DB520 Oracle Security

Kurzbeschreibung:

Das Training **DB520 Oracle Security** ist für ORACLE-Administratoren konzipiert, die für die Sicherheit der Oracle-Systeme zuständig sind.
In diesem Workshop zeigen wir Ihnen potenzielle Sicherheitsschwachstellen auf und erarbeiten Lösungsansätze in praxisorientierten Übungen.
Nach dem Training sind Sie in der Lage, Daten vor unberechtigtem Zugriff zu schützen und in der Datenbank sowie im Netz zu verschlüsseln. Außerdem können Sie dafür sorgen, dass Applikationen Daten, je nach Berechtigung, individuell präsentieren.

Zielgruppe:

Der Workshop **DB520 Oracle Security** richtet sich an Oracle Administratoren, die für die Sicherheit der Oracle Systeme zuständig sind.

Voraussetzungen:

Um dem Lerntempo und Inhalten des Kurses **DB520 Oracle Security** gut folgen zu können, sind tiefergehende Kenntnisse der Oracle Verwaltung erforderlich.

Alternativ empfehlen wir vorab den Besuch des Oracle Trainings:

- DB201 Oracle Admin Basics

Sonstiges:

Dauer: 4 Tage

Preis: 2090 Euro plus Mwst.

Ziele:

- Sie erkennen Sicherheitsschwachstellen in Ihrem Oracle Datenbanksystem und sind in der Lage, diese zu beheben.
- Sie können individuelle Berechtigungen je nach Anforderung konfigurieren.

Inhalte/Agenda:

- **Rechtliche Einordnung**
  - Grundzüge BSI
  - Bundesdatenschutzgesetz (BDSG)
  - Datenschutzgrundverordnung (DSGVO)
  - KRITIS

- **Auditing**
  - Formen (Mandatory, SYS, Standard)
  - trigger-basierendes Auditing
  - Fine-Grained Auditing
  - Oracle Audit Vault
  - Unified Auditing

- **Autorisierung (Datenzugriffskontrolle)**
  - Rollenkonzept
  - Privilegien
  - AccessControlListen und AccessControlEntries für Freigaben über das Netzwerk
  - Code Based Security

- **Identifizierung und Authentifizierung**
  - Benutzer- und Passwortverwaltung (Passwortschutz, -policies, -komplexität)
  - OS-authentifizierte Benutzer
  - Kennwortdatei
  - Secure External Password Store
  - Single-Sign-On Komponente Kerberos-Verschlüsselung: Client-Methoden (DBMS_CRYPTO, DBMS_OBFUSCATION_TOOLKIT(bis 19c))
  - Transparent Data Encryption auf Spalten-, Tablespace-Ebene, Keystore-Management (bis 11g Wallet)
  - Backup und Dumpverschlüsselung

- **Absicherung der Datenübertragung**
  - Absicherung des Listener
  - Connection Manager
  - native Verschlüsselung des SQL*Net-Verkehrs
  - Secure Sockets Layer

- **Überprüfen von Sicherheitslücken**
  - SQL Injection
  - Datenbank-Links
  - Trigger-Sicherheit
  - Initialisierungsparameter

- **Virtual Private Database und Fine Grained Access Control (FGAC)**

- **Unterdrückung der Ausgabe sensibler Dateninhalte durch Data Redaction**

- **Direkte Anbindung einer Oracle-Datenbank an das Active Directory (AD)**

- **Identifikationen von Schwachstellen mit DBSAT (Database Security Assessment Tool)**

- **Leitfaden zur Erstellung eines Security Handbuchs**

- **Add-Ons**
  - Anonymisierung von Daten mittels Data Masking