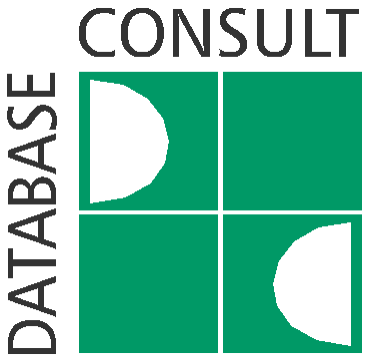



# Das ewige Thema:
# DBAs und Datenschutz

SIG Security – 26. März 2014

Dr. Günter Unbescheid

Database Consult GmbH

Jachenau

# Database Consult GmbH

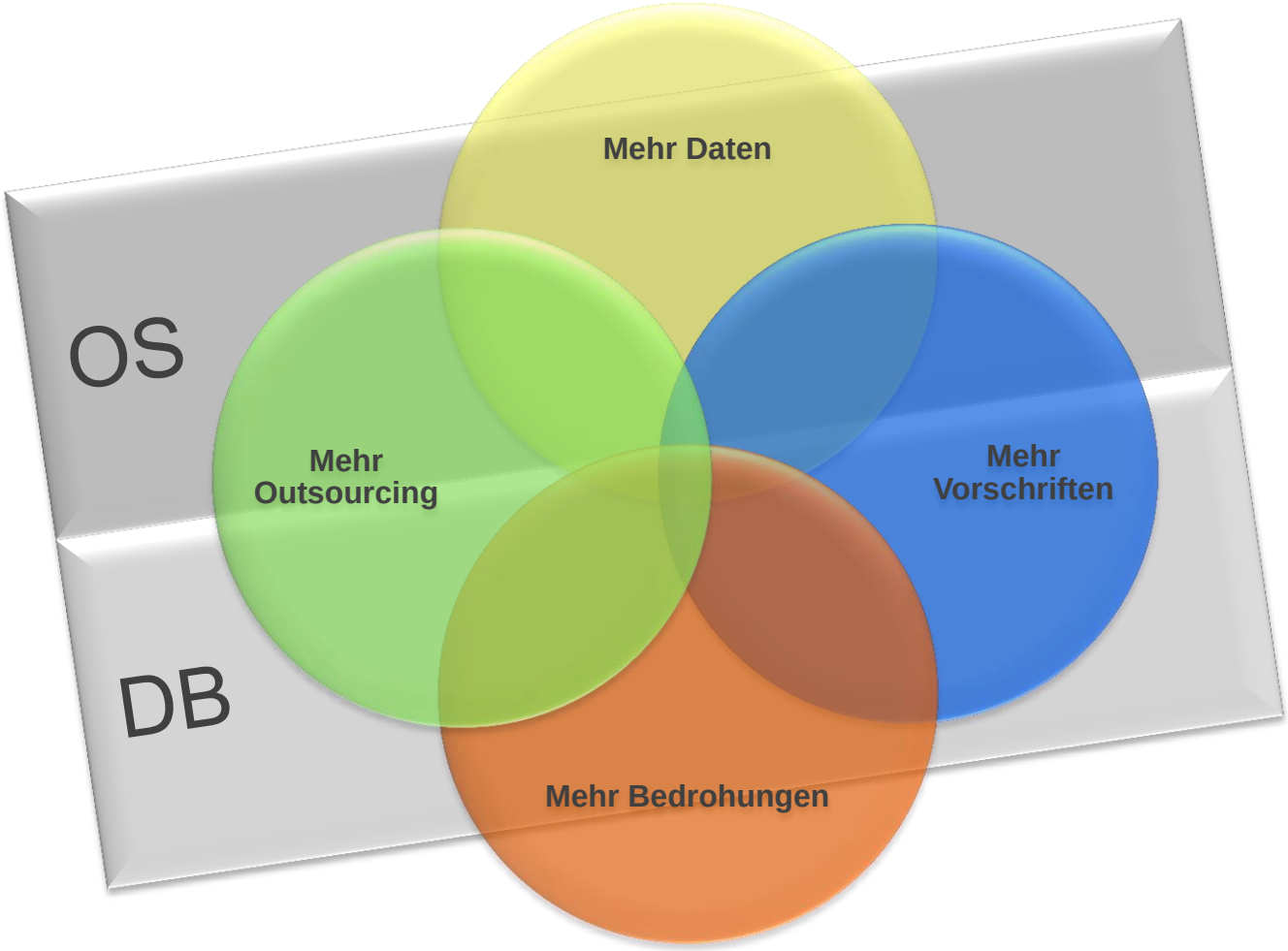
- Gegründet 1996
- Kompetenzen im Umfeld von ORACLE-basierten Systemen
- Tätigkeitsbereiche
  - Security, Identity Management
  - Tuning, Installation, Konfiguration, Systemanalysen
  - Support, Troubleshooting, DBA-Aufgaben
  - Datenbankdesign, Datenmodellierung und –design
  - Maßgeschneiderte Workshops
  - www.database-consult.de
- Seit 2012 – Kooperation mit trivadis makes IT easier.

DBAs und Datenschutz

# Agenda

- Ausgangspunkt und Motivation
- Der gesetzliche und thematische Rahmen
- Das grundlegende Dilemma
- Strategische Lösungsmodelle
- Werkzeuge des Identity Managements

# DBA im Spannungsfeld



# Der gesetzliche Rahmen

- Datenschutzrisiko durch (umfassenden) Zugriff auf Basisdaten, Infrastruktur und Sicherungen
- Der Begriff „Datenschutz“ hat sich entwickelt (Wiki):
  - Anfangs Schutz der Daten selbst vor Verlust, Beschädigung etc.
  - Schutz der Persönlichkeitsrechte bei der elektronischen Speicherung privater Daten (informationelle Selbstbestimmung / Schutz der Privatsphäre)
- Begriffliche Unterschiede EU und USA
  - USA: Daten gehören dem „Sammler“
  - EU: Daten gehören der beschriebenen Person
  - „Safe Harbour“ Abkommen/Verpflichtung – derzeit ausgesetzt (PRISM)
- Gesetztlicher Schutz personenbezogener Daten
  - Bundesdatenschutzgesetzt, Landesdatenschutzgesetze, Rechtsnormen (TKG etc.)

# Der gesetzliche Rahmen (2)



- Personenbezogen =
  - Beschreibung persönlicher oder sachlicher Verhältnisse einer natürlichen Person
- Kontrollorgane: DSB – Leiter der verantw. Stelle – Geschäftsleitung Schutzbeauftragte
- Verpflichtung auf das Datengeheimnis betrifft nicht die Wahrung / den Schutz von Firmengeheimnissen

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. (§5 BDSG)

# Die 7 Grundprinzipien des DS bei PB Daten



- Verbot mit Erlaubnisvorbehalt
  - Ausnahmen nach Regelung
- Direkterhebung
  - Erhebung beim Betroffenen
- Datensparsamkeit
  - sparsamer Umgang, Aufbewahrungsfristen
- Datenvermeidbarkeit
  - so wenig wie möglich gemäß Ziel
- Transparenz
  - Kenntnis des Betroffenen
- Zweckbindung
  - Zweck vor der Erhebung festzulegen
- Erforderlichkeit  (kontrovers diskutiert)

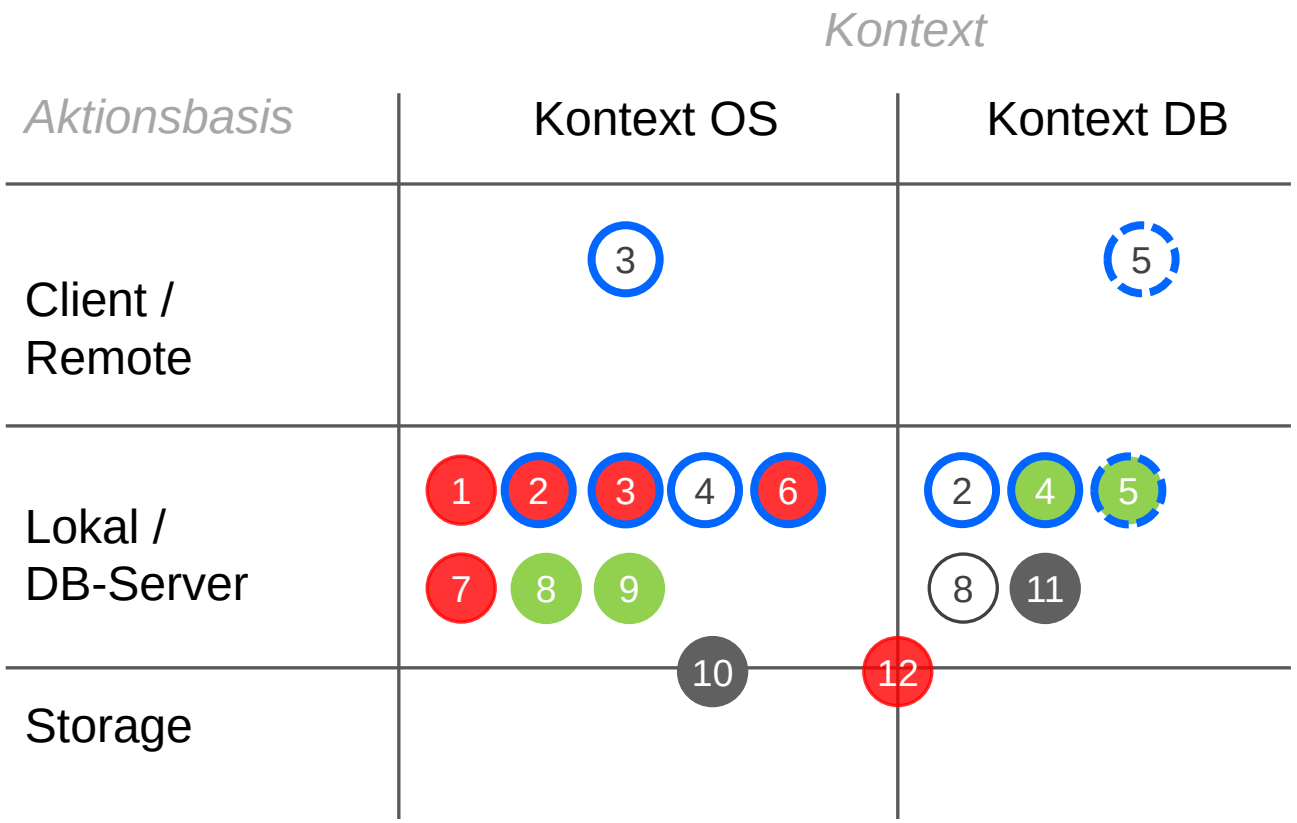
# Maßnahmenspektrum für Administratoren

- Technisch organisatorische Maßnahmen (TOM) formulieren
- Ausweitung des PB Datenschutzes auf „Firmengeheimnisse“
- Log-/Trace-/Audit-Daten: Eindeutige Aufbewahrungsfristen mit nachhaltiger Löschung
- Reduzierung des Personenkreises durch strikte Rollentrennung
- Audit-Daten: forensische Analysen empfohlen/wichtig
- Anonymisierung sinnvoll für:
  - Audit-Reports
  - Zweckgebundene Überschreitung der Fristen
- Herausforderung: Der Umgang mit administrativen Zugriffsprivilegien

# Aufgabenspektrum DBA

(1) Oracle Software Installation
(2) Oracle Patch-Installation
(3) Start/Stop-Aktionen: Datenbank, Listener, Agenten …
(4) Datenbank Konfiguration/Installation
(5) Datenbank Wartung: diverse alltägliche Aufgaben
(6) Backup/Recovery
(7) Troubleshooting: Log-/Trace-Dateien (Listener, RDBMS etc.)
(8) Monitoring: Verfügbarkeit/Performance (Bereitstellung)
(9) Housekeeping: Aufräumarbeiten
(10) Storage: ASM-Administration
(11) Schema Deployment (für Applikationen)
(12) Auditing: Konfiguration/Auswertung

# Aufgabenspektrum




Nummern referenzieren voranstehende Folie

- Kundenspezifisch
- Alternative oder Zusatz
- Gelegentlich oder weniger kritisch
- häufig oder kritisch
- Mit SYSDBA / SW-Owner

# Rückschlüsse

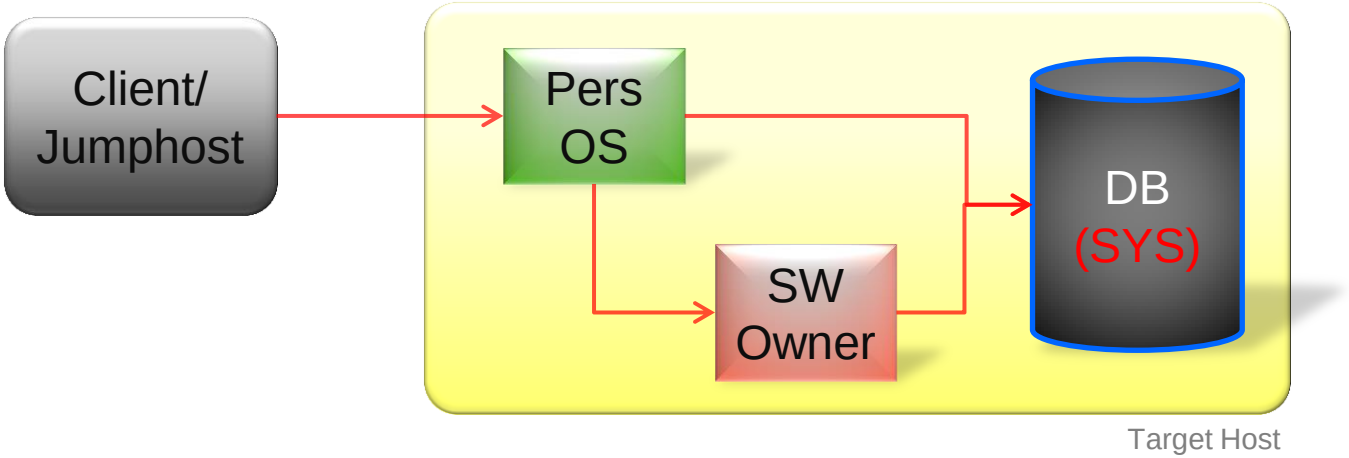
- Ein großer Teil der Aufgaben erfordert SYS/SYSDBA Privilegien oder SW-Owner Zugriffe
  - Aktivitätsschätzungen ergeben ca. 40 – 60% je nach Auswertung
  - Die Häufigkeit erfordert permanente Privilegierung
  - Gefahr des Mißbrauchs
- Administrative Fachdatenzugriffe nur ca. 10% - 20%
- Weitere Admin-Aufgaben sind „privilegierbar“
  - Least Privilege durch maßgeschneiderte Systemprivilegien
  - Z.B. `create user`, `manage tablespace` etc.
- Personalisierte DB-Administratoren sind zuwenig, ggf. nicht nötig
- Personalisierte OS-User garantieren die Nachvollziehbarkeit in allen Tätigkeitsbereichen
- Dilemma beim Datenschutz: Der Umgang mit Admin-Privilegien

# Grundlegende Strategien

- Permanente Privilegierung
  - „SYSDBA“ steht pauschal zur Verfügung
- Temporäre Privilegierung
  - „SYSDBA“ wird Event-gesteuert freigeschaltet
- Gemischte temporäre Privilegierung
  - Permanenter Zugang, SYSDBA nur temporär
- SYSDBA-Eingrenzung
  - Beschneidung der SYSDBA-Rechte
- Für alle Modelle gilt:
  - Eindeutige Nachvollziehbarkeit administrativer Aktionen
  - Revisionssicherheit der Audit- bzw. Lof-Daten – diverse Ebenen
  - Automatisierte Analysen der Audit-Daten
  - Starke Authentifizierungsmethoden, aktuelle Administration
  - Klassifizierung der DBs kann Aufwand reduzieren helfen

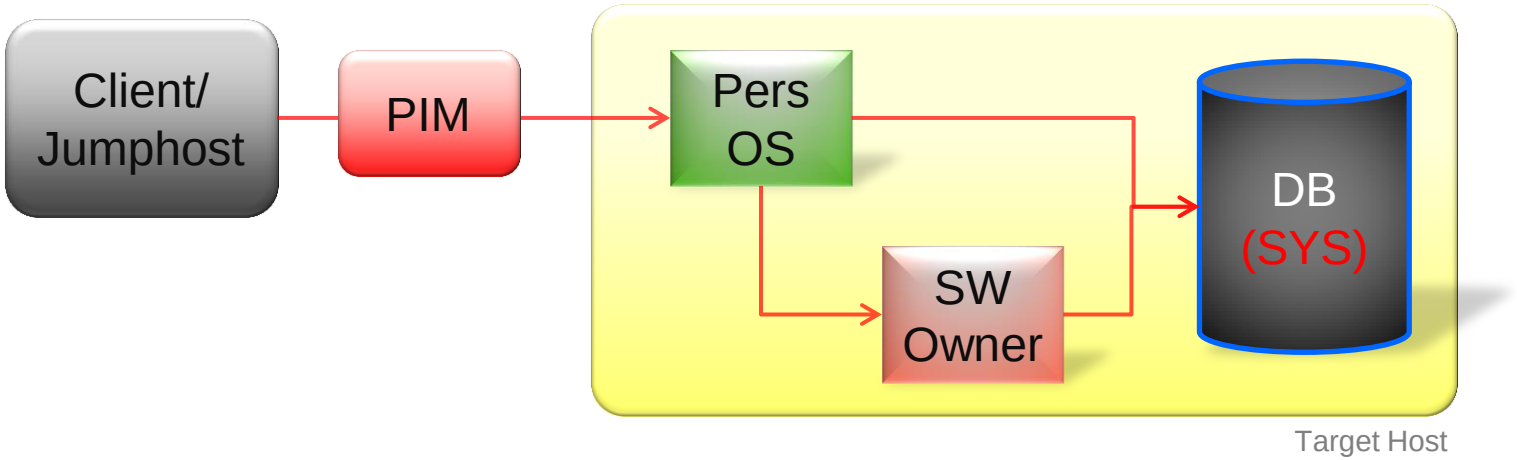
# Permanente Privilegierung





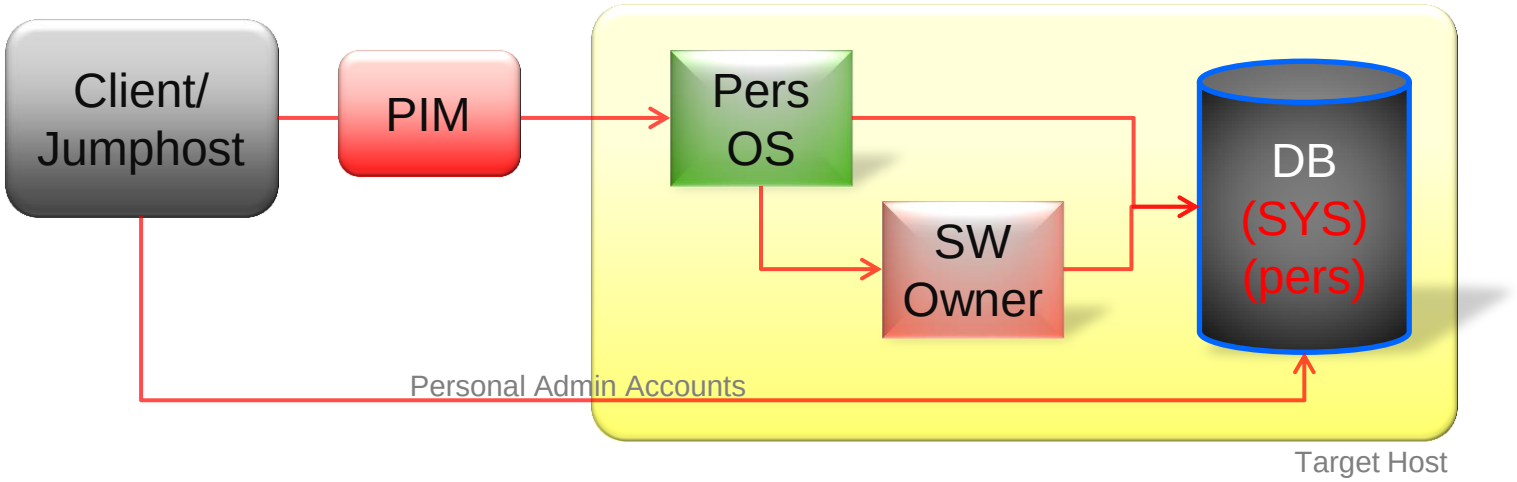

- Personal OS-User auf dem Target – Mitglied DBA-Gruppe
- Authentifizierung per PW, SSH-Keypair / SmartCard / Zertifikat …
- Per `sudo` Wechsel auf SW-Owner
- SYSDBA *from remote* ausschalten
- DB-Auditing z.B. über `audit_syslog_level` (*remote logging*)
  - Zentrale Rolle für das Auditing!
- DB-User SYS – nachvollziehbar über OS-User

# Temporäre Privilegierung




- PIM-System verwaltet Zugriffe auf Targets – eigenes Logging
  - Freischaltung durch PW-Bekanntgabe oder Bereitstellung (Menü)
  - Lokale, native Authentifizierung auf dem Target, oder
  - Zentralisierung der Authentifizierung, z.B. über Active Directory
- Freischaltung nur bei Event/Incident, ansonsten Abschottung
- Ansonsten wie das Vorgängermodell

# Gemischte temporäre Privilegierung

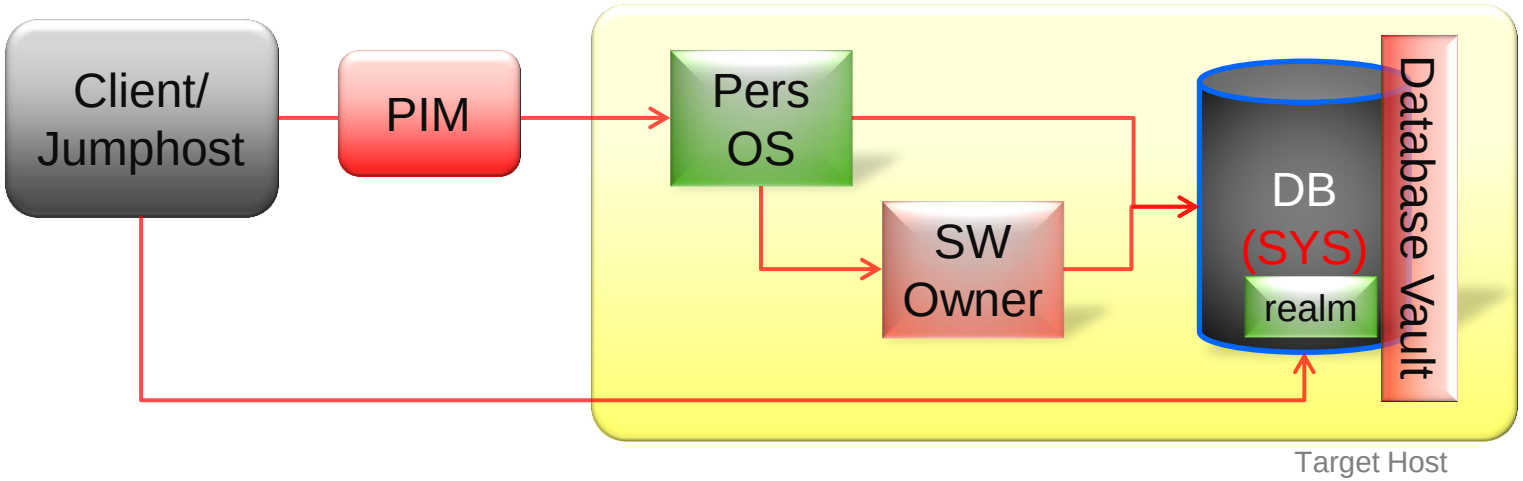



- Wie Vorgänger, jedoch werden Admin-Aktionen klassifiziert
- Aktionen ohne Datenschutz-Auswirkungen werden ohne Freischaltung *from remote* zugelassen – personal DB-User
  - Maßgeschneiderte Systemprivilegien und Rollen in der DB
  - Zentralisierung möglich
- Aktionen mit Auswirkungen auf den Datenschutz sowie lokale Maßnahmen laufen über die Freischaltung

# Gemischte temporäre Privilegierung

- Ergänzend:
  Möglichkeiten der Zentralisierung für remote DB-(Admin-)Zugriffen
- Enterprise User-Konzept
  - Enterprise Benutzer im Verzeichnisdienst (AD, OID, OUD)
  - Globale Benutzer in DB (*shared schema*)
  - Methoden: Direkter Eintrag, Server Chaining, DIP
  - Authentifizierung: Passwort, Kerberos, Zertifikat
  - Enterprise+Globale Rollen zur Autorisierung
  - Ab 11g SYSDBA möglich
  - Proxy-User möglich für Arbeiten in fremden Zielschemata
  - Ad hoc Freischaltungen möglich
- Externe Kerberos-Authentifizierung
- PKI/Zertifikate/Smardcards zur Authentifizierung

# SYSDBA-Eingrenzung

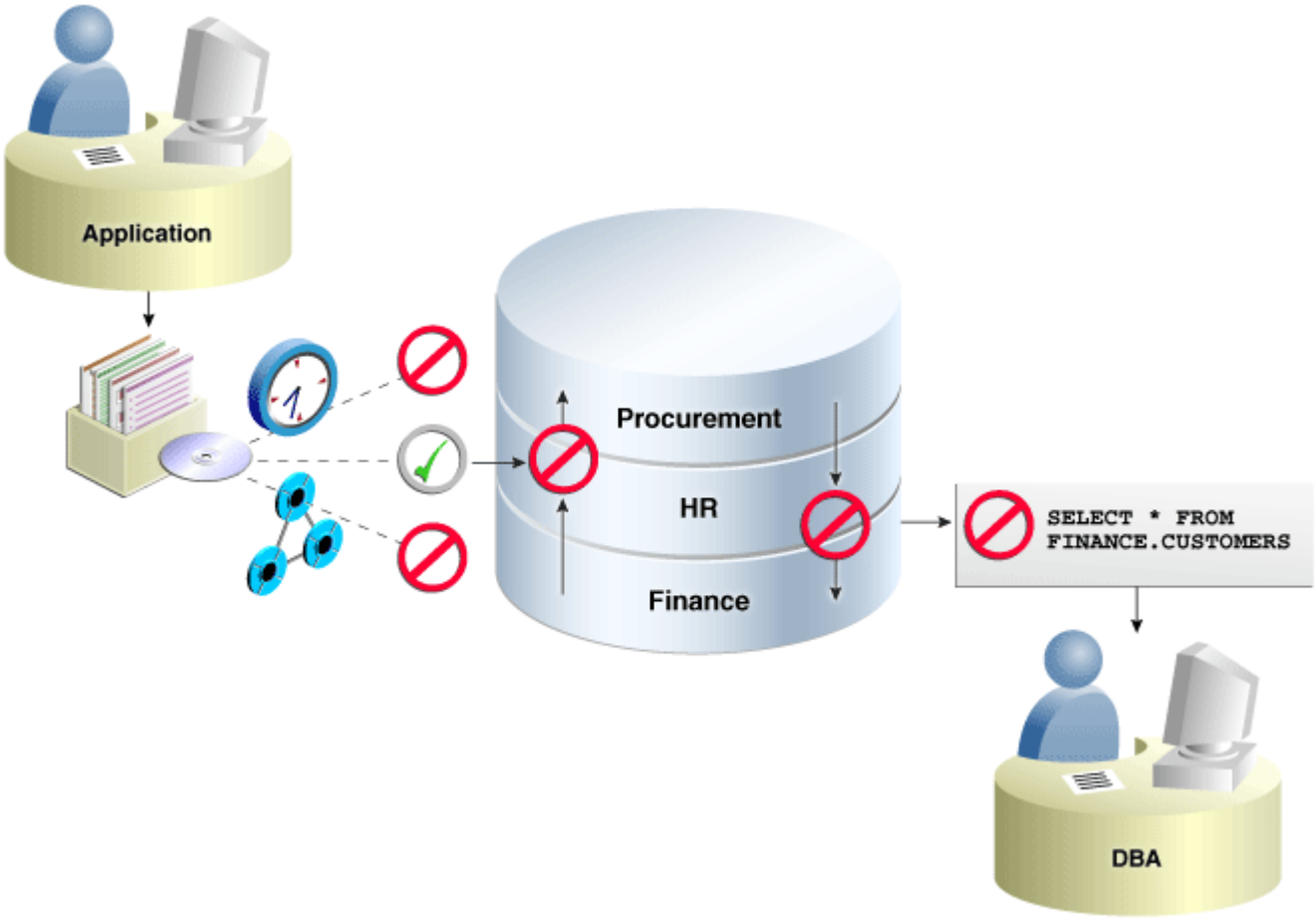



- Admin-Schutzzonen in Form von realms (innerhalb der DB)
- Zusätzliche Rollen: realm-Administratoren etc.
- Schutz vor SYSDBA- und Any-Rechten
- Kein Schutz auf OS-Ebene (Log- und Trace-Dateien etc.)
  - Achtung: Ausschalten auf Target möglich – Monitoring!
- Auch bei App-Konsoldierungen und Privilegien-bewußten Vorgaben
- Einsatz von PIM ist möglich für lokale OS-Aktionen

# Database Vault

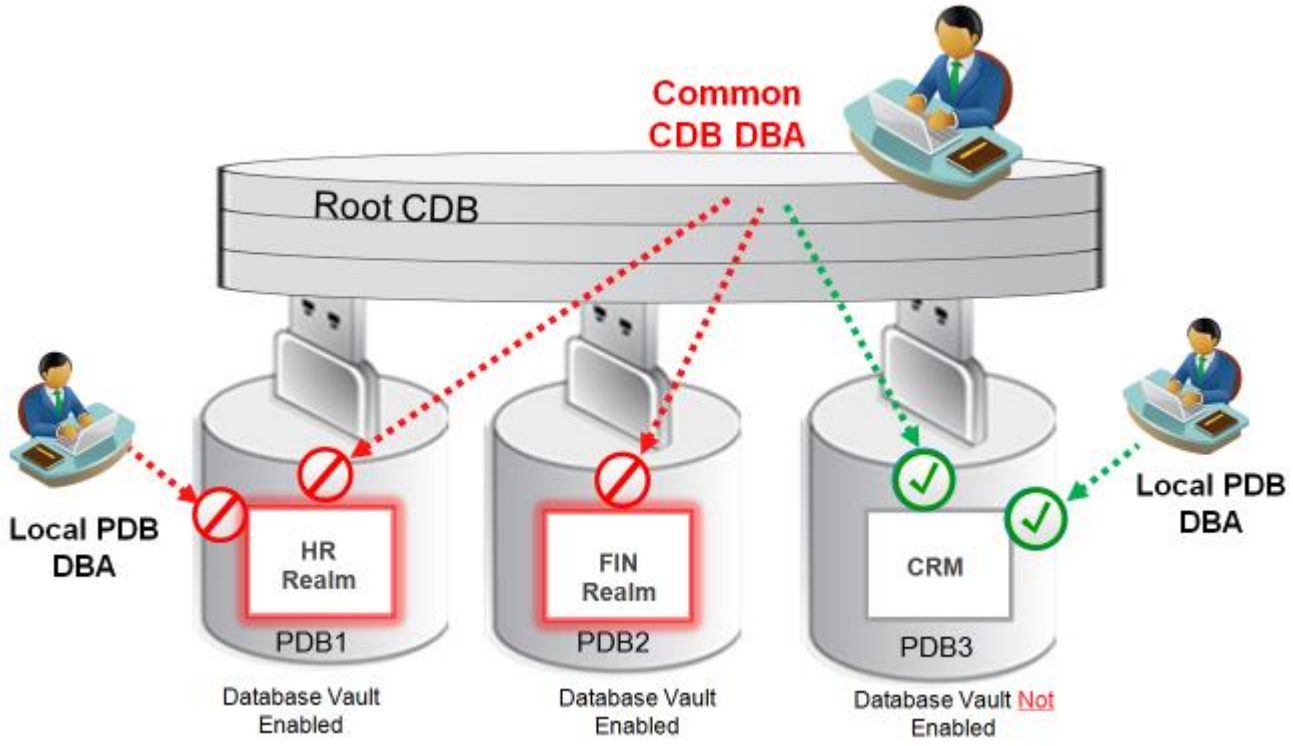
- Kostenpflichtige Option der Enterprise Edition der Datenbank
  - Verfügbar ab Oracle 10g Release 2
- Einschränkung administrativer Benutzer innerhalb der Datenbank
  - Sinnvoll bei SYSDBA-Priivilegien
  - Kein Schutz auf OS Ebene
- Konzept
  - Daten in eigenen Tablespaces – DVSYS und DVF
  - Modifikation/Reduktion von Standardrollen (DBA, IMP_FULL_DATABASE, EXECUTE_CATALOG_ROLE)
  - Package-Calls und grafische Oberfläche
- Objektschutz durch *realms*, *rule sets* und *command rules*
  - Zugriff nur durch Owner und explizite Grant-Ermächtigungen

# Oracle Database Vault



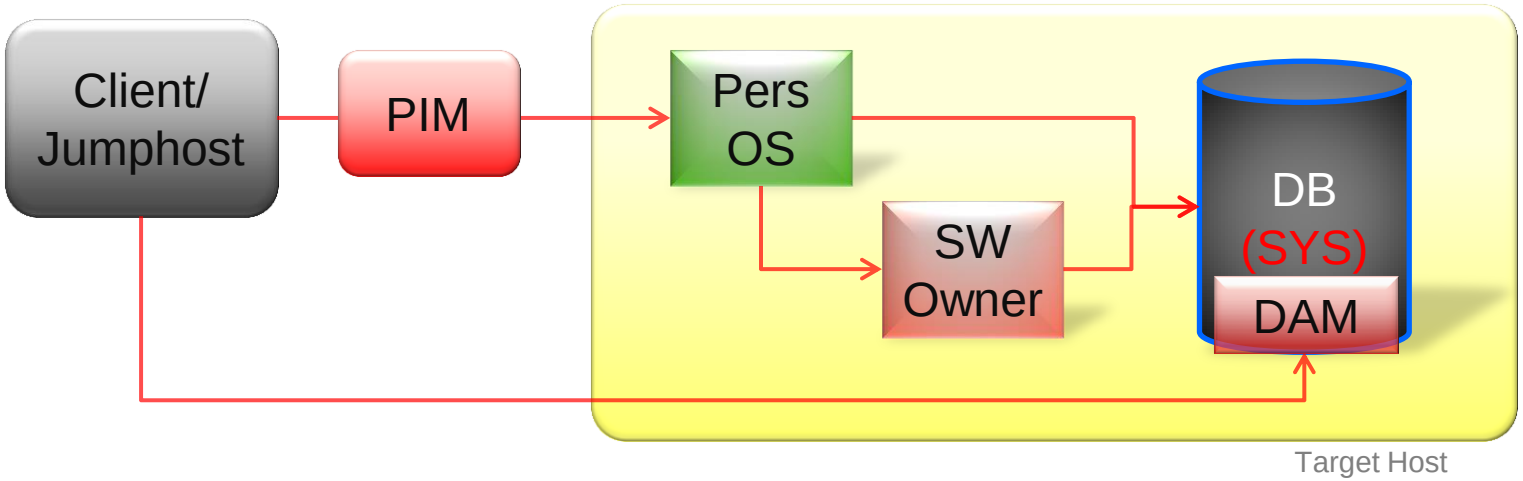

Quelle: Oracle

# Database Vault 12c



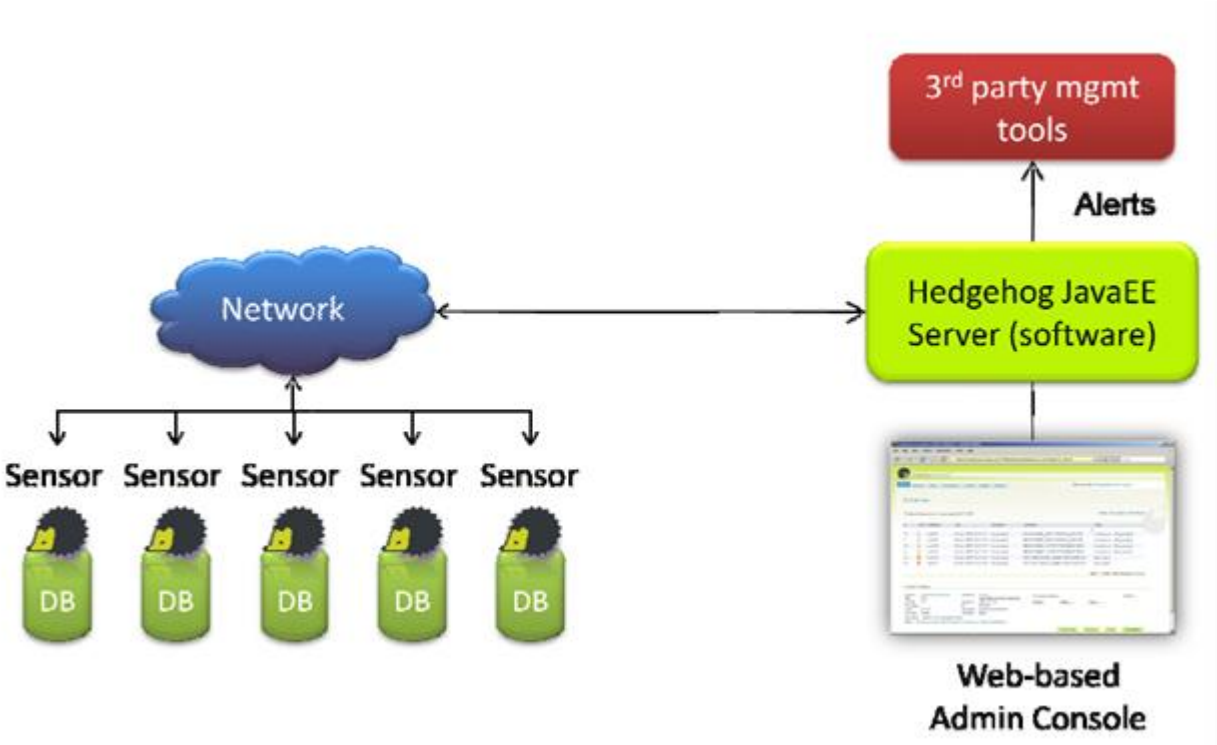

Quelle: Oracle

# SYSDBA-Eingrenzung (alternativ)




- Database Activity Monitoring (DAM)
  - Activity Monitoring über SGA-Pooling auf der Basis eines Regelwerks
  - Lokaler Agent - Zentrales Repository (auch NON-Oracle Systeme)
  - Vordefinierte und Custom Rules, Berichte etc.
- Sperrung von Aktionen möglich durch *Session Aborts*

# DAM




Quelle McAfee

# Weitere PIM Werkzeuge



- Database Activity Monitoring (DAM)
  - Ehemals Sentrigo Hedgehoc, Übernahme 4/2011 durch McAfee
  - Agenten/Sensoren auf den DB Servern „monitoren“ SGA
  - Regeln protokollieren Aktionen – kill session möglich
- OPAM - Oracle Privileged Account Manager
  - Oracle Fusion Middleware Application unter Oracle WebLogic Server
  - PW Repository zur Generierung, Bereitstellung und Management
  - Anpassung der PW auf den Zielsystemen
- Oracle Identity Manager (OIM)
- User Management for Databases (UM4DB)  (OIM++)
  - In Deutschland auch CUA4DB
  - Zentralisierte Verwaltung und Verteilung von User Accounts
  - Connectoren auf den Zielsystemen

# Weitere PIM Werkzeuge

- CyberArK – Privileged Account Management
- Centrify – zentralisiertes Identity-Management, AD Authentication
- PowerBroker (beyondtrust)
- ArcSight  (HP) – Loganalyse und –management
- Weitere Produkte von DELL/Quest, IBM etc.

# Fazit

- Datenschutz für/vor Administratoren erfordert ein konzertiertes Vorgehen und ist nicht auf Knopfdruck verfügbar
- Es gibt keine „Best Practises“, gutes Design ist nötig
- Verschiedene Softwaretechniken stehen zur Verfügung
- Entscheidend ist darüber hinaus auch das menschliche Zusammenwirken bei den Konzeption und Konfiguration

# Danke für‘s Zuhören

www.database-consult.de