

Agenda

1. Überblick
2. Risiko Analyse und Kategorisierung
3. Risiko Minimierung
4. Oracle 12c Release 2 Datenbank Sicherheitsfeatures (Auswahl)
5. Datenbank Sicherheitsfeature und GDPR / DSGVO
6. Fazit

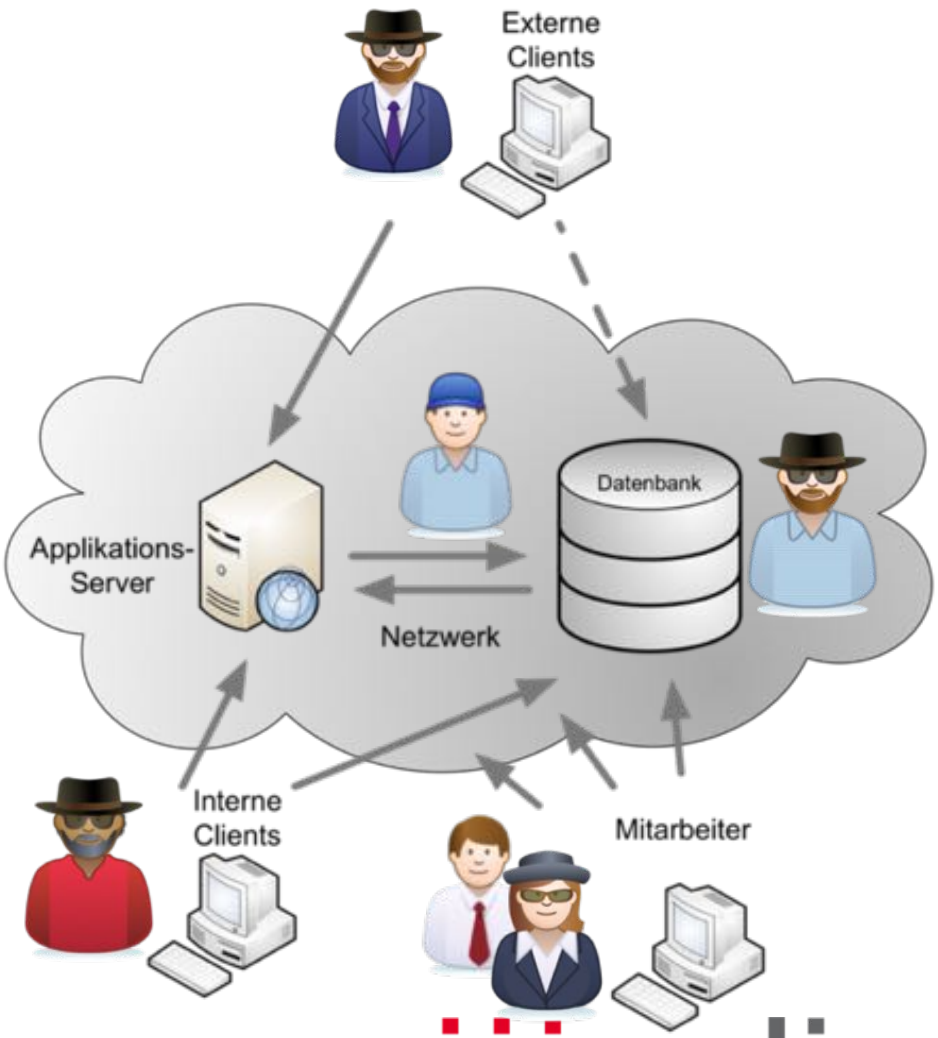
trivadis makes IT easier.

Überblick

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



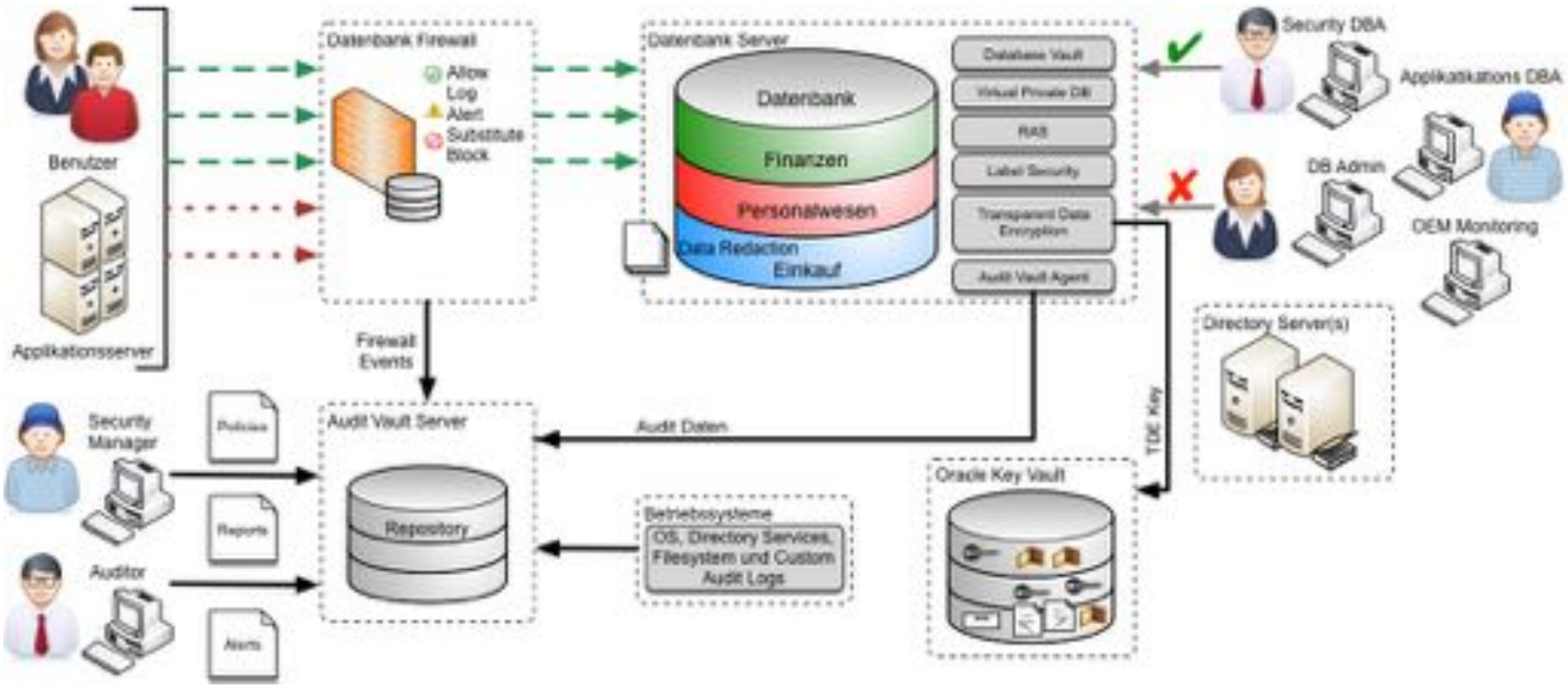
trivadis
makes IT easier.

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.

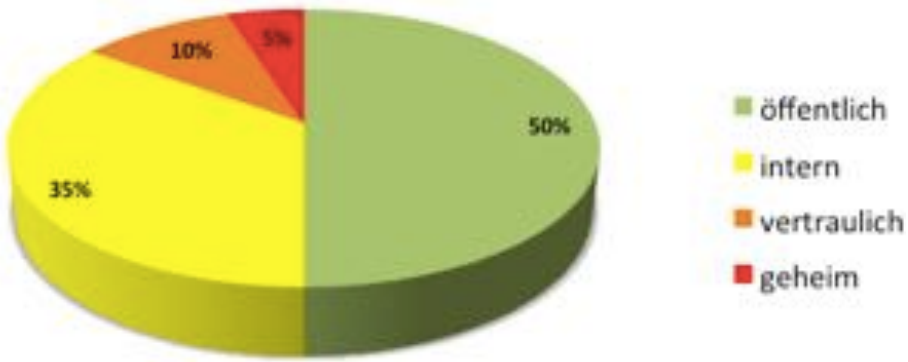
Maximale Datensicherheit Architektur



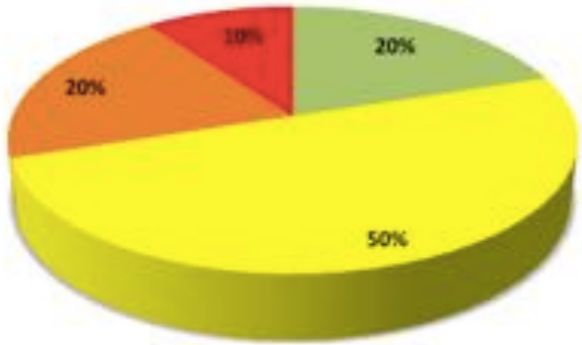
trivadis makes IT easier.

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.

Risiko Analyse und Kategorisierung

trivadis makes IT easier.

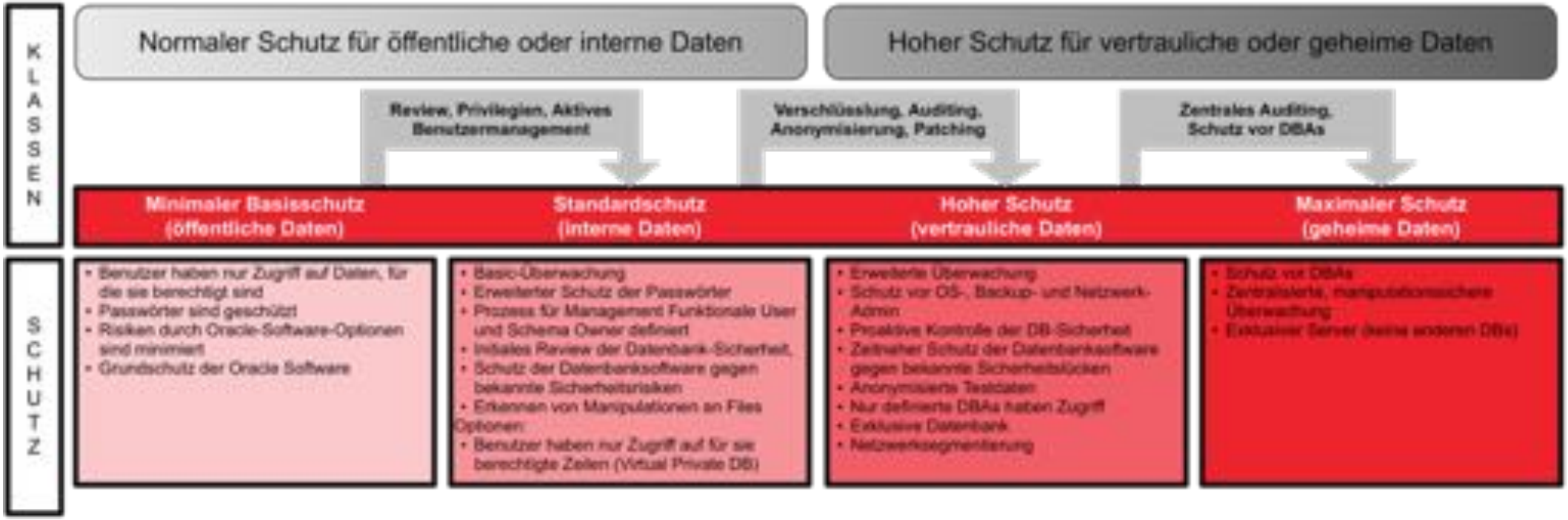
Risikoanalyse

- 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, ...

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)

Risiko Matrix (1)



trivadis makes IT easier.

Risiko Matrix (2)

MASSNAHMEN				
	• Rollenkonzept • Einfache Passwort Profile • Oracle Standardpasswörter geändert • Löschen nicht benötigter Oracle Optionen • Locken nicht interaktiv benötigter Oracle-Accounts Software	• Komplexere Passwortprofile • Definiertes Benutzer- und Rollenkonzept • Keine Shared User • Anmeldung mit Schema-Owner nur für Release-Prozess möglich (durch DBA) • Kein PUBLIC und/oder ANY-Privilegien • Public-Privilegien werden entfernt • Datenbank-Parameter gesetzt	• Verschlüsselung der Datenfiles, Backups und Netzwerks • Anonymisierung des Testsystems • Anonymisierung der Exports für Softwarelieferanten • Personalisierte Accounts für OS und DB	• Segregation of Duties • Database Vault / Appliance
	Auditing	**Auditing** • Standardauditing • Aufbewahrung: 6 Monate	**Auditing** • Erweitertes Audit auf kritische Daten • Aufbewahrung: min. 2 Jahre	• **Auditing** • Audit Vault, DB Firewall, etc. • Aufbewahrung: 7 Jahre
	Patching • Einspielen von Patch Sets max. 3 Monate nach erscheinen	**Patching** • 2x pro Jahr Einspielen von CPUs/PSUs bzw. von Patch Sets (wenn verfügbar)	**Patching** • Einspielen von CPUs/PSUs max. 1 Monat nach Erscheinen	**Patching**
	Review	**Review** • Initialer Review, Bericht über Security-relevante Parameter, ANY-Privilegien, ...	**Review** • halbjährliches Review der DB, unterstützt durch Software (z.B. Tvd-SecAudit)	**Review**
	Umgebung	**Umgebung** • Passwörter dürfen nirgendwo im Klartext sein (z.B. im Applicationserver, Scripts)	**Umgebung** • Datenbank-Server befinden sich in einer eigenen Security-Zone	**Umgebung** • Eigener, dedizierter Server ohne andere Datenbanken, Applikationen, Software, ...

trivadis makes IT easier.

Risiko Matrix (3)

KONSEQUENZEN				
	Anforderungen	**Anforderungen an Data-Owner** • Benutzer-, Rollen- und Privilegien Konzept muss zusammen mit Data-Owner definiert werden	**Anforderungen** • Kritische Tabellen müssen definiert werden	**Anforderungen** • Prozesse müssen geändert werden (z.B. Benutzer-Verwaltung liegt beim Kunden)
	Kosten • Reguläre Lizenzkosten	**Kosten** • Diskplatz (minimal)	**Kosten** • Diskplatz (mittel) • ASO: 13k • Data Masking Pack: 13k • RepView: 1k pro DB	**Kosten** • Diskplatz (hoch) • AVDF Server • Database Vault • Weitere Tools/Produkte

trivadis makes IT easier.

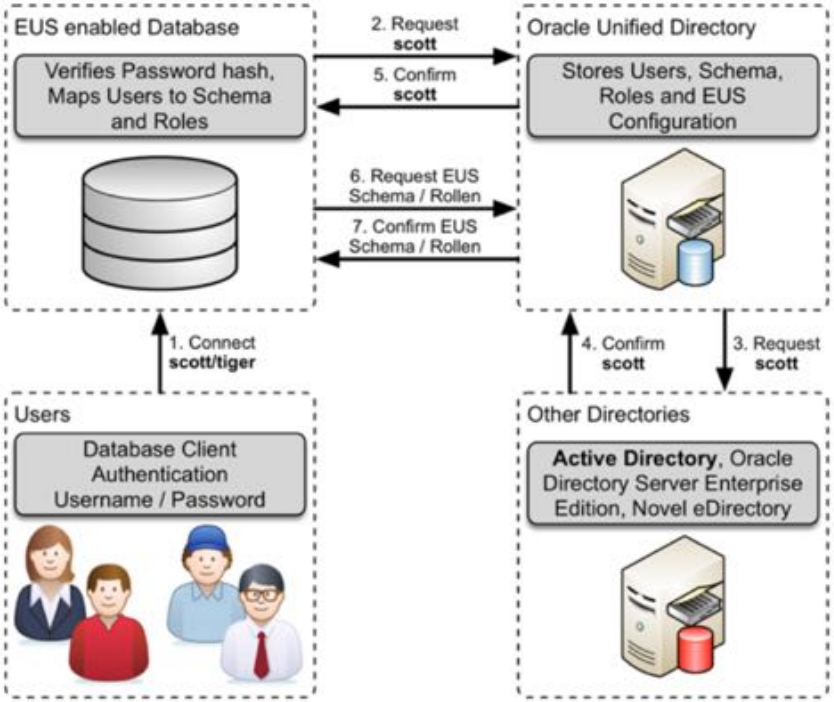
Risiko Minimierung

trivadis makes IT easier.

Authentifizierung

Risiko

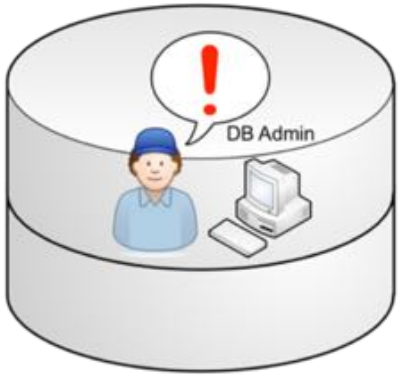
- Password Authentifizierung
  - Aktuelle Password Hashs SQLNET.ALLOWED_LOGON_VERSION_*
  - Password Profile z.B Passwort Länge
- Starke Authentifizierung
  - Kerberos Authentifizierung
  - Radius Authentifizierung
  - SSL zertifikatsbasierte Authentifizierung
- Enterprise User Security
  - Zentrales Verzeichnis der Datenbanken, Benutzer und Berechtigungen
- Identity und Access Management

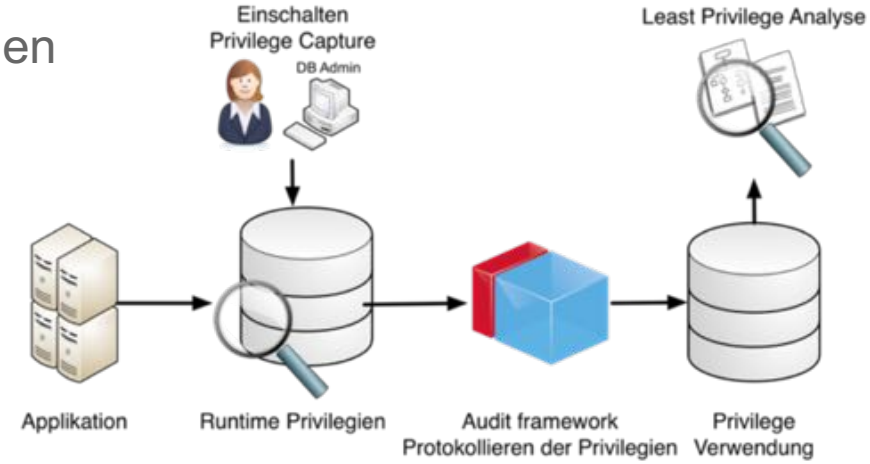


trivadis
makes IT easier.

Autorisierung

- Wie werden die Berechtigungen vergeben/verwaltet?
  - Rollen und Berechtigungskonzept
- Umgang mit kritischen Privilegien und hoch privilegierten Benutzern wie SYS, SYSDBA etc
- Analyse und Kontrolle der Berechtigungen
  - Privileg Analysis

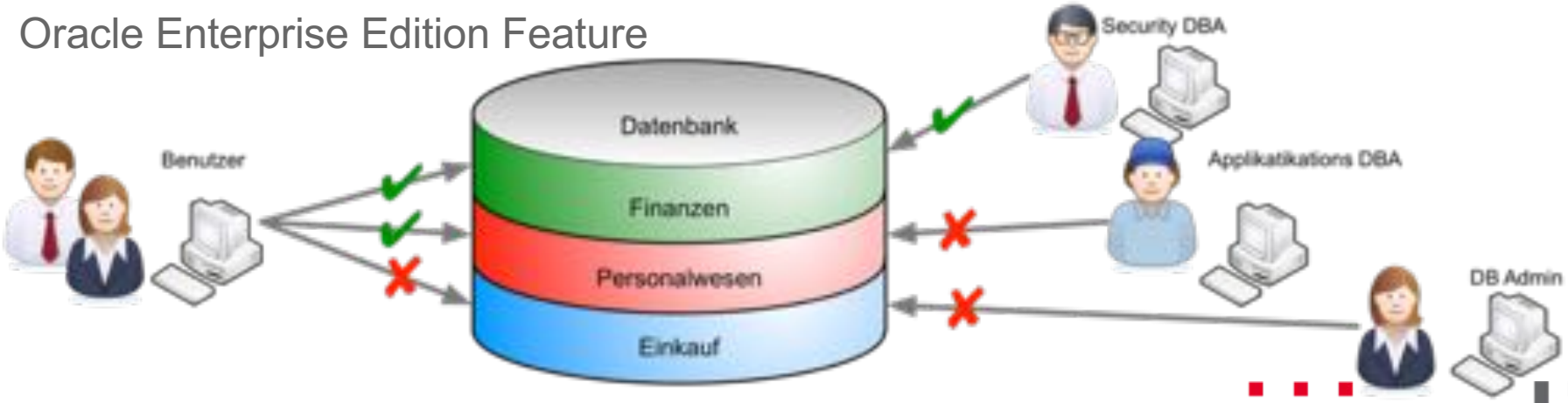




trivadis makes IT easier.

Autorisierung – Virtual Private Database

- Einschränkung der Zugriff in Abhängigkeit von Policies
  - Ein Zusatzprädikat wird bei jedem Tabellenzugriff an die WHERE Clause des Statements angehängt
  - Kann auch nur für einzelne dieser Befehle aktiviert werden
  - Für Tabellen und Views unterstützt
- Mandantenfähigkeit für einen Datenbank
- Oracle Enterprise Edition Feature



trivadis makes IT easier.

Autorisierung – Data Redaction

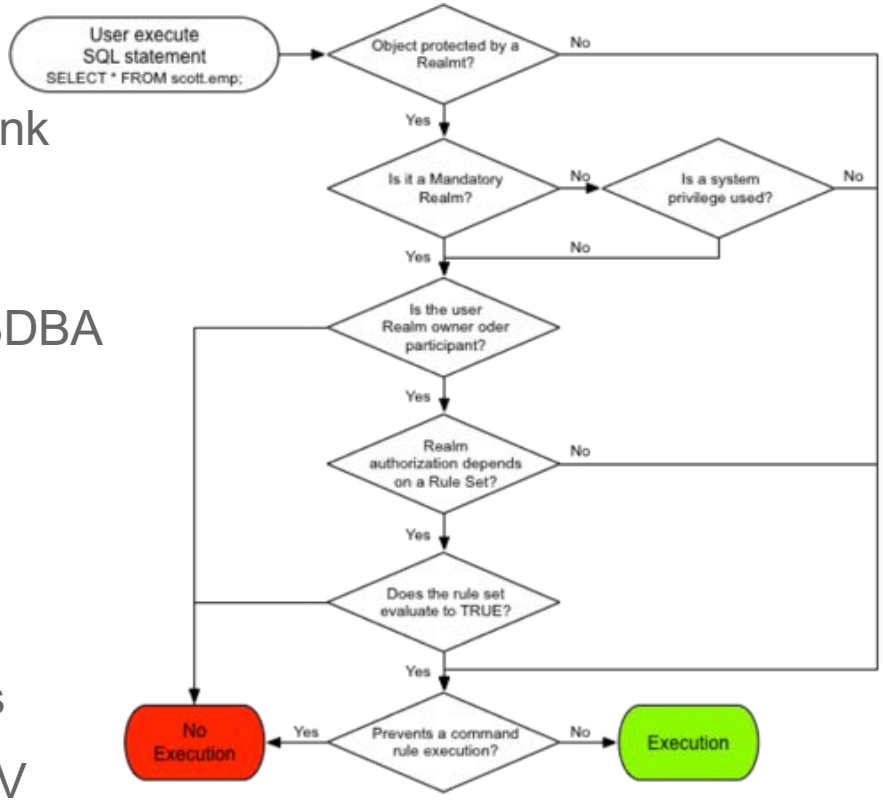
- Maskierung der Datenausgabe / Darstellung mithilfe von Policies
- Transparent für jede Anwendung
  - Zugriff mit SQLPlus oder in der Anwendung

	Original -> Redacted
☑ Random Redaction	4022-5231-5531-9855 -> 4042-6344-0547-9855 09/30/73 -> 11/30/73
☑ RegExp Redaction	94025-2450 -> 94025-[hidden] tom.lee@acme.com -> [redacted]@acme.com
☑ Partial Redaction	068-35-2299 -> ***-**-2299 D1L86YZV8K -> D1******8K
☑ Full Redaction	05/24/75 -> 01/01/01 11 Rock Bluff Dr. -> XXXXXXXXX

trivadis makes IT easier.

Autorisierung – Database Vault

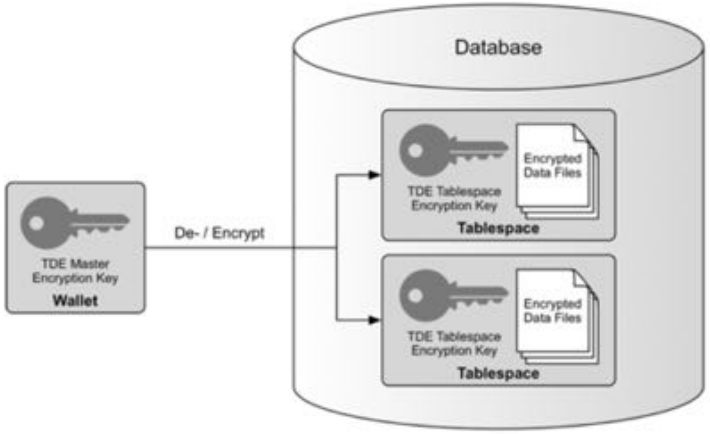
- Schützt definierbare Bereiche in der Datenbank vor beliebigen Benutzern
  - Auch vor administrativen und hoch privilegierten Benutzern wie SYS bzw. SYSDBA
- Geschützt werden nur Daten in einer Realm
  - Realms schützen Daten auf Schema oder Objekt Ebene
- Rules, Rule Sets und Command Rules zur Kontrolle / Steuerung der Zugriffe auf Realms
- Die Datenbank kann auch mit aktiviertem DBV durch SYS bzw. SYSDBA verwaltet werden



trivadis makes IT easier.

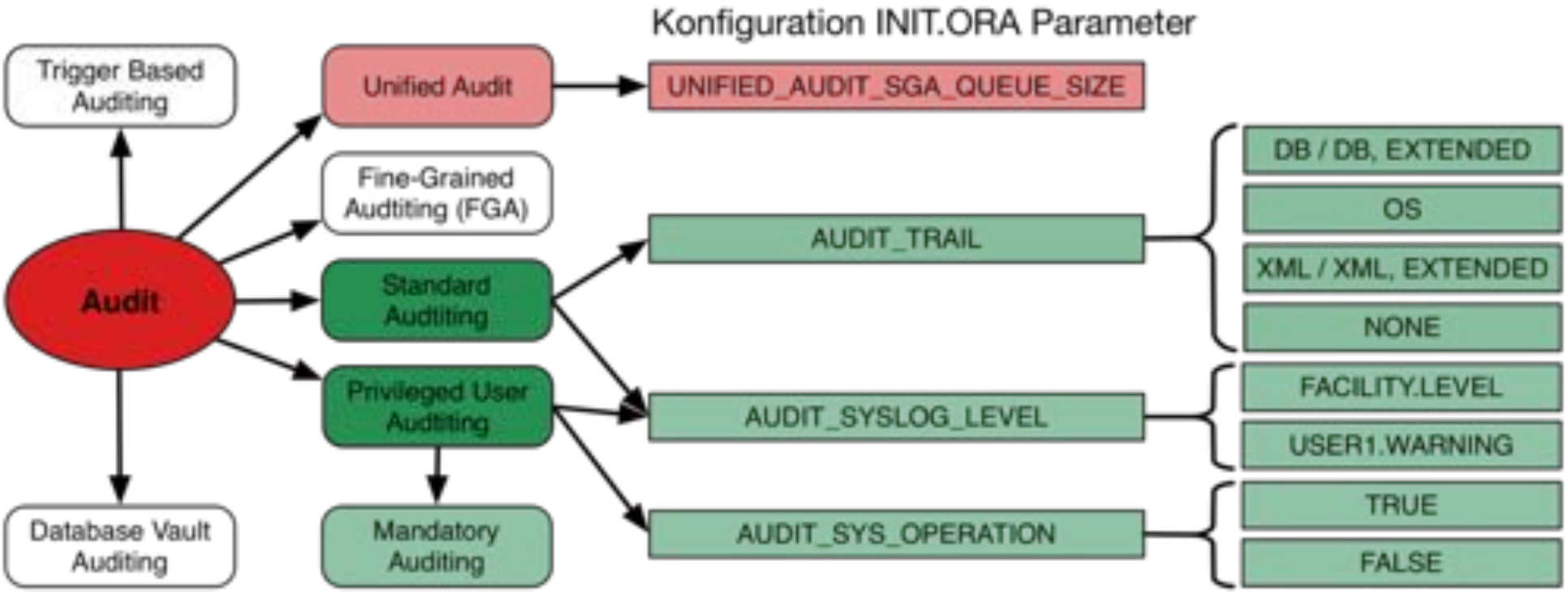
Verschlüsselung

- Verschlüsselung der Daten at REST
- Spalten Verschlüsselung
  - Verschlüsselung einzelner Spalten
  - Einschränkungen bezüglich Daten Typen, Indizes und Fremdschlüsseln
- Tablespace Verschlüsselung
  - Verschlüsselung ganzer Tablespaces
  - Daten müssen in neuen Tablespaces migriert bzw. reorganisiert werden
  - Seit Oracle 12.2 auch **live / online** Verschlüsselung der Tablespaces



trivadis makes IT easier.

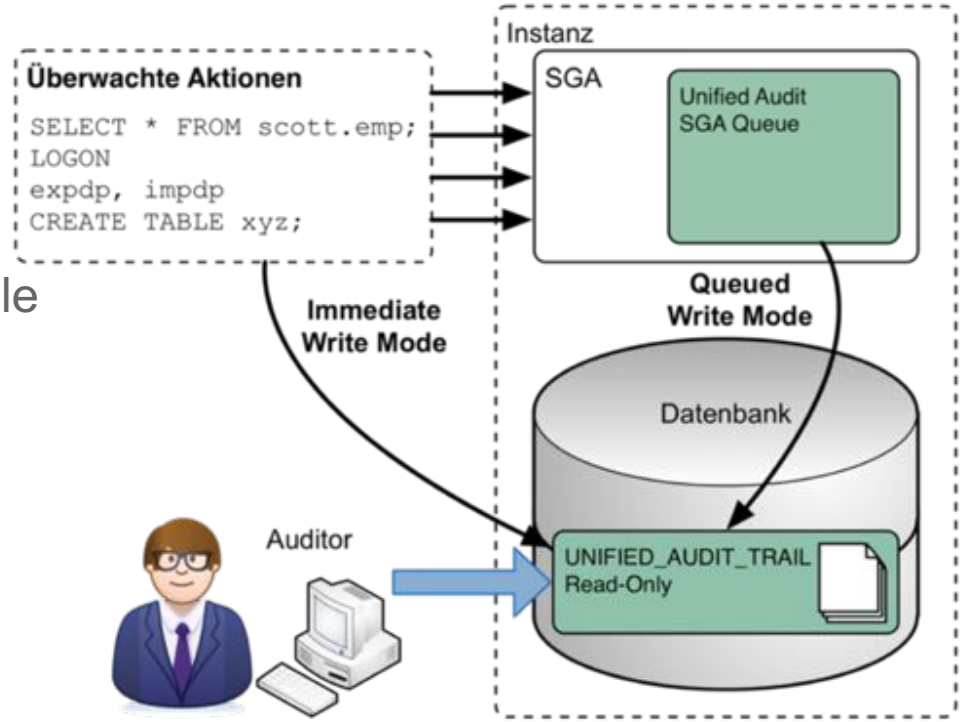
Auditing



trivadis makes IT easier.

Auditing – Unified Audit

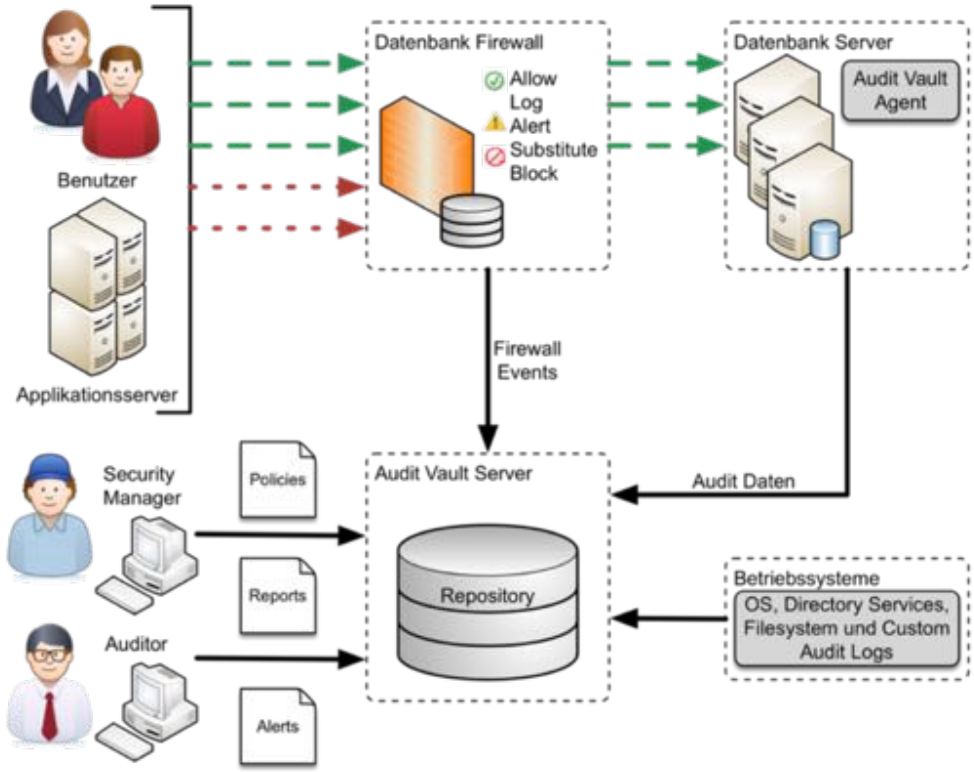
- Neuer Audit Trail seit Oracle 12c
- Zentraler / Einheitlicher Audit Trail
- Schnelle Audit Engine, einfachere Kontrolle des Zugriffes, verbesserte Performance
  - Minimale Mehrbelastung bei der Verarbeitung
  - Minimale Mehrbelastung bei Transaktionen
- Policy basiertes Auditing
  - Z.B. alles was mit der Rolle DBA gemacht wird



trivadis makes IT easier.

Auditing – Audit Vault und Database Firewall

- Zentralisierte Verwaltung, Sammlung und Auswertung der Audit werden Auditeinträge
- Klassisches Audit
- Regel basiertes Audit mit der Datenbank Firewall
- Activity Monitoring



trivadis
makes IT easier.

Oracle 12c Release 2 Datenbank Sicherheitsfeatures

trivadis makes IT easier.

Autentifizierung und Password Verifier

- Oracle Patchset 12.1.0.2 führt SHA-2 Support für 12C Password Version ein
  - Neuer zusätzlicher Password Verifier respektive Hash in spar4
- Starke Password Verifiers by Default
  - ALLOWED_LOGON_VERSION_SERVER bei Default auf 12 (war 8)
  - Bei Default werden nur 11g und 12c Password Verifier (Hash) erstellt
  - 10g Password Verifier wird nur erstellt wenn ALLOWED_LOGON_VERSION_SERVER auf 11 seht
- Higher Security geringere Kompatibilität
  - Es gibt immer noch viele Anwendungen welche nicht mit case sensitiven Passwärtern umgehen können

trivadis makes IT easier.

Automatische Sperrung von Accounts

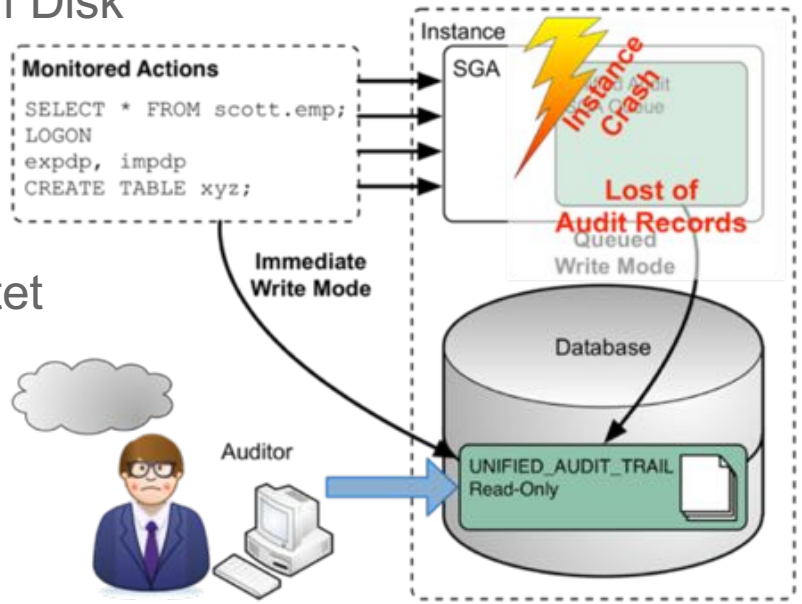
- Sperren der inaktiven Benutzer bzw. sperren von Benutzer die **n** Tagen nicht mehr eingeloggt waren
  - Setzen von INACTIVE_ACCOUNT_TIME in einem Oracle Profile
  - Wert zwischen 15 u d 24855 oder auf UNLIMITED gesetzt
  - LAST_LOGIN_TIME wird verwendet
- Neue Spalten in DBA_USERS gemäss cdenv.sql
  - LOCAL_TEMP_TABLESPACE – Standard Lokales Temp Tablespace
  - INHERITED – Wurde dieser Benutzer durch einen weiteren Container vererbt
  - DEFAULT_COLLATION – Standard Kollation vom Benutzer
  - IMPLICIT – Ist dieser Benutzer ein allgemeiner Benutzer oder impliziert durch eine Applikation erstellt

trivadis makes IT easier.

Unified Audit und Queue Management

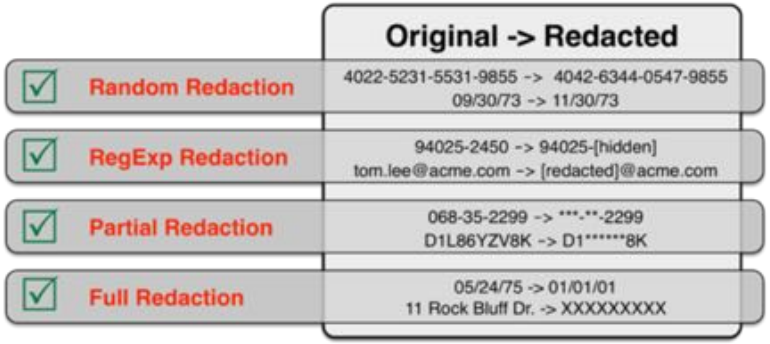
- Deprecation von UNIFIED_AUDIT_SGA_QUEUE_SIZE
  - Audit Daten werden sofort in eine interne relationale Table geschrieben
  - Kein Datenverlust im Fall eines Instance Crash / SHUTDOWN ABORT
- Abschaffung von Flush der Audit Trail Records auf Disk
  - Daten werden sofort in eine interne relationale Table geschrieben
  - Existierende Unified Audit Records müssen **Transferiert** werden
- Unified Audit ist standardmässig nicht eingeschaltet
  - Neue Datenbanken laufen im **Mixed Mode**
  - Reiner Unified Mode mit binary relink sehe MOS Note 1567006.1

```
cd $ORACLE_HOME/rdbms/lib
make -f ins_rdbms.mk uniaud_on ioracle
```



trivadis makes IT easier.

Data Redaction

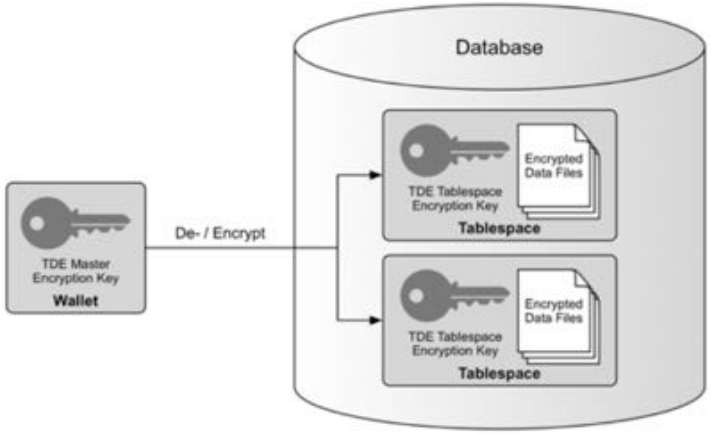


- Erstellen von Named Data Redaction Policy Expressions
  - Wieder verwenden von Named Expressions in verschiedenen Policies
  - Updates werden in einer Named Policy Expressions gemacht, sind in allen zugewiesenen Spalten aktiv
- Erweiterter Support für Redaction von Unstrukturierten Daten
  - Redaction von CLOB and VCLOB basierend auf Regulären Ausdrücken
  - Oracle 12c R1 unterstützt nur Full Redaction für CLOB/VCLOB. Daten werden als ***[redacted]*** angezeigt.

trivadis makes IT easier.

Übersicht Transparent Data Encryption 12cR2

- TDE Tablespaces **live / online** Konvertierung
  - Verschlüsseln, Entschlüsseln oder rekey eines vorhandenen Tablespaces
  - Keine Datenreorganisation nötig wie bis anhin
  - TDE Migration läuft im Hintergrund …
    Ist nicht ganz “Gratis”



- Möglichkeit zum **entschlüsseln** eines Tablespaces
- Komplette Verschlüsselung einer DB inklusive internen Tablespaces
  - SYSTEM, SYSAUX und UNDO
- TDE Tablespace offline Konvertierung zur Parallelisierung...
  - DataGuard zuerst physische Standby verschlüsseln und anschliessend Switchover...
  - Oder Tablespace für Tablespace verschlüsseln

trivadis makes IT easier.

Transparent Data Encryption Initialisierungsparameter

- Einführung eines neuen Initialisierungsparameter ENCRYPT_NEW_TABLESPACES
  - Neue Tablespaces werden mit **AES128** verschlüsselt
  - Die Oracle Variante von “Cloud Databases are always encrypted”
  - TDE wallet muss vorgängig konfiguriert und geöffnet werden
- Mögliche Werte
  - CLOUD_ONLY — Nur Tablespace in der Cloud sind verschlüsselt
  - ALWAYS — Jedes neue Tablespace ist verschlüsselt
  - DDL — Verschlüsselung nur durch Angabe in DDL Statement
- Obwohl es einen versteckten Parameter gibt **_default_encrypt_alg** ist es nicht möglich den Standardwert für die Verschlüsselung anzugeben
- Weitere hidden Parameter im Zusammenhang mit TDE

trivadis makes IT easier.

TDE Unterstützt weitere Verschlüsselungsalgorithmen

- SEED und ARIA für South Korea…
  - SEED ist ein Block Cipher Algorithmus mit 128bit Blöcken und 128bit Keys entwickelt in den 1990's
  - ARIA ist ein Block Cipher Algorithmus ähnlich zu AES mit 128bit Blöcken und variablen Schlüsseln (128, 192 or 256) entwickelt in 2003
- GOST für Russland …
  - GOST ist ein Block Cipher Algorithmus ähnlich zu DES mit 64bit Blöcken / 256bit Keys entwickelt in den 1970's

trivadis makes IT easier.

TDE Unterstützt Entschlüsselung und Rekey

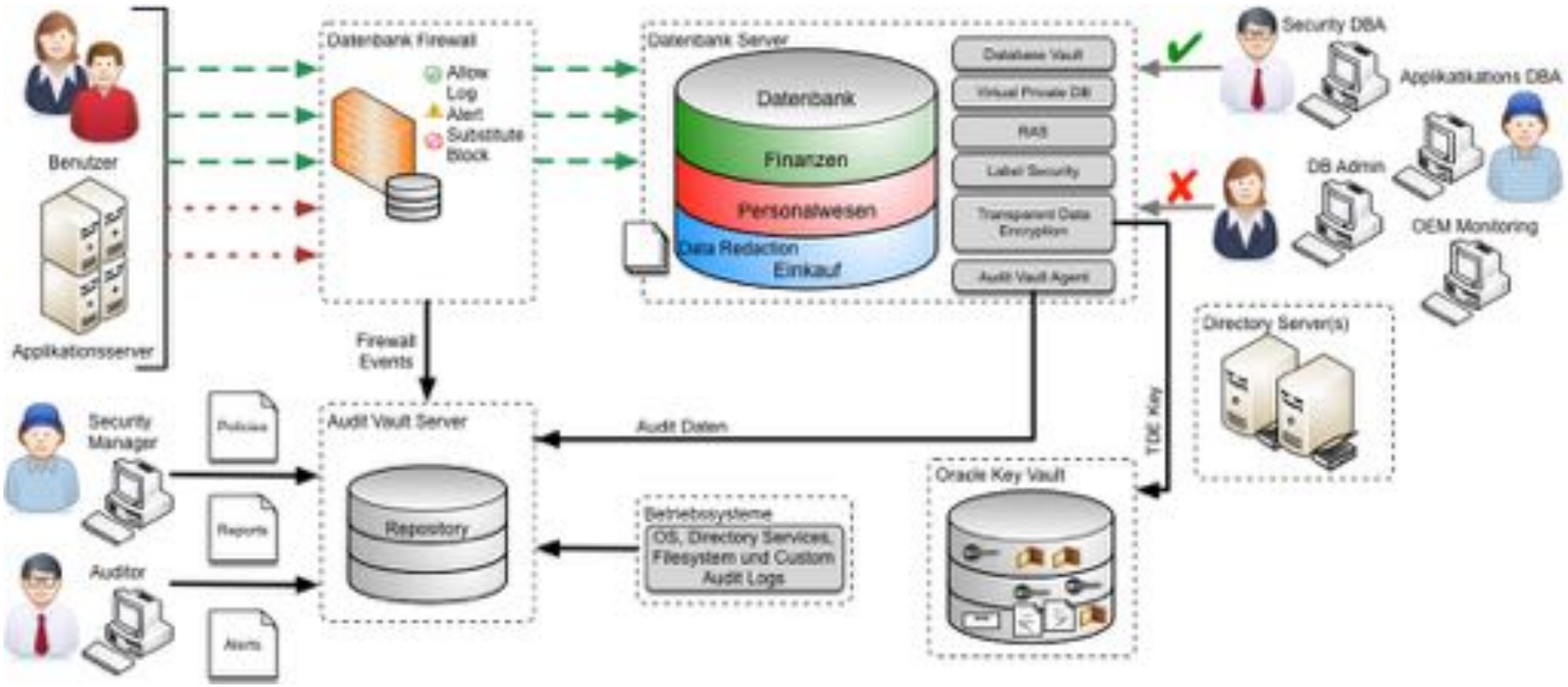
- Verschlüsselte Tablespaces können komplett entschlüsselt werden
  - Verschlüsselung in der Cloud und entschlüsselt On-Premises
- ReKey - neu Verschlüsslung jedes Blockes mit dem neuen Master Key

trivadis makes IT easier.

Datenbank Sicherheitsfeature und GDPR / DSGVO

trivadis makes IT easier.

Maximale Datensicherheit Architektur



trivadis makes IT easier.

Database Security Feature und GDPR / DSGVO

GDPR	Massnahmen	Database Security Features
Beurteilen	Prozesse, Datensensibilität, Risiko Assessment	
Verhindern	Verschlüsselung	• Transparent Data Encryption (OEE) • Key Vault (OEE/OSE) • Netzwerk Verschlüsselung • Externe Verschlüsselung
	Fine Grained Access Control	• Virtual Private Database (OEE)
	Anonymisierung / Pseudonymisierung	• Data Masking • Data Reduction • Drittprodukte
	Trennen der Verantwortlichkeiten	• Database Vault, Label Security (OEE) • Active Database Monitoring

trivadis makes IT easier.

Database Security Feature und GDPR / DSGVO

GDPR	Massnahmen	Database Security Features
Erkennen	Auditing	• Database Audit Standard (OEE/OSE) • Unified Audit (OEE/OSE) • Fine Grained Audit (OEE) • Applikationsaudit
	Active Monitoring	• Audit Vault and Database Firewall • McAffee Activity Monitoring • Imperva SecureSphere
	Alarmierung	• dito
	Rapportierung	• dito

- OEE Oracle Enterprise Edition
- OSE Oracle Standard Edition / Standard Edition One

trivadis makes IT easier.

Database Security Feature

- Oracle bietet einen viel Zahl von Security Feature und Produkten
- Wie sieht das Risiko in ihrem Unternehmen aus?
- Welche Datenbank Option wird benötigt, um GDPR Compliant zu sein?
  1. Oracle Advanced Security
  2. Oracle Data Masking
  3. Alle
  4. Keine
  5. Kommt darauf an

trivadis makes IT easier.

Fazit

- Sicherheit muss an vielen Stellen umfassend umgesetzt werden
- Als erstes müssen Sie wissen, was Sie brauchen
- Mit Oracle 12c R2 bringt nicht so viele Neuerungen im Security Umfeld wie 12c R1
  - Ein paar sinnvolle Verbesserungen und einige "must have" für Cloud-Umgebungen
- Endlich besteht die Möglichkeit, vorhandene Tablespaces zu verschlüsseln

trivadis makes IT easier.

Trivadis Lösungen

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

trivadis
makes IT easier.

Datenbank Server Security Reviews

- Professionellen Überblick über den Zustand Ihrer Oracle Instanzen
- **Transparenzgewinn** durch die Dokumentation der Review Ergebnisse und daraus resultierenden Risiken
- **Risikoreduktion** durch konkrete kurz- und mittelfristige Massnahmen zur nachhaltigen Verbesserung
- Kundenspezifischer Fokus
  - Allgemein, Security, Performance

Trivadis Factsheet

Packaged Consulting Solutions

Fixpreislösungen für Oracle- und Microsoft-Datenbankserver

DIE LÖSUNG AUF EINEN BLICK

Einfach – Methodisch – Kompetent. Benötigen Sie einen Review Ihrer Datenbankinfrastruktur oder ein Hochverfügbarkeits-Setup? Dann sind unsere Dienstleistungspakete für Oracle und Microsoft- Datenbankserver genau das richtige: ein klar definiertes Resultat zu einem festen Preis. Sie profitieren dabei von unserer ausgewiesenen Expertise und unserer langjährigen Erfahrung im Datenbank-Infrastruktur-Engineering.

UNSER ANGEBOT

Mit den **Review-Paketen** analysieren und bewerten wir Ihre Oracle- oder SQL-Server Datenbanksysteme bezüglich Konfiguration, Performance, Security oder Lizenzierung. Unsere Review-Pakete liefern die Grundlage für die Optimierung Ihrer Datenbank-Infrastruktur.

- Database Basic Review – den Zustand Ihrer Datenbank auf einen Blick
- Database Performance Review – wir zeigen Ihnen auf wo es klemmt

trivadis
makes IT easier.

Trivadis Package Consulting Solutions

- **Review-Pakete**
  - Analyse Ihres Systems
  - Bewertung / Gewichtung
  - Massnahmenkatalog und Empfehlungen
- **Setup-Pakete**
  - Installation und Konfiguration nach Trivadis Best-Practice
  - Durchführung von Funktionscheck
- Einfache Abwicklung
- Klar definierter Dienstleistungsumfang zu einem festen Preis

Trivadis Factsheet

Packaged Consulting Solutions

Fixpreislösungen für Oracle- und Microsoft-Datenbankserver

Trivadis makes IT easier.

DIE LÖSUNG AUF EINEN BLICK

Einfach – Methodisch – Kompetent. Benötigen Sie einen Review Ihrer Datenbankinfrastruktur oder ein Hochverfügbarkeits-Setup? Dann sind unsere Dienstleistungspakete für Oracle und Microsoft- Datenbankserver genau das richtige: ein klar definiertes Resultat zu einem festen Preis. Sie profitieren dabei von unserer ausgewiesenen Expertise und unserer langjährigen Erfahrung im Datenbank-Infrastruktur-Engineering.

UNSER ANGEBOT

Mit den **Review-Paketen** analysieren und bewerten wir Ihre Oracle- oder SQL-Server Datenbanksysteme bezüglich Konfiguration, Performance, Security oder Lizenzierung. Unsere Review-Pakete liefern die Grundlage für die Optimierung Ihrer Datenbank-Infrastruktur.

- Database Basic Review – den Zustand Ihrer Datenbank auf einen Blick
- Database Performance Review – wir zeigen Ihnen auf wo es klemmt

trivadis makes IT easier.

Infrastruktur Optimierung

- **Transparenzüber** Zustand, Risiken und Optimierungspotential Ihrer IT-Infrastruktur und den betriebsnahen IT-Prozessen
- **Kostenoptimierung** durch effizientere Nutzung der Ressourcen
- **Risikominimierung** durch bewährte Konzepte, langjährige Erfahrung und erstklassige Expertise

IT Infrastruktur-Optimierung

General Assessment

Trivadis makes IT easier.

PERFORMANCE & CAPACITY | BACKUP & RECOVERY | OPERATION OPTIMIZATION | LICENSE OPTIMIZATION | CLOUD OPTIMIZATION

Unser Angebot

- Umfassende **Gesamtanalyse** Ihrer **Oracle** oder **Microsoft** Infrastruktur
- Vor-Ort Interview, Stichproben und Validierung durch erfahrene Consultants
- Kompakter Bericht mit konkreten Optimierungsempfehlungen und Massnahmenkatalog; inkl. Präsentation
- CHF 3'490.–

Ihr Nutzen

- **Transparenz** über Zustand, Risiken und Optimierungspotential Ihrer IT-Infrastruktur und den betriebsnahen IT-Prozessen
- **Kostenoptimierung** durch effizientere Nutzung der Ressourcen
- **Risikominimierung** durch bewährte Konzepte, langjährige Erfahrung und erstklassige Expertise

Warum Trivadis?

- Trivadis ist führend bei der IT-Beratung, der Systemintegration, dem Solution Engineering und der Erbringung von IT-Services mit Fokussierung auf Microsoft- und Oracle-Technologien in der Schweiz, Deutschland, Österreich und Dänemark.
- 20+ Jahre Erfahrung in Infrastruktur Engineering und Betriebsoptimierung.
- Wir unterstützen Sie von der **Analyse**, über die **Planung** bis zur **Umsetzung** Ihres Optimierungsvorhabens

trivadis makes IT easier.

Cloud Governance Assessment

- Grundlage für die Nutzung und Integration von Cloud Services
- Belastbare Grundlage
- Konkrete Massnahmen zur Umsetzung
- Identifikation der notwendigen Rollen & Skills
- Verbindliche Policy im Umgang mit Cloud Services und Cloud Providern

trivadis makes IT easier.

Cloud Readiness Assessment

- **Umfassende Analyse** Ihrer Infrastruktur im Hinblick auf eine Cloud basierte Infrastruktur
- **Transparenz** bezüglich Kosten und Nutzen
- **Fundierte** Beurteilung der Machbarkeit und der Risiken
- **Praktische Roadmap** für Ihr Cloud-Transformations-Vorhaben
- Schnelle und risikolose Cloud-Adaption

trivadis
makes IT easier.

Links und Quellen

- Trivadis das Unternehmen https://www.trivadis.com/de/unternehmen
- Trivadis Toolbox für Oracle und SQL Server
  https://www.trivadis.com/de/trivadis-toolbox
- Trivadis Oracle und SQL Server Review
  https://www.trivadis.com/de/packaged-consulting-solutions
- Trivadis Infrastruktur Optimierung und Cloud Readiness
  https://www.trivadis.com/de/it-infrastruktur-optimierung
- Trivadis Training https://www.trivadis.com/de/training
- Trivadis Security Expert Team https://www.trivadis.com/de/security

trivadis makes IT easier.

Links und Quellen

- Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates
  http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679
- Datenschutz-Grundverordnung DSGVO https://dsgvo-gesetz.de/
- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)
  https://www.edoeb.admin.ch/datenschutz/00618/00802/00812/index.html?lang=de
- Medien Mitteilung Bundesamt für Justiz BJ zur Revision DSG
  https://www.bj.admin.ch/bj/de/home/aktuell/news/2016/ref_2016-12-21.html
- Vorentwurf DSG
  https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf

trivadis makes IT easier.

Links und Quellen

- Microsoft GDPR Informationen
  - Whitepaper https://aka.ms/gdprwhitepaper
  - Web https://www.microsoft.com/en-us/trustcenter/Privacy/GDPR
- Oracle und GDPR http://www.oracle.com/technetwork/database/security/wp-security-dbsec-gdpr-3073228.pdf

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

trivadis
makes IT easier.