

Checkliste Datenbankhärtung

Passwörter	OK?
1. Sind alle Standardpasswörter geändert?	()
2. Sind alle nicht benötigten Standardbenutzer gesperrt?	()
3. Sind Regeln für gültige Passwörter über <i>password verify function</i> definiert?	()
4. Werden starke Authentifizierungsmechanismen eingesetzt? z.B. Kerberos, RADIUS, SSL, PKI (<i>Oracle Advanced Security</i>)	()
Sicherheitspatches	OK?
1. Werden die vierteljährlichen Critical Patch Updates (CPUs) zeitnah eingespielt?	()
2. Werden sonstige sicherheitsrelevante Patches von Oracle eingespielt?	()
Netzwerkzugang	OK?
1. Erfolgt eine Netzwerkverschlüsselung über SSL? (<i>Oracle Advanced Security</i>)	()
2. Nutzen Sie eine zertifizierte Authentifizierung (Clients/Server)? (<i>Oracle Advanced Security</i>) <i>unterstützt die gängigen Verschlüsselungsstandards (AES, 3DES168, DES, RC 4)</i> <i>transparente Datenverschlüsselung (AES bis zu 256 Bit oder 3DES168)</i>	()
Listener	OK?
1. Haben Sie ein Listenerpasswort gesetzt?	()
2. Haben Sie den Listenerstandardports 1521 geändert?	()
Privilegien	OK?
1. Vergeben Sie nur die tatsächlich benötigten Privilegien? (<i>principle of least privilege</i>)	()
2. Existiert eine Zugriffsbeschränkung des Nutzers PUBLIC, v.a. auf bestimmte PL/SQL-Packages (utl_tcp, utl_inaddr)?	()
3. Existiert eine Zugriffsbeschränkung des Privilegs <i>CREATE DATABASE LINK</i> ?	()
4. Gewähren Sie Nutzern nur eine Rolle, wenn er alle Privilegien der Rolle benötigt?	()
Software	OK?
1. Sind die Sample Schemas in Produktionsumgebungen deinstalliert?	()
Aktivierung des Schutzes der Datenverzeichnisse	OK?
1. Sind die Rechte der Oracle Verzeichnisse auf einem Minimum beschränkt?	()
Backup und Disaster Recovery	OK?
1. Ist das Backup verschlüsselt? (<i>Oracle Advanced Security</i>)	()