

Oracle Datenbanksicherheit – Konzepte und Studien zu Risiken und Gefahrenpotential, Software zum Thema Sicherheit

Sorgen Sie aktiv für Sicherheit! Wir bieten Ihnen ein Frühwarnsystem für mögliche Sicherheitslücken, damit die Daten Ihres Unternehmens gut geschützt sind.

Oracle Datenbanken werden in einer Vielzahl von Unternehmen und öffentlichen Einrichtungen zur dauerhaften Speicherung hochsensibler Daten verwendet. Doch nicht immer sind diese Daten so sicher geschützt, wie sie es sein sollten. Lassen Sie Ihre Datenbank von uns prüfen. Wir ermitteln, wo Ihre Datenbank Schwachstellen hat und sagen Ihnen, welche aktiven Sicherheitsmaßnahmen zum Schutz Ihrer Daten ergriffen werden müssen.

Die Einführung von Sicherheitssystemen erschöpft sich nicht in der Installation von Firewalls, die wahren Werte des Unternehmens müssen geschützt werden. Wir sorgen für Datensicherheit. Wir binden ausgewählte Lösungen für höchste Sicherheitsansprüche in ihre Oracle Umgebung ein. Werkzeuggestützt lässt sich die Integrität von Datenbanken täglich testen, um unerwünschte Veränderungen schnell ermitteln zu können.

Wir bieten:

- Analyse Ihrer Datenbank-Schnittstellen
- Analyse Ihrer Datenbank-Konfiguration
- Überprüfung der Einhaltung von Sicherheitsstandards
- Organisatorische Verbesserungsvorschläge
- Werkzeuggestützte permanente Sicherheitsüberwachung

Studien für Ihre Datensicherheit:

Sind Sie sich sicher, dass Sie sicher sind?

Die Netcos AG erstellt Fallstudien über Datenbanken auch in Ihrem Unternehmen. Wir zeigen Ihnen Möglichkeiten auf, wie die Datenhaltung in der Oracle Datenbank empfindlich in ihrer Funktion beeinträchtigt werden kann. Das Wissen über dieses Gefahrenpotential ermöglicht es Ihnen, sich aktiv dagegen zur Wehr zu setzen. Mit den Ergebnissen der Studie erstellen wir für Sie ein Frühwarnsystem zum Schutz Ihrer Daten. Gehen Sie auf Nummer sicher! Testen Sie Ihre Sicherheit, bevor es andere tun.

Oracle Repscan

Repscan ist ein Repository und Vulnerability Scanner für Oracle Datenbanken

Key Features:

- Überprüfen des Oracle Data Dictionaries auf Veränderungen
- Oracle DB Vulnerability Scanner mit über 150 verschiedenen Tests
- Überprüfung von mehr als 600 Default-Passwörtern
- Agentenlose Architektur
- Mit eigenen SQL-Regeln erweiterbar bzw. anpassbar
- Aktualisierte SQL-Regeln durch Updates
- XML-Konfigurationsdateien
- Anpassbare XML/XSL-Reports
- Verwendung bestehender oder eigener Baselines möglich
- Verschlüsselung von SQL-Regeln und Passwörtern möglich
- Command Line Interface
- lauffähig ohne Installation
- lauffähig unter Windows und Linux

Oracle Repscan von unserem Partner, Alexander Kornbrust, ist der erste Security Scanner, der sowohl Datenbanken auf sichere Konfigurationen bzw. Einstellungen hin überprüft, als auch die Integrität des Data Dictionaries mit Hilfe von Baselines vergleicht.

Dadurch lassen sich bestehende Oracle Datenbanken auch nachträglich auf Veränderungen (z.B. Datenbank Rootkits) hin überprüfen.

Repscan wurde von Anfang an auf leichte Erweiterbarkeit, Plattformunabhängigkeit und Usability hin entworfen.

Die Überprüfungen lassen sich mit eigenen SQL-Statements erweitern. XML-Reports sind per XSL-Stylesheet an das Corporate Identity anpassbar und die übersichtlichen Meldungen mit Ampelfarben (Rot/Grün) erlauben auch die schnelle Überprüfung einer Vielzahl von Datenbanken.

Verwendungsarten

Pen test:

In diesem Modus überprüft Repscan die bestehenden Datenbanken auf unsichere Konfigurationen bzw. Datenbank-Einstellungen. Der dabei erzeugte Report enthält detaillierte Hinweise, wie die einzelnen Probleme zu beheben sind.

Audit:

Im Audit-Modus überprüft Repscan bestehende Datenbanken auf unsichere Konfigurationen bzw. Datenbank-Einstellungen und vergleicht **zusätzlich** das Data Dictionary auf Modifikationen (z.B. in Views, Packages, ...). Damit lassen sich auch Datenbank-Rootkits finden.

Baseline:

Im Baseline-Modus erzeugt Repscan eine neue Baseline des Data Dictionary. Dies ist nach Upgrades oder Updates der Datenbank notwendig.

Systemvoraussetzungen

Betriebssystem:

Microsoft Windows 2000 SP4,
Microsoft Windows XP SP1,
Microsoft Windows PE

Prozessor: mind. Pentium 200 MHz
RAM: 256 MB
Festplatte: mind. 10 MB

Weitere Voraussetzungen

Microsoft .NET 1.1 SDK
Oracle Client Software
(frei verfügbar unter
<http://otn.oracle.com/software/>)
Microsoft IE 4.01 oder höher,
Mozilla Firefox

Netzwerkverbindung zu Oracle
Datenbanken

Testversion

Limitierte Testversion (maximal
2 Datenbanken) erhältlich.
Die Testversion enthält nur eine
eingeschränkte Anzahl von SQL
Überprüfungen

Beispiele:

Verwendete Parameter

Parameter	Value	MD5
dbinfolist	databases.xml	3d81751e9be14c74cf2a25c19c7de507
dbchecklist	exec.xml	2698889f8eb6bfb7a055ff66e16c9c16
action	check	
signatures	signatures\	
reportfile	scanreport.xml	25ebd0340c3dda607cece8c57f86ed73
rulesonly	No	

Gescannte Datenbanken

Datenbank Name	Signatur	Ergebnis
ora_test_10104	signatures\ora10104_sig.csv	OK
ora_prod_10103	signatures\ora10103_sig.csv	OK
ora_sales_10103	signatures\ora10103_sig.csv	OK
ora_dev_90205	signatures\ora90205_sig.csv	OK
ora_dev2_90206	signatures\ora90206_sig.csv	Fehler
ora_edu_90206	signatures\ora90206_sig.csv	OK
ora_stage_90206	signatures\ora90206_sig.csv	OK
ora_marketing_8174	signatures\ora8174_sig.csv	Fehler
ora_mark_test_8174	signatures\ora8174_sig.csv	OK
ora_iasdb	signatures\ora9014_sig.csv	OK

Veränderte Objekte in ora_dev2_90206

Art der Modifikation	Owner	Type	Name	neue MD5-Checksumme
hinzugefügt	SYS	FUNCTION	VERIFY_SOURCE	1e8244a80dfcc6a7a9edcc4cd3b8b0c8
hinzugefügt	SYSTEM	SYNONYM	DBA_USERS	9d5a69aeabcf6fd020a5d02d61e6fa3f
verändert	SYS	VIEW	DBA_USERS	b00c9f18c7d8514ab5ef69f7040c92a1
verändert	SYS	VIEW	V_SSESSION	779aabb2a44dc5281ea314f5acecccc32
verändert	SYS	PACKAGE	DBMS_SYS_SQL	e74522aaf07bcf94c201165270967761

Die folgenden Regelverletzungen wurden in ora_dev2_90206 gefunden:

Kontext	Beschreibung
OUTLN	OUTLN verwendet das Standard Password OUTLN. Bitte ändern Sie dieses Password als DBA mit folgendem Kommando ALTER USER OUTLN IDENTIFIED BY % NEWPASSWORD%;
REMOTE_OS_AUTHENT ist TRUE	REMOTE_OS_AUTHENT ist auf TRUE gesetzt und es existieren OPSS. Oracle nimmt daher an, dass das Remote Betriebssystem den Benutzer bereits authentifiziert hat.

Mehr Informationen über uns und unser Angebot finden Sie unter www.netcos.de oder Sie setzen sich persönlich mit uns in Verbindung. Wir beraten Sie gerne.