



> **Wie mache ich meine Oracle
Datenbank fit fürs PCI Audit?**
Angela Espinosa, LH Systems

11. Februar 2014



Lufthansa Systems

IT that makes your life easier

> Agenda

- ▶ **Vorstellung LH Systems AG**
- ▶ Definition PCI DSS
- ▶ Voraussetzung / abgesteckter Rahmen
- ▶ Der Einstieg
- ▶ Härtung der Datenbank nach PCI DSS Anforderung
- ▶ Knackpunkte
- ▶ Zusammenfassung



> Vorstellung Lufthansa Systems AG



> Vorstellung Lufthansa Systems AG

- breites Spektrum an IT-Leistungen – Full Service Provider
- Unterstützung bei Optimierung von Prozessen und IT-Landschaften
- weltweit führende Position in der Aviation-Industrie
- rund 2.800 Mitarbeitern
- mehrere Standorte in Deutschland und 16 weiteren Ländern (Hauptstandort: Frankfurt am Main)
- 6.800 Quadratmeter Rechenzentrumsfläche mit über 2.500 Servern
- Kunden: Fluggesellschaften, Unternehmen aus Industrie, Transport und Logistik, Energie, Medien und Verlage, Touristik und Gesundheitswesen
- Security: eigenes PCI Competence Center
- ISO, PCI und IKS geprüft und zertifiziert



> Agenda

- ▶ Vorstellung LH Systems AG
- ▶ **Definition PCI DSS**
- ▶ Voraussetzung / abgesteckter Rahmen
- ▶ Der Einstieg
- ▶ Härtung der Datenbank nach PCI DSS Anforderung
- ▶ Knackpunkte
- ▶ Zusammenfassung



> Definition PCI DSS



- PCI DSS = Payment Card Industry Data Security Standard
- Regelwerk im Zahlungsverkehr bezogen auf Kreditkartentransaktionen
- von allen wichtigen Kreditkartenorganisationen unterstützt
- Erfüllung der Regeln durch alle Unternehmen und Dienstleister, die Kreditkarten-Transaktionen speichern, übermitteln, oder abwickeln
- Falls nicht → Strafgebühren, Einschränkungen, Untersagung der Akzeptanz der Kreditkarten
- Regelungen bestehen aus einer Liste von zwölf Anforderungen an alle Systemkomponenten der Unternehmen



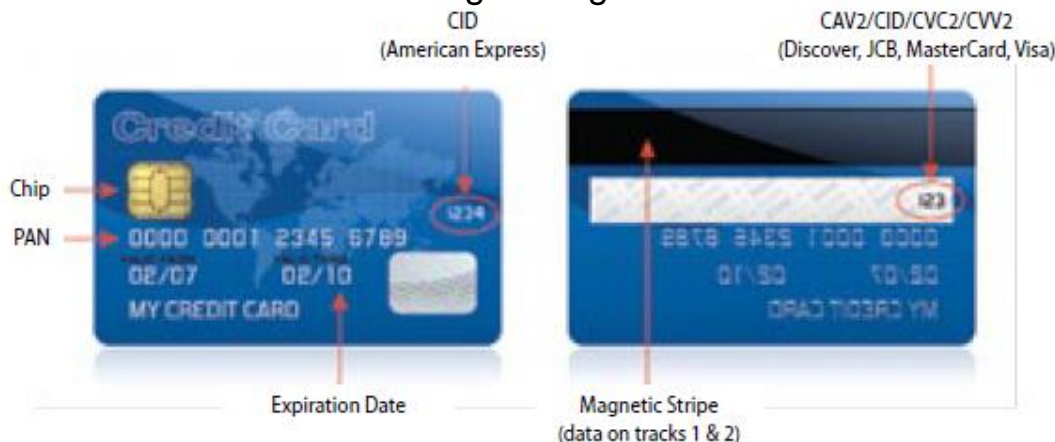
> Agenda

- ▶ Vorstellung LH Systems AG
- ▶ Definition PCI DSS
- ▶ **Voraussetzung / abgesteckter Rahmen**
- ▶ Der Einstieg
- ▶ Härtung der Datenbank nach PCI DSS Anforderung
- ▶ Knackpunkte
- ▶ Zusammenfassung



> Voraussetzung / abgesteckter Rahmen

- Datenbanksicherheit ist ein sehr umfangreiches Thema
- Wie werden die Kreditkartendaten in der Datenbank abgelegt?
 - Keine Verschlüsselung durch die Applikation
 - zusätzliche Sicherheitsmaßnahmen
 - z.B. Installation und Konfiguration von Oracle Database Vault und Oracle Transparent Data Encryption
 - Berücksichtigung deren Besonderheiten im Betrieb
 - Thema für einen neuen Vortrag
 - Verschlüsselung durch die Applikation
 - Aufwand der Härtung verringert sich



> Agenda

- ▶ Vorstellung LH Systems AG
- ▶ Definition PCI DSS
- ▶ Voraussetzung / abgesteckter Rahmen
- ▶ **Der Einstieg**
- ▶ Härtung der Datenbank nach PCI DSS Anforderung
- ▶ Knackpunkte
- ▶ Zusammenfassung



> Der Einstieg



- Man ist nicht auf einen Schlag „PCI compliant“.
- iterativer Lernprozess bezüglich Prozessen und Härtung
- kontinuierlicher Vorgang bezüglich Audits und neuen Regelungen

- 1. Basis schaffen: Härtungsregeln und Prozesse
 - Unterstützung im Internet, um Härtungsregeln zu definieren:
 - Center for Internet Security → Security Benchmarks für Datenbanken auch für Oracle
 - → Qualitätsverbesserungen durch Mitwirken von u.a. Alexander Kornbrust (Security Consultant)

- 2. Erweiterung um PCI Anforderungen
 - PCI DSS Regeln:
 - aktuelle Version 2.0 bis 31. Dezember 2014 aktiv und gültig
 - ab November 2013 neue Version 3.0 mit zahlreichen neuen Unteranforderungen



> Agenda

- ▶ Vorstellung LH Systems AG
- ▶ Definition PCI DSS
- ▶ Voraussetzung / abgesteckter Rahmen
- ▶ Der Einstieg
- ▶ **Härtung der Datenbank nach PCI DSS Anforderung**
- ▶ Knackpunkte
- ▶ Zusammenfassung



> Härtung der Datenbank nach PCI DSS Anforderung

- **Anforderung 2:**
Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden
- Änderung von:
 - Standardpasswörter aller Oracle internen Benutzer (dba_users_with_defpwd)
 - Standardeinstellungen wie Listenerport 1521 und Datenbankname ORCL
- Demo- oder Testschemas löschen und nicht benötigte Features nicht installieren
- Nichtkonsolen-Verwaltungszugriffe mittels starker Verschlüsselung (SSH, VPN, SSL/TLS)
- keine Remote SQLNET Verbindung außer bei Oracle Advanced Security Option (ab 11.2.0.4 inklusive).



> Härtung der Datenbank nach PCI DSS Anforderung

- Entsprechende Sicherheitsparameter setzen:
- `07_DICTIONARY_ACCESSIBILITY=FALSE`
Erlaubt sonst Zugriff auf Objekte im SYS Schema durch die EXECUTE ANY PROCEDURE und SELECT ANY DICTIONARY Berechtigung
- `REMOTE_LOGIN_PASSWORDFILE=NONE`
Passwortfile beim Login benutzt oder nicht und welche DBs dieses nutzen
- `SEC_CASE_SENSITIVE_LOGON=TRUE`
Speicherung der Passwörter „case sensitive“
durch Schwachstelle (CVE-2012-3137) (CPU/PSU Oktober 2012 behoben) konnten Passwörter geknackt werden



> Härtung der Datenbank nach PCI DSS Anforderung

- `SEC_MAX_FAILED_LOGIN_ATTEMPTS=6` (Vorgabe durch PCI DSS 2.0)
wie oft man sich mit falschem Passwort einloggen darf, bevor Oracle die Verbindung kappt
Überschreiben der Einstellung durch Zuweisen von Profilen an die Benutzer
- `SEC_RETURN_SERVER_RELEASE_BANNER=FALSE`
liefert die Information der Release- und Patchnummer
Angreifer kann Schwachstellen der jeweiligen Releases ausnutzen
- `REMOTE_LISTENER=''`
sollte nicht gesetzt sein, da sonst Spoofing Verbindungen möglich



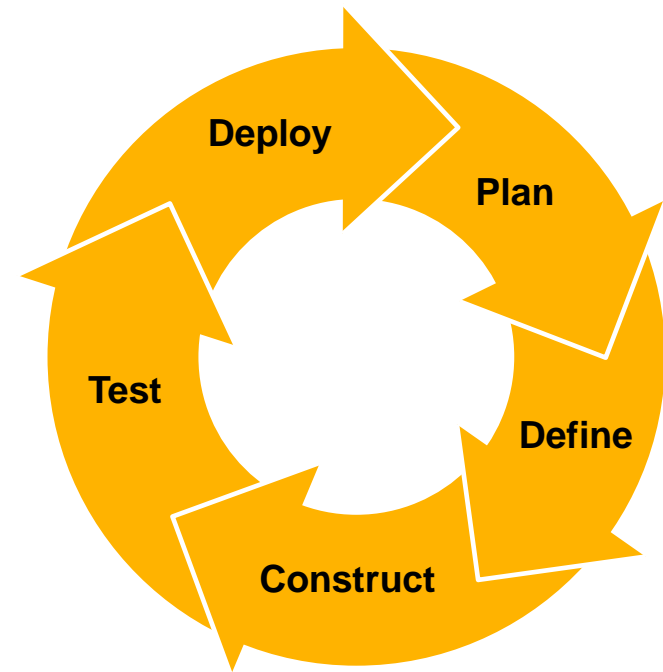
> Härtung der Datenbank nach PCI DSS Anforderung

- PUBLIC hat mehr als 10.000 Rechte
 - jeder Benutzer, der angelegt wird, erbt diese Privilegien
 - Wichtig: Entfernen von Ausführungsrechten von PUBLIC auf Objekte und Pakete (in Absprache mit Applikation)
 - Benutzerberechtigungen einschränken (auch Oracle interne Benutzer)
 - Motto: "So wenig wie möglich und so viele wie nötig" (ANY, DBA-Rechte)
 - Oracle 12c bietet Privilege Analysis (Database Vault)
-
- Listener sicher konfigurieren:
 - `ADMIN_RESTRICTIONS_<listener_name>=ON`
Änderung des aktiven Listeners nur in listener.ora mit Restart
 - `SECURE_REGISTER_listener_name=IPC/TCPS`
Einschränkung der Protokolle, die sich auf Listener verbinden dürfen



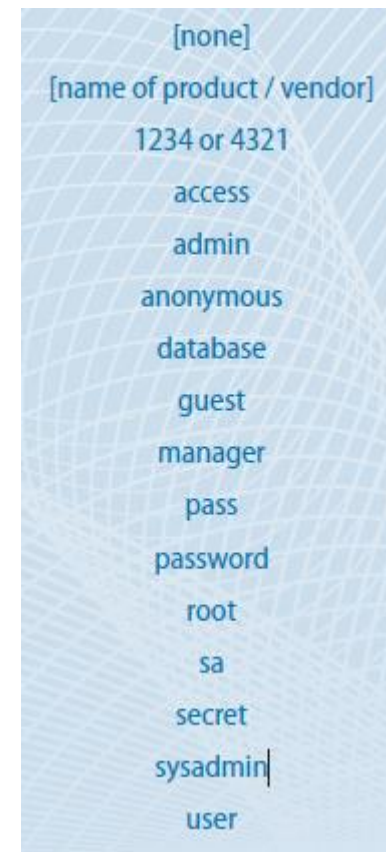
> Härtung der Datenbank nach PCI DSS Anforderung

- **Anforderung 6:**
Entwicklung und Wartung sicherer Systeme und Anwendungen
- "Always patch a running system if necessary"
- Immer auf dem neuesten Stand bleiben (Release/PSU/Sicherheitspatches)
- Einspielen innerhalb von 30 Tagen
- Prozess und Beschreibung
- Prüfung mit:
`SELECT * FROM DBA_REGISTRY_HISTORY;`



> Härtung der Datenbank nach PCI DSS Anforderung

- **Anforderung 8:**
Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
- Personalisierung in der Datenbank oder auf andere Art (OS-Ebene)
- jeder Datenbankadministrator hat eigenen Benutzer
- kein Sammelaccount → "/" as sysdba" für den Betrieb nur im Notfall anwendbar
- Passwortauthentifizierung
- Passwort Verify Funktion → sichere Passwörter
- Profile einrichten (Reuse Max, Idle Time, Expire Time, Password Lock Time, Failed Login Attempts) und Benutzern zuweisen

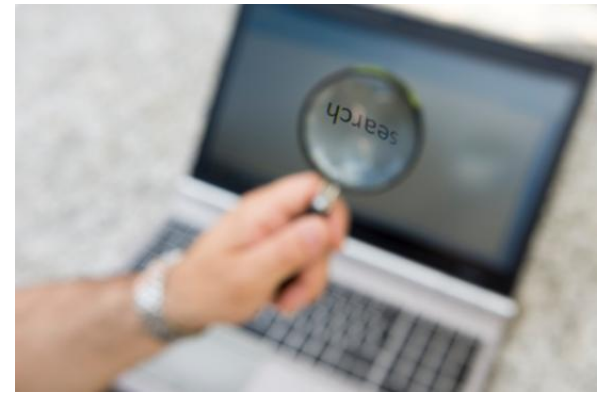


> Agenda

- ▶ Vorstellung LH Systems AG
- ▶ Definition PCI DSS
- ▶ Voraussetzung / abgesteckter Rahmen
- ▶ Der Einstieg
- ▶ Härtung der Datenbank nach PCI DSS Anforderung
- ▶ **Knackpunkte**
- ▶ Zusammenfassung



> Knackpunkte - Auditing



- **Anforderung 10:**
Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
- Automatisierte Audit-Trails zur Rekonstruktion folgender Ereignisse:
 - Alle individuellen Zugriffe auf Karteninhaberdaten
 - Alle Aktionen von einer Einzelperson mit Root- oder Administratorrechten
 - Zugriff auf die Audit-Trails
 - Ungültige logische Zugriffsversuche
 - Verwenden von Identifizierungs- und Authentifizierungsmechanismen
 - Initialisierung der Audit-Protokolle sowie das Erstellen und Löschen von Objekten auf Systemebene
- Audit-Trails müssen enthalten:
BenutzerID, Ereignistyp, Datum und Uhrzeit, Angabe von Erfolgen oder Fehlern, Ereignisursprung, Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen
- Schutz der Audit-Dateien vor Veränderungen, Zugriff einschränken, möglichst schnelle Sicherung auf zentralen Protokollserver



> Knackpunkte - Auditing

- Viele Anforderungen
 - umsetzbar mit einigen Hürden (auch ohne Oracle Audit Vault)
- "Die Kombination macht es"
- Angefangen mit privilegierten Benutzern:
 1. SYSDBA und SYSOPER Auditing
AUDIT_SYS_OPERATIONS=TRUE
 2. Loggen in das Syslog Log
AUDIT_TRAIL=OS
 3. Empfangskanal für Syslog Deamon
AUDIT_SYSLOG_LEVEL=LOCAL2.WARNING.



> Knackpunkte - Auditing

- Auditieren von normalen Benutzern:
- "Normales" Auditing loggt nicht alle Informationen mit (SQL Statement fehlt)
- Trick:
AUDIT_TRAIL=XML, EXTENDED
- alle wichtigen Informationen zu Benutzern und deren Statements → nicht an den SYSLOGD
- Erzeugung von XML Dateien
- AUDIT_DUMP_DEST geeignet definieren → eigenes Filesystem
- Beachtung der Berechtigung der Dateien (nur von Oracle Software Owner beschreibbar)
_TRACE_FILES_PUBLIC=FALSE (default)



> Knackpunkte - Auditing

- Was heißt das im Umkehrschluss?
- 1. Einschränken des Oracle Software Owner in seiner Benutzung
- 2. „/ as sysdba“ (Sammelaccount) darf nicht benutzt werden → Nachvollziehbarkeit „gestört“
- 3. zusätzlichen eingeschränkten Benutzer für den normalen Betrieb einsetzen
 - kann nicht die XML Dateien manipulieren
 - Prozessbeschreibung/Konzept
- 4. Schnellstmöglicher Transfer der XML Dateien auf zentralen Protokollserver
 - Eingeschränkten Share an Betriebssystem mounten (nur von root zugreifbar)
 - Dateien dorthin zeitnah verschieben
- 5. Zentraler Protokollserver muss XML Dateien auswerten können z.B. von ArcSight (SmartConnector for Oracle Audit XML Connector)



> Knackpunkte - Auditing

- 6. Einstellen des AUDIT

AUDIT SELECT TABLE,INSERT TABLE,UPDATE TABLE,DELETE TABLE BY USER;

- 7. Prüfung der Auditeinstellungen:

SELECT * FROM DBA_STMT_AUDIT_OPTS where audit_option in ('SELECT TABLE','INSERT TABLE','UPDATE TABLE','DELETE TABLE');

- Ausblick Oracle 12c Unified Auditing (SYSLOGD wird nicht mehr bedient)



> Knackpunkte - FIM

- Dateiintegritätsüberwachung
- Linux → SAMHAIN

- Erkennung von Veränderung an statischen Dateien
- Programm-, Bibliotheks-, Skript- und Konfigurationsdateien

- Ausnahme: ständig ändernde Dateien wie Protokolldateien, Datenbank Datendateien

- Erstellung einer Prüfsummendatenbank bei initialen Installation
- Aktualisierung nach jedem Softwareupdate
- Regelmäßige Überprüfung gegen Datenbank
- Schutz der FIM-Prüfsummendatenbank selbst
- Bei Abweichungen der gespeicherten Prüfsummen
- Ereignisse an zentralen Protokollserver



> Knackpunkte - SIEM USE CASES

- Definition von verdächtigen und auffälligen Events
 - Alarm auslösen
- Beispielsweise:
 - Benutzer ändert einen Datenbankparameter
 - Benutzer legt einen anderen Benutzer an
 - Verschiedene Möglichkeiten: create user, grant user identified by
- Konfiguration beliebig erweitern
- Beispiele des Identitätswechsels ohne Passwort:
 - DBMS_SYS_SQL (undokumentiert), DBMS_IJOB (undokumentiert)
 - sys.kupp\$proc (undokumentiert), Alter User su (feature)
 - Proxy User (feature), Any Procedure (feature)
 - Become User (feature), KUPP_PROC_LIB (undokumentiert)
- in Oracle 12c Auditieren von oradebug möglich



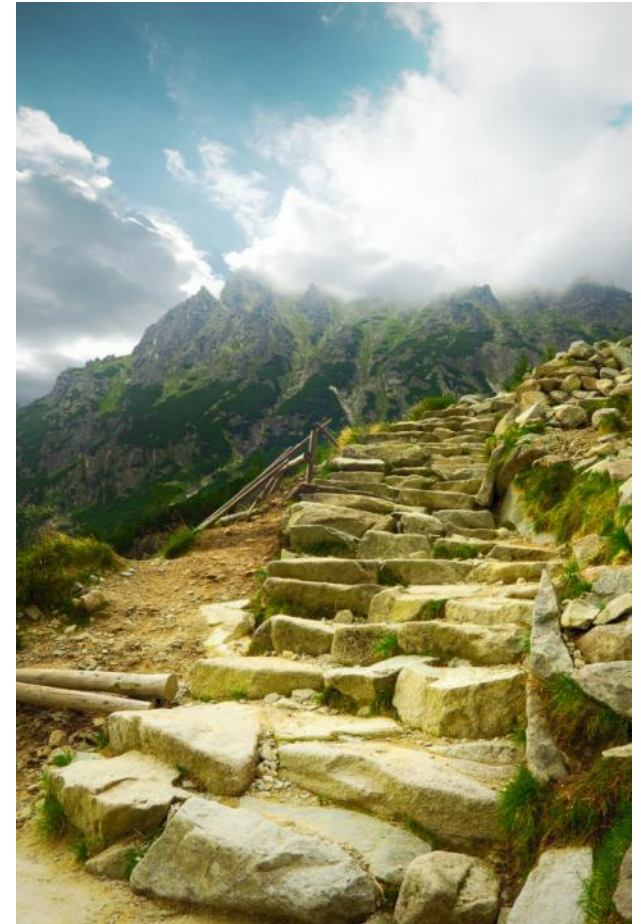
> Agenda

- ▶ Vorstellung LH Systems AG
- ▶ Definition PCI DSS
- ▶ Voraussetzung / abgesteckter Rahmen
- ▶ Der Einstieg
- ▶ Härtung der Datenbank nach PCI DSS Anforderung
- ▶ Knackpunkte
- ▶ **Zusammenfassung**



> Zusammenfassung

- "Dieser Weg wird kein leichter sein!"



> Danke für Ihre Aufmerksamkeit! Fragen?



11. Februar 2014



Lufthansa Systems

IT that makes your life easier