DB520 Oracle Security

Kurzbeschreibung:

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

Zielgruppe:

Oracle Administratoren, die für die Sicherheit der Oracle Systeme zuständig sind.

Voraussetzungen:

Um dem Lerntempo und Inhalten des Trainings **DB520 Oracle Security** gut folgen zu können, sind tiefergehende Kenntnisse des Betriebssystems Unix oder Windows nötig.

Kenntnisse der Oracle Verwaltung oder Teilnahme am Seminar Oracle Admin Basics (DB201) sind zu empfehlen.

Sonstiges:

Dauer: 4 Tage

Preis: 2090 Euro plus Mwst.

Ziele:

Nach Ende des Trainings ORACLE Security erkennen Sie Sicherheitsschwachstellen in Ihrem Oracle Datenbanksystem und sind in der Lage, diese zu beheben.
Zudem können Sie eigenständig 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, Access-Control-Listen für Netzwerk-Callouts, 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), Transparent Data Encryption auf Spalten-, Tablespace-Ebene, Keystore-Management (bis 11g Wallet), Secure File LOBs, 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)
- Leitfaden zur Erstellung eines Security Handbuchs
- **Add-Ons:** Anonymisierung von Daten mittels Data Masking