Ein Weg zur sicheren Datenbank – mit BSI IT-Grundschutz und Oracle Best Practice

Marion Stößer

14.4.2015, Mannheim

KTBL

Agenda

- BSI IT-Grundschutz (ISMS)
- Die Bedrohung von außen: System und Datenbank härten
- Die Sicht von innen: Benutzer, Verschlüsselung und Integrität
- Die Organisation: Administration, Kontrolle und Sensibilisierung
- Fazit

BSI IT-Grundschutz – Welche Werte? Welcher Schaden?

- Zu schützende Grundwerte
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
- Weitere Werte
  - Rückverfolgbarkeit
  - Nachvollziehbarkeit
- Schadensfälle
  - „Compliance“ Verstoß gegen Gesetze, Regularien, Normen, Bescheide, Verträge, Lizenzen (BDSG, PCI DSS)
  - Imageschaden
  - Möglicher finanzieller Schaden

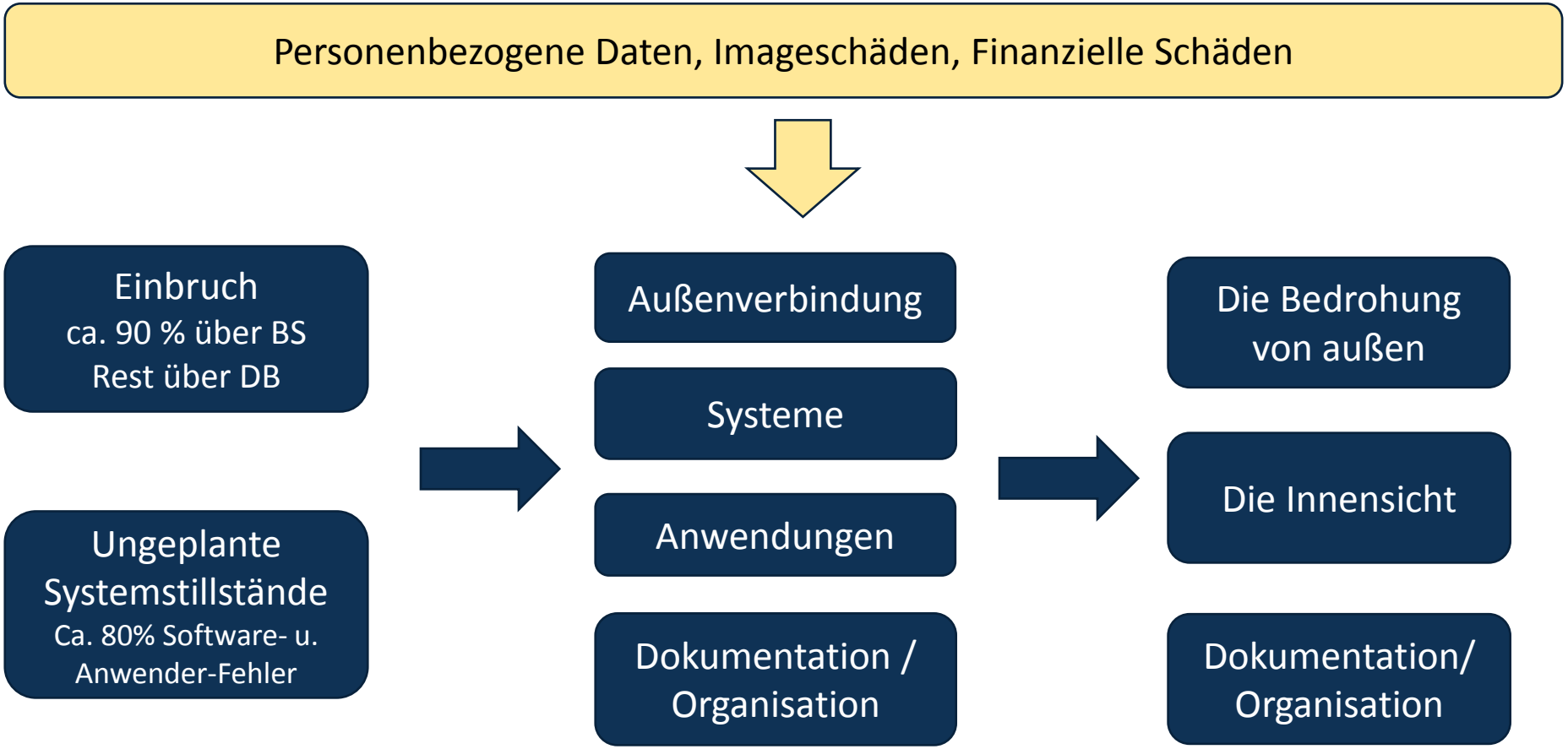
BSI IT-Grundschutz – Welche Gefahren? Welche Maßnahmen

- Schutzbedarfsanalyse
  - Was geschieht wenn DB nicht verfügbar?
  - Was kann geschehen, wenn Unbefugte an diese Daten gelangen?
  - Was passiert wenn Daten manipuliert werden oder auf sonstige Art inkonsistent werden?
- Baustein B 5.7 Datenbanken
  - Gefährdungen
  - Die Maßnahmen sind generischer Natur und über alle Bausteine gleichförmig strukturiert:

    Planung und Konzeption, Beschaffung, Umsetzung, Betrieb, Notfallvorsorge

BSI IT-Grundschutz – Welche Maßnahmen? Welche Reihenfolge?

- Prioritäten in der Umsetzung



Die Bedrohung von außen - Überblick

- System härten
  - Architektur
  - Verschlüsselung der Datenkommunikation
  - Passwörter
- Datenbank härten
  - SQL Injektion
  - DB Links
  - Festlegen von Obergrenzen für Ressourcen

Die Bedrohung von außen – System härten

- M 5.117 Integration in Sicherheitsgateway (-> IT-Architektur)
  - Datenbankserver in eigene DMZ
- Der Listener
  - Zugriff auf bestimmte Rechner einschränken
  - Protokolle, die nicht verwendet werden entfernen
- M 4.72 Datenbank-Verschlüsselung (-> Datenkommunikation)
  - Nativ über SQL*Net (sqlnet.ora)
  - SSL (Advanced Security Option, Zertifikate, Wallet,…)
- M 4.7 Änderung voreingestellter Passwörter

  bei BS und Datenbank
  - keine trivialen Passwörter verwenden (siehe Zugang-Authentifizierung)
  - nicht über alle Instanzen/Server dieselben Passwörter
  - Personalisierte User einsetzen

  Oracle
  - Metadaten-view dba_users_with_defpwd
  - Verzögertes Login (ab Oracle 11g init-Parameter sec_max_failed_log_attempts)
  - User-Profile setzen (Parameter: failed_login_attempts)

Die Bedrohung von außen – Datenbank härten

- M 2.363 SQL-Injektion

  Finde ‚anfällige Prozedur'

  Über Rückgabewert oder Fehlermeldungen der Funktion, kann der Angreifer Informationen über DB sammeln

  Proceduren haben per Default alle Rechte des Schema.

  Beim Anlegen kann invoker_right_clause/ definer's right gesetzt werden

  Bis Oracle 10: Netzwerkzugriffe aus DB sind per deafult möglich

  Utl_tcp, utl_smtp, utl_mail, utl_http, utl_inaddr
  Ab 11 Access Control List (ACL)

  ⇒Software-Entwicklung

  - Applikation darf keine Fehlermeldung nach Außen geben, die Rückschlüsse auf verwendete Systeme erlauben
  - Verwende stored Procedure mit bind variablen und concatiniere nicht den Inhalt
    Kein grant execute/select on XYZ to public
  - Datentyp explizit festlegen
  - Überprüfe ob die übergebenen Daten dem erwarteten Datentyp entsprechen
  - Von besonderen Zeichen bereinigen:
  - Hochkommata, Slash und Backslash, Semikolon, NULL, Zeilenvorschub und Zeilenumbruch

Die Bedrohung von außen – Datenbank härten

- M 4.67 Sperren und Löschen nicht benötigter DB-Accounts

  Auffinden installierter und verwendeter Oracle-Komponenten

  v$option, dba_registry, dba_feature_usage_statistics

  Schema löschen bzw. Sperren

  1. Löschen
  2. User Status auf expired und locked setzen
  3. User Passwort ungültig machen

  Package ‚sperren`: Revoke execute from public

- B 1.14 Patch- und Änderungsmanagement – Einspielen von Patches
- M 4.71 DB-Links
  - Nur DBA sollte Recht haben dblinks anzulegen (vor oracle 10 in Rolle Connect enthalten)
  - Keine public DB Links verwenden
- M 4.73 Festlegen von Obergrenzen für Selektionen (-> Ressourcen)
  - Ressource über User profile steuern
  - User temporären tablespace zuweisen, Default temp. Tablespace festlegen

Die Sicht von innen - Überblick

- Benutzermanagement
- Authentisierung – Zugang
- Autorisierung – Zugriff
- Datenverschlüsselung
- Integrität

Die Sicht von innen – welche Benutzer? welche Anwendung/DB?

- M 2.132 Regelungen für die Einrichtung von Datenbankbenutzern

  Benutzertypen – Rechteprofile:
  - Administrator / DBA,
  - Applications User / Technischer User,
  - Enduser / persönlicher User

- M 2.128 Zugangskontrolle

  Passwortmanagement
  - Passwörter über User profile steuern Einstellung pro Benutzertyp

    Password_lifetime, password_reuse_xx, password_grace_time, passwort_lock_time
  - Passwortkomplexität:

    Passwortprüfunktion kann Profile zugewiesen werden (Parameter: passwort_verify_function)
    Ab 11g Unterscheidung Groß und Kleinbuchstaben (init-Parameter SEC_CASE_SENSITIVE_LOGON=FALSE/TRUE)

  Authentifizierungsmethoden

  Datenbank-Authentifizierung, single sign on, secure Socket Layer(SSL), Secure External Passwort Store (wallet), Oracle Key Vault

Die Sicht von innen: welcher Benutzer? Welche Daten?

- M 2.129 Zugriffskontrolle – Autorisierung

  Datenbankobjekte eindeutig einem Schema zugeordnen
  - Vermeidung von public Synonym / private synonym

  Schutz der Daten: System- und Objektprivilegien werden an Rollen vergeben, Rollen an Benutzer
  - Nur Privilegien vergeben die benötigt werden
  - Any Rechte nur wenn notwendig

  Trennung von Daten und Funktionalitäten
  - Verwendung von Views und Prozeduren

  Oracle spezifisch
  - Access Control Lists (ACL) für Netzwerk-Callouts (Ab Oracle 11g)
    davor freier Zugriff auf Packes Utl_tcp, utl_smtp, utl_mail, utl_http, utl_inaddr
  - Oracle Database Vault (verhindert das DBA Anwendungsdaten sieht)

- M 2.129 Inferenzprävention

  Zugriffsberechtigung Tabellen/Spalten
  - Virtual Private Database (VPD)
  - Fine Grained Access Control (FGAC) (Ab Oracle 11g)
  - Oracle Label Security

Die Sicht von innen: korrekte Daten, versteckte Daten

- M 2.130 Integrität

  Einsatz von Constraints

  Rückverfolgbarkeit
  - Wer macht wann ein insert, update oder delete?
  - Was war der alte Wert, was der neue Wert
  - Trigger based auditing: dml-trigger

- M 4.72 Verschlüsselung

  Gespeicherte Daten prozedural oder deklarativ verschlüsseln
  - Prozedural: dbms_crypto (veraltet dbms_obfuscation_toolkit)
  - Deklarativ: Advanced Security Option(ASO), Tranparent Data Encryption (TDE) (ab Oracle 10g)
  - Data Masking, Data Reduction

Die Organisation – Übersicht

- Administration
- Notfallvorsorge
  - Zur Erinnerung: ungeplante Systemausfälle durch Anwenderfehler
- Kontrolle
  - Siehe unten
- Dokumentation
  - konkrete Vorschläge in BSI Maßnahmen
- Planung, Installation und Konfiguration
- Sensibilisierung
  - der Mitarbeiter, Kollegen, Vorgesetzen und
  - sich selbst
- Patch und Änderungsmanagement
  - Zur Erinnerung: ungeplante Systemausfälle durch Softwarefehler (z.B.: fehlerhafte Updates)

Die Organisation: Kontrolle - Rückverfolgbarkeit

- M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems

  Maßnahmen zur Protokollierung und Auditierung im sinnvollem Umfang

  Trigger Based Auditing

  Mit event-triggern Informationen über connects und disconnect gewinnen

  Fine Grained Auditing

  Engmaschige Kontrolle auf Zeilen und Spaltenebene.

  Oracle Auditing

  Hilfreich bei Sicherheitsbestandsaufnahme und Angriffserkennung samt Forensik

  - Fehlerhafte Datenbank-Logins (audit create session whenever not succesful)
  - Hochprivilegierte Datenbank-Aktivitäten der sysdbas protokollieren (Init.ora Parameter audit_sys_operations=TRUE
  - Create, drop und alter Operationen auf table, index, procedure, trigger, directory, public snymonm und profil

Die Organisation: Kontrolle – Status Quo DB

- M 4.70 Durchführung einer Datenbanküberwachung
  - Datenfragmentierung,
  - Datenvolumen und Füllgrad
  - Auslastung der Datenbank
- M 4.69 regelmäßige Sicherheitschecks

  Security Checklisten:
  - CIS Benchmark – basiert auf Buch Oracle Security Step-by-Step von Pete Finnigan und anderen 2003
  - Oracle Security Checklist – allgemeine Zusammenfassung von Hinweisen und Best Practice

  Eigene Scripts für
  - installierte und verwendete Komponenten
  - Profile, Rollen , Privilegien, Synonyme, DB-Links, user public
  - Etc.

  Tool basiert:

  Enterprise Manager – Configuration Management Pack enthält Regelbibliothek

Fazit: produktspezifisch - generisch

- Oracle Community
  - Neue Features und aktuelle Bedrohungen stehen im Vordergrund
  - ‚altes'- ist nicht so leicht zu finden
  - Schwerpunkt bei Administrationsthemen
  - Viele Praxis-Tipps für konkrete Umsetzung
- BSI Bausteine
  - Allgemeiner Leitfaden: von Architektur bis Integrität
  - Konkrete Empfehlungen für Dokumentation und Organisation
  - Weiterführende Bausteine: Sensibilisierung, Patch- und Änderungsmanagement; Protokollierung, Datensicherung, etc.

Fazit: Secuity-Lifecycle

- Regelmäßige Checks der umgesetzten Maßnahmen
- Sensibilisierungsmaßnahmen
- Notfallübungen (Know How Aufbau und halten)
- Regelmäßige Revision der Umsetzung
  - Was ist noch / jetzt relevant?
  - Was ist absolutes Muss?
  - Was bringt viel mit wenig Aufwand?