Datenbanksicherheit
Überwachung und Kontrolle

Dr. Ing. Oriana Weber
07/06/2011

Agenda

- Leitfragen
- Warum sind Datenbanken attraktive Ziele?
- Klassifizierung von DB Sicherheitsrisiken
- Die Komplexität der Steuerung und des Schutzes von Datenbanken
- Best Practices für Datenbank-Sicherheit
- Der Datenbank-Sicherheit Zyklus
- Überwachung der Datenbank-Sicherheit
- Live Demo

Leitfragen

- **Wissen Sie wo alle Ihre Datenbanken sind?**
  - Neue Anwendungen
  - Test & Dev
- **… und wissen Sie welche Datenbanken vertrauliche Informationen speichern?**
  - Besonders diejenigen, die der Einhaltung gesetzlicher Vorschriften unterliegen
- **können Sie die notwendigen Berichte an Auditoren geben?**
- **… und wie sicher sind Ihre Datenbanken?**
  - Version/Patch Level
  - Die häufigsten Konfigurationschwächen:
  - Passwörter, geteilte Kennwörter, unsicherer Code, Backdoors, etc.

Warum sind Datenbanken attraktive Ziele?

sentrigo

McAfee

- Handel mit Datenbanken
  - Hohe Werte von digitalen Informationen
  - Wert von mehreren Milliarden Dollar pro Jahr
  - Legal oder illegal?

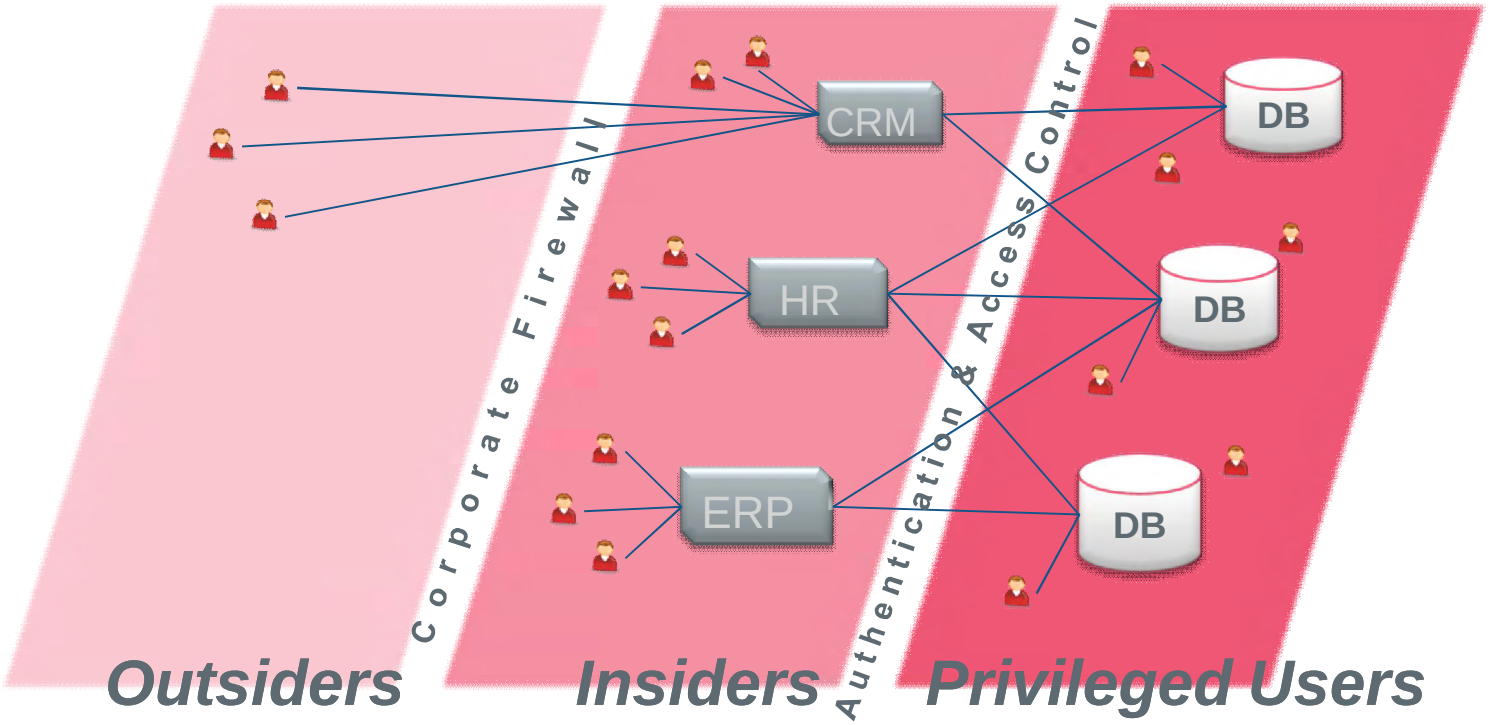
- Der Fall von “Darkmarket” (2008).
  - Die Seite hat drei Jahre bestanden
  - Handel von Kreditkarten-Daten
  - Austausch von Informationen für Computer-Betrug
  - In 6 Wochen wurden US $431,000 verdient, langfristig wären bis zu 20 Mio. möglich gewesen
- Der Fall von “**H**aupt-**S**chweizer **B**ank” (2009-2010).
  - Diebstahl einer DB mit Daten zu ca. 15000 Schweizer Bankkonten
  - Angebot der deutschen Regierung: US$3,5 Mio; US$500 Mio an hinterzogenen Steuern könnten eingefordert werden
  - Der Mann wird von der französischen Regierung geschützt

Klassifizierung von DB Sicherheitsrisiken (1/2)

- Vulnerabilität: Sicherheitslücke im Code eines DBMS
- Audit-Kontrollen: Fehlen von Audit-Kontrollen
- Konfiguration: Konfigurationsvariablen
- Programmierung: Vulnerabilität (Buffer overflow, SQL injection, etc.)
- Authentifizierung: Nutzer - Authentifizierung
- Datenübertragung: „Verpackungsmethoden“ von Daten die zwischen Datenbankserver und Benutzeroberfläche ausgetauscht werden

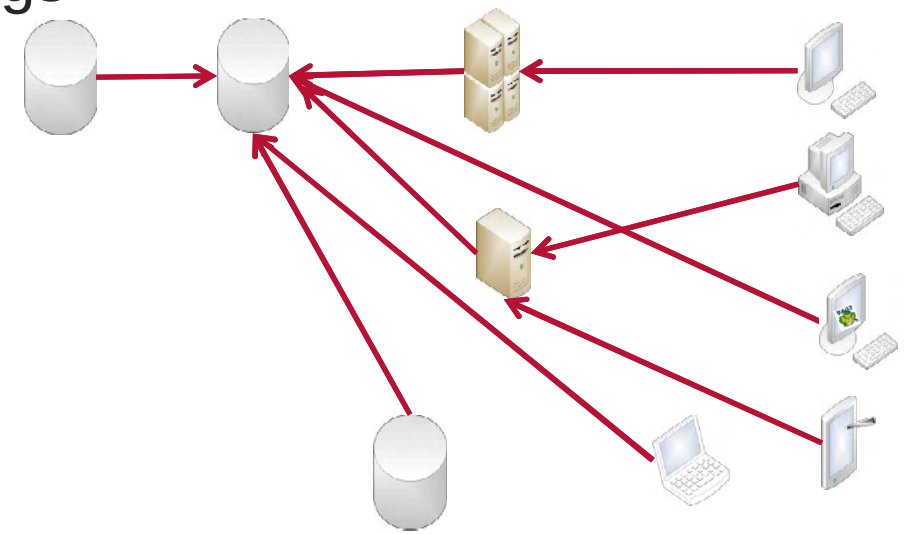
Klassifizierung von DB Sicherheitsrisiken (2/2)

- Malware (Backdoors, Rootkits)
- Gestohlene Backup-Bänder und Festplatten
- Keine Überwachung des Zugangs und Transaktionen der Datenbank in Echtzeit



Die Komplexität der Steuerung und des Schutzes von Datenbanken

- Normalerweise erfolgt die Veröffentlichung (im Internet) der neuen Schwachstellen und neuen Formen des Angriffs schneller als die Veröffentlichung der Lösungen
- Kein Monitoring von Zugriffen und Transaktionen in Echtzeit
- Variierende Anzahl von Servern und Instanzen
- Data-Flow-Modell ist nicht einheitlich
- Die Informationen werden kontinuierlich repliziert
- Verschiedene Formen des Zugangs
- Patch Update



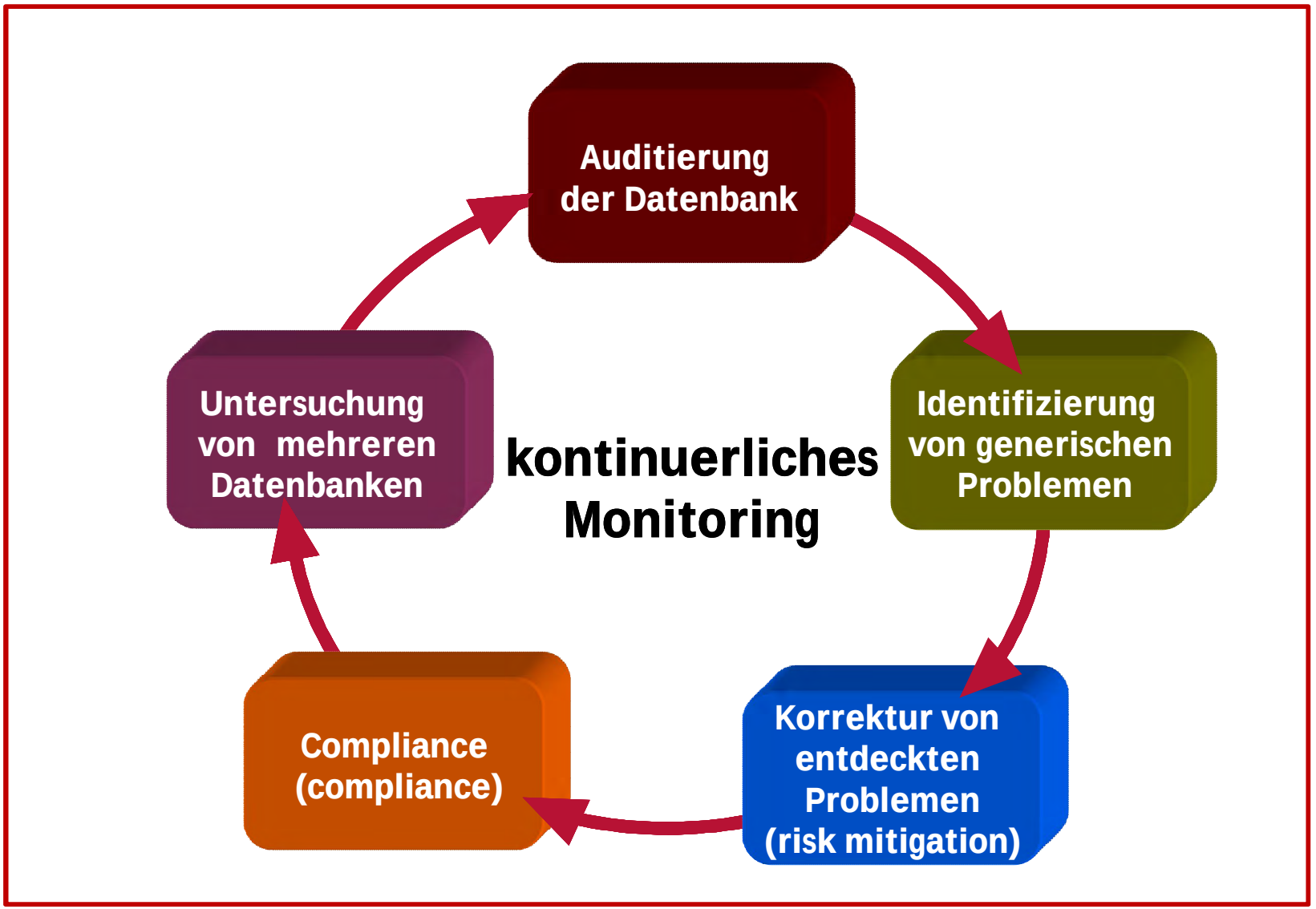
Best Practices für Datenbank Sicherheit

1. Mapping und Documenting der DB Servern
2. Änderung der Benutzer-Passwörter und Default-Scheme
3. Änderung der Standard-Port der für den Listener des Datenbank-Server definiert ist
4. Kontrolle der Privilegien von aktiven DB Anwendern und den Rollen und Privilegien von DBA, Entwicklern und Super-Usern klar begrenzen
5. Wenn möglich löschen der Stored-Procedures mit Zugriff auf das Betriebssystem von der Datenbank

Best Practices für Datenbank Sicherheit

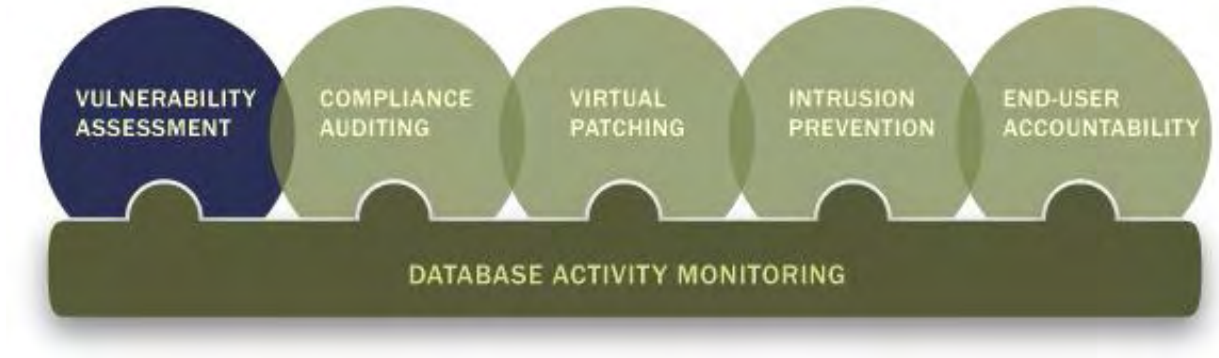
6. Definition von Passwort-Sicherheitsrichtlinien für Datenbankanwender
7. Vermeiden Sie Embedded-Passwörter (| Info. verschlüsseln)
8. Beseitigen der Gefahr von SQL-Injection (verm. || & ‘’)
9. Behalten Sie Ihre RDBMS aktualisiert und gepatcht
10. Besuchen Sie regelmäßig die Sicherheits-Website Ihres RDBMS-Herstellers
11. Regelmäßige Prüfung des Sicherheitsstatus Ihrer Datenbanken (DB-Audit)

Der Datenbank-Sicherheit Zyklus



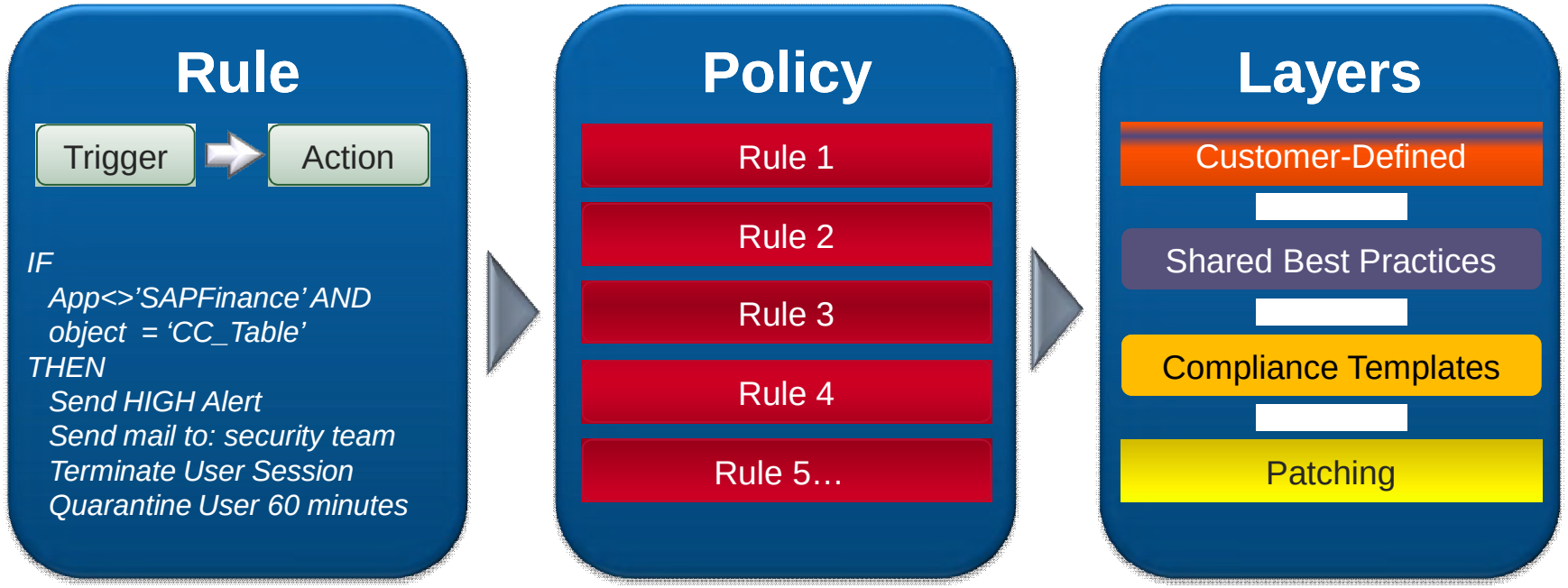
Überwachung der Datenbank-Sicherheit

- Für eine wirksame Überwachung:
  - Definition der Phasen der normalen Aktivitäten in der Datenbank: Benutzer-, Datenbank-Objekte, Sitzungen
  - Defininiton von Sicherheitspolitiken
  - Implementierung der aktuellen Patches
  - Umsetzung der internationalen und nationalen Standards für Informationssicherheit
  - Mapping von Zugriffen auf die Datenbank in Echtzeit



Definition von Regeln

- Die Definition von Folgendem ist nötig:
  - Richtlinien (Regeln)
  - Sicherheitspolitiken, welche den internen oder internationalen Vorschriften folgen



Erfüllung der Anforderungen der Datenschutzgesetze

Gesetz	Anforderungen	Sicherheitspolitik
Datenschutzgesetz(LOPD). Sicherheitsmaßnahmen - verordnungen, § 98 Identifizierung und Authentifizierung	Der verantwortliche Daten-Controller soll einen Mechanismus definieren , der die wiederholten Versuche begrenzt, wenn es ein en unerwünschten oder unauthorisierten Zugriff auf das Informationssystem gibt.	LOPD.RMS.A98.AI. Die nicht autorisierten Zugriffsversuche sollten blockiert werden. Regel: Wird der Zugriff nicht gestattet ,dann sollte er blockiert werden und die jeweillige Informationen sind zu speichern
Datenschutzgesetz (LOPD). Sicherheitsmaßnahmen-verordnungen, § 103. Sicherheitsmaßnahmen bei der Behandlung von persönlichen Daten (3)	Die Mechanismen, die das Zugriffsprotokoll ermöglichen sollen unter der direkten Kontrolle des zuständigen Sicherheitsverantworlichen sein, ohne dass die Deaktivierung oder deren Manipulation möglich ist.	LOPD.RMS.A103.3.MSTDCP. Nur der Administrator überwacht die Aufzeichnungen des Zugangs zu personenbezogenen Daten. Die Aufzeichnungen dürfen nicht deaktivierrbar oder manipulierbar sein. Regel1: Alle Zugriffe zu den persönlichen Daten sollten gespeichert werden. Regel 2: Profile die nur die Informationen lesen können sollten definiert werden
Datenschutzgesetzes (LOPD). Sicherheitsmaßnahmen-verordnungen, § 103. Sicherheitsmaßnahmen bei der Behandlung von persönlichen Daten (5)	Der Sicherheitsbverantworliche sollte mindestens einmal im Monat Auditinformationen nachprüfen und sollte einen Bericht mit den identifizierten Problemen und Prüfungen erstellen	LOPD.RMS.A103.5.MSTDCP. Eine Überwachung der gespeicherten Informationen sollte gemacht werden und die identifizierten Probleme solltenin einem Bericht beschrieben werden.

Live Demo

- Wie kann Hedgehog Enterprise Sie unterstützen ?

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Kontakt: orianaw@sentrigo.com

orianay.weber@googlemail.com