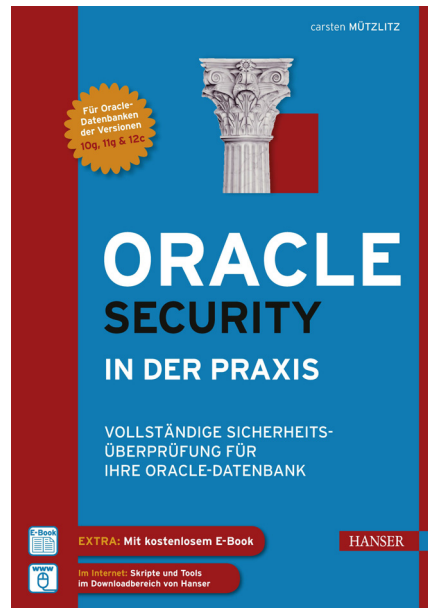


HANSER



Inhaltsverzeichnis

zu

„Oracle Security in der Praxis“

von Carsten Mützlitz

ISBN (Buch): 978-3-446-43869-9

ISBN (E-Book): 978-3-446-43923-8

Weitere Informationen und Bestellungen unter
<http://www.hanser-fachbuch.de/978-3-446-43869-9>

sowie im Buchhandel

© Carl Hanser Verlag München

Inhalt

1	Vorbemerkung	1
2	Einführung	5
3	Grundlagen zur IT-Sicherheit bei Datenbanken	9
3.1	Die vier Grundbedrohungen	9
3.2	Bedrohungs- und Risikoanalyse	11
3.3	Ausflug in den Gesetzesdschungel	14
3.3.1	Gesetzliche Anforderung an das Vorhandensein eines Sicherheitskonzepts	16
3.3.2	Haftung von IT-Mitarbeitern	17
3.3.3	Bundesdatenschutzgesetz	19
3.3.4	Gesetz zur Bekämpfung der Wirtschaftskriminalität	21
3.4	Sicherheitszonen einer Oracle-Datenbank	23
4	Lösungen für eine höhere DB-Sicherheit (Best Practices)	25
4.1	Passwortmanagement	26
4.1.1	Kurzer Ausflug: Kerberos und Enterprise User Security	33
4.2	Feature-Umfang - neue und nicht mehr vorhandene Features	38
4.3	Mindestsicherheit implementieren (Härtung)	40
4.4	Rollenmanagement	45
4.5	Sicheres Datenbank-Link-Konzept	49
4.6	Schutz von Anwendungen	52
4.7	Datenschutz implementieren	59
4.8	Ressourcenmanagement	63
4.9	Zwecktrennung in der Datenbank	66
4.10	Protokollierung	68
4.11	Prozesse zum Erhalt des guten Sicherheitszustands	71
4.12	Health Checks	73
4.13	Einführung in das Patching	74

4.14	Neuerungen in der Oracle-Datenbank 12c	78
4.14.1	Benutzer- und Passwortmanagement	79
4.14.2	Rollenmanagement und Zugriffskontrolle	80
4.14.3	Neues oder altes Audit-Konzept (Unified Auditing)	87
4.14.4	SoD in Datenbank (SYSBACKUP, SYSDBG, SYSKM, SYS)	94
4.14.5	Privileganalyse („Least Privilege“-Konzept)	96
4.14.6	Transparent Sensitive Data Protection (TSDP)	100
4.14.7	Data Redaction	102
4.14.8	Real Application Security	104
4.14.9	Neuerung bestehender Security-Features	105
4.14.10	Interessante Konzepte	106
4.14.11	Nicht mehr unterstützte Features der 12c-Datenbank	120
5	Sicherheit einer Oracle-Datenbank prüfen	121
5.1	Datenbankkonfiguration	123
5.1.1	Abfrage 1001: erste Datenbankinformationen	124
5.1.2	Abfrage 1001.1: Datenbankinformationen zu 12c (Container)	125
5.1.3	Abfrage 1002: Datenbankversion	128
5.1.4	Abfrage 1003: genutzte Datenbankoptionen	129
5.1.5	Abfrage 1003.1: benutzte Optionen und Funktionen der Datenbank ...	131
5.1.6	Abfrage 1004 – 1005: Enterprise Manager Informationen	134
5.1.7	Abfrage 1006: Advanced Security Option (ASO) im Einsatz	136
5.1.8	Abfrage 1007: Security-Parameter in init.ora	138
5.1.9	Abfrage 1007.1: Show Hidden init.ora-Parameter	142
5.1.10	Abfrage 1008: UTL_FILE_DIR und DIRECTORIES	144
5.1.11	Abfrage 1009: OPEN_LINK und Anzahl der Datenbank-Links	146
5.1.12	Abfrage 1010: SQL-Tuning	147
5.1.13	Abfrage 1011: Status der Controlfiles	148
5.1.14	Abfrage 1012: Redo Logs	148
5.1.15	Abfrage 1013: Archive Logs	149
5.1.16	Abfrage 1014: Tablespace-Informationen	150
5.1.17	Abfrage 1015: Tablespace-Extents	151
5.1.18	Abfrage 1016: Tablespace-Contents	152
5.1.19	Abfrage 1017 – 1020: Temporary-Tablespace-Information	153
5.1.20	Abfrage 1021: Datendateiinformationen	155
5.1.21	Abfrage 1022: Objekte im SYSTEM-Tablespace	157
5.1.22	Abfrage 1023: mögliche Benutzer mit falschem Default-Tablespace ...	158
5.1.23	Abfrage 1024: SYSAUX-Tablespace	159
5.1.24	Abfrage 1025: öffentliche Abhängigkeiten in Objekten	160
5.1.25	Abfrage 1026: Synonyme auf Objekte in entfernten Datenbanken ...	162
5.1.26	Abfrage 1027: Kommentare aus der Historie	163
5.1.27	Abfrage 1028: Oracle-Standard-Schemata	164
5.1.28	Abfrage 1029: manuelle Prüfung auf Default-Passwörter	166
5.1.29	Abfrage 1030: Prüfung auf Default-Passwörter mittels View	179
5.1.30	Abfrage 1030.1: User- und Passwort-Hashes	180

5.1.31	Abfrage 1031: Passwortdatei	181
5.1.32	Abfrage 1032: Profile anzeigen	183
5.1.33	Abfrage 1033: Einstellungen der sicherheitsrelevanten Profile	184
5.1.34	Abfrage 1034: Passwort-Verify-Funktion	185
5.1.35	Abfrage 1035: Datenbank-Links	186
5.1.36	Abfrage 1036: mögliche Privilegien der entfernten DB-Benutzer aus den Datenbank-Links	187
5.1.37	Abfrage 1037: Wallets	189
5.1.38	Abfrage 1038: Wallet-Zugriffssteuerungsliste (ACL)	190
5.1.39	Abfrage 1039: spezielle Trigger (Logon, Startup)	191
5.1.40	Abfrage 1040: Information-Lifecycle-Management (12c)	192
5.1.41	Abfrage 1041: Zugriffssteuerungslisten (ACL) für Network Packages (HOST)	193
5.1.42	Abfrage 1042: Zugriffssteuerungslisten für Network Packages (XML) ..	195
5.1.43	Abfrage 1043: vollständige Informationen zur XML-Datenbank	195
5.1.44	Abfrage 1044: Zugriffssteuerung auf Dateien im Betriebssystem	205
5.1.45	Abfrage 1045: APEX-Gateway-Konfiguration	207
5.1.46	Abfrage 1046: SQL*Net-Konfiguration	210
5.1.47	Abfrage 1047: installierte Komponenten	215
5.1.48	Abfrage 1048: Patches	217
5.2	Datenbanküberwachung (Auditing)	218
5.2.1	Abfrage 2001: AUDIT-init.ora-Parameter	219
5.2.2	Abfrage 2002: Welche Systemprivilegien werden protokolliert?	221
5.2.3	Abfrage 2003: Welche Systemprivilegien werden nicht protokolliert? ..	224
5.2.4	Abfrage 2004: protokollierte Systemprivilegien im System	227
5.2.5	Abfrage 2005: Überwachung von Objektprivilegien	229
5.2.6	Abfrage 2006: 100 Audit-Datensätze von „Heute“	230
5.2.7	Abfrage 2007: 100 FGA-Audit-Datensätze von „Heute“	232
5.2.8	Abfrage 2008: überwachte Systemprivilegien	233
5.2.9	Abfrage 2009: komplette Audit-Policy überwachter Systemprivilegien .	235
5.2.10	Abfrage 2009.1: Unified Audit-Policies (12c)	237
5.2.11	Abfrage 2010–2012: Audit-Fehlerprüfung gemäß Oracle-Empfehlung ..	239
5.2.12	Abfrage 2013: Wer verfügt über Audit-Systemprivilegien?	240
5.2.13	Abfrage 2014: Shared Database Logons	242
5.2.14	Abfrage 2015: Detailinformationen zu den Shared Database Logons (nur Heute)	244
5.2.15	Abfrage 2016: verwaiste Benutzer (letzte Anmeldung > 90 Tage)	245
5.2.16	Abfrage 2017: Database Control Logins	248
5.2.17	Abfrage 2018: fehlerhafte Logins = Bruteforce-Attacken	249
5.2.18	Abfrage 2019: aktuelle Sessions	251
5.2.19	Abfrage 2020: Prüfung auf alte EM-9i-Sessions	253
5.2.20	Abfrage 2021: Übersicht der Datenbankbenutzer	254
5.2.21	Abfrage 2022: Übersicht der Datenbankbenutzer per Status	256
5.2.22	Abfrage 2023: Übersicht der Datenbankbenutzer per Profil	257
5.2.23	Abfrage 2024: Datenbankbenutzer sortiert nach Sperrdatum	258

5.2.24	Abfrage 2025: Datenbankbenutzer sortiert nach Ablaufdatum	259
5.2.25	Abfrage 2026: alle Nicht-Oracle-Standarddatenbankbenutzer	261
5.2.26	Abfrage 2027: Nutzer in der Passwortdatei	263
5.2.27	Abfrage 2028: Übersicht der Benutzer und deren Profil	264
5.2.28	Abfrage 2029: unsichtbare Benutzer	266
5.2.29	Abfrage 2030: Rootkits	267
5.2.30	Abfrage 2031: unsichtbare Rollen	268
5.2.31	Abfrage 2032: aktivierte Funktionen und Optionen	269
5.2.32	Abfrage 2033: alle nicht registrierten Schemata anzeigen	270
5.2.33	Abfrage 2034: alle ausgeschalteten Trigger anzeigen	272
5.2.34	Abfrage 2035: alle ausgeschalteten Constraints anzeigen	273
5.2.35	Abfrage 2036: alle Benutzer, die Objekte verwalten	275
5.2.36	Abfrage 2037: alle Benutzer, die <i>keine</i> Objekte verwalten (ohne Objekte)	276
5.2.37	Abfrage 2038: Diagnoseinformationen	277
5.2.38	Abfrage 2039: Unified Audit Application Context Attributes	278
5.2.39	Abfrage 2040: Audit-Policies für Real Application Security	279
5.2.40	Abfrage 2041: aktivierte Audit-Policies für Real Application Security	280
5.2.41	Abfrage 2042: Audit-Einträge für Real Application Security	281
5.3	Datenbankverfügbarkeit	283
5.3.1	Abfrage 3001: init.ora-Parameter	284
5.3.2	Abfrage 3002: Control-Dateien	287
5.3.3	Abfrage 3003: Log-Dateien	288
5.3.4	Abfrage 3004: fragmentierte Objekte	289
5.3.5	Abfrage 3005: Objekte mit möglichen Extent-Problemen	290
5.3.6	Abfrage 3006: ungültige Objekte	292
5.3.7	Abfrage 3007: Fast Recovery Area	293
5.3.8	Abfrage 3008: verwaltete Dateien in der Fast Recovery Area	294
5.3.9	Abfrage 3009: Übersicht zu RECYLCEBIN	295
5.3.10	Abfrage 3010: wiederhergestellte Objekte in der Datenbank	296
5.3.11	Abfrage 3011: RMAN-Konfiguration	296
5.3.12	Abfrage 3012: Übersicht des RMAN-Status der letzten 7 Tage	297
5.3.13	Abfrage 3013: Übersicht verfügbarer Backups	299
5.3.14	Abfrage 3014: korrupte Datenbackups	300
5.3.15	Abfrage 3015: korrupte Datenblöcke	301
5.3.16	Abfrage 3016: aktuelle Sessions mit hoher CPU-Belastung	302
5.3.17	Abfrage 3017: aktuelle Sessions mit hohen Wartezeiten	303
5.3.18	Abfrage 3018: aktuelle Sessions mit hohen Datenbankzeiten	304
5.3.19	Abfrage 3019: ASM-Attribute	306
5.3.20	Abfrage 3020: ASM-Dateien	307
5.3.21	Abfrage 3021: Data Guard-Statusinformationen	308
5.3.22	Abfrage 3022: Informationen zu Instance Caging und zum Ressourcen-Manager	310
5.3.23	Abfrage 3023: Ressourcen-Manager-Informationen pro Container	311

5.3.24	Abfrage 3024: zusätzliche Ressourcen-Manager-Informationen pro Container	312
5.3.25	Abfrage 3025: Informationen zu Inkompatibilitäten	314
5.3.26	Abfrage 3026: nicht genutzte Indizes	315
5.3.27	Abfrage 3027: Liste der letzten Änderungen an den Objekten	316
5.3.28	Abfrage 3028: zeitlich beschränkte Historie von Alerts	317
5.3.29	Alert.log prüfen	319
5.4	Datenbank-Zugriffskontrolle	319
5.4.1	Abfrage 4001: Übersicht aller Benutzer (Schema) in der Datenbank ...	321
5.4.2	Abfrage 4001.1: Übersicht aller COMMON- und LOCAL-Benutzer (Schema) in der Datenbank 12c	324
5.4.3	Abfrage 4001.2: Zugriff auf Container	326
5.4.4	Abfrage 4002: Übersicht aller Datenbankadministratoren	328
5.4.5	Abfrage 4003: Übersicht aller SYSDBAs	330
5.4.6	Abfrage 4004: Übersicht ROLES/USERS mit Audit-Privilegien	332
5.4.7	Abfrage 4005: zusammenfassende Zählung der Berechtigungen auf das Data Dictionary	333
5.4.8	Abfrage 4006: Übersicht der Rollen und Benutzer mit Zugriffsrechten auf SYS-Objekte	335
5.4.9	Abfrage 4007: Übersicht der Rollen in der Datenbank	337
5.4.10	Abfrage 4008: Übersicht der Nicht-Standardrollen	339
5.4.11	Abfrage 4009: Übersicht zu Rollen mit erhöhtem Schutz	342
5.4.12	Abfrage 4010: Übersicht zu Datenbank-Accounts, die Rollen anlegen ..	343
5.4.13	Abfrage 4011: Übersicht der Datenbank-Accounts und deren Rollenberechtigungen	345
5.4.14	Abfrage 4012: Übersicht zu Datenbank-Links und möglicher Berechtigungen in Remote-Datenbanken	347
5.4.15	Abfrage 4013: Anzahl der SYSTEM-Privilegien verschiedener Benutzer	349
5.4.16	Abfrage 4014: Rolle-an-Rolle-Hierarchie	350
5.4.17	Abfrage 4015: Übersicht aller Systemprivilegien an Rollen und User ...	352
5.4.18	Abfrage 4016: Übersicht aller Benutzer und Rollen mit ANY-Privilegien	355
5.4.19	Abfrage 4017: Übersicht aller Benutzer und Rollen mit EDITION-Privilegien	357
5.4.20	Abfrage 4018: Übersicht aller Benutzer und Rollen mit POWER-Privilegien	358
5.4.21	Abfrage 4019: Übersicht aller Benutzer und Rollen mit Account-Management-Privilegien	360
5.4.22	Abfrage 4020: Übersicht aller Benutzer und Rollen mit ALTER SESSION	362
5.4.23	Abfrage 4021: Übersicht aller Benutzer und Rollen mit ALTER SYSTEM	364
5.4.24	Abfrage 4022: Übersicht aller Benutzer und Rollen, die die RLS umgehen können	365

5.4.25	Abfrage 4023: Übersicht aller Benutzer und Rollen mit UNLIMITED TABLESPACES	366
5.4.26	Abfrage 4024: Detailübersicht aller Benutzer mit Tablespace-Quota	368
5.4.27	Abfrage 4025: Übersicht aller Benutzer/Rollen mit Standardrollen (CONNECT, RESOURCE)	369
5.4.28	Abfrage 4026: Übersicht aller Benutzer/Rollen mit EXP/IMP_FULL_DB	372
5.4.29	Abfrage 4027: Übersicht aller Benutzer und Rollen, die gefährliche Rollen besitzen	374
5.4.30	Abfrage 4028: Übersicht der Zugriffe auf Network-Packages	376
5.4.31	Abfrage 4029: Übersicht der Abhängigkeiten auf Network-Packages ...	378
5.4.32	Abfrage 4030: ACL-Übersicht auf Network-Packages	380
5.4.33	Abfrage 4031: Übersicht der Berechtigungen auf XML-Datenbank-ACL	382
5.4.34	Abfrage 4032: Übersicht aller Dateien der XML-DB-ACL	383
5.4.35	Abfrage 4033: Übersicht aller EXECUTE-Berechtigungen auf Nicht-Standard-User	387
5.4.36	Abfrage 4034: Übersicht aller Objektprivilegien in der Datenbank (ohne PUBLIC)	388
5.4.37	Abfrage 4035: Übersicht aller Objektprivilegien in der Datenbank (Special Grants)	390
5.4.38	Abfrage 4036: Übersicht aller PUBLIC-Objekt- und Systemprivilegien in der Datenbank	392
5.4.39	Abfrage 4037: Übersicht der VPD-Policies	394
5.4.40	Abfrage 4038: Übersicht aller Datenbank-CONTEXTs	396
5.4.41	Abfrage 4039: Übersicht der Proxies	397
5.4.42	Abfrage 4040: Übersicht der Java-Permission	398
5.4.43	Abfrage 4041: Übersicht zu Directories und deren Zugriffsberechtigungen	400
5.4.44	Abfrage 4042: an PL/SQL gegrantete Rollen	402
5.4.45	Abfrage 4043: Credentials für externe Prozeduraufrufe	403
5.4.46	Abfrage 4044: Liste nicht vorhandener Digest Verifiers (Upgrade XMLDB)	404
5.4.47	Abfrage 4045: Übersicht zu Transparent Sensitive Data Protection (TSDP)	406
5.4.48	Abfrage 4046: Data Redaction-Policies	407
5.4.49	Abfrage 4047: Privileganalyse	408
5.4.50	Abfrage 4048: Invoker-Rechte für Views und PL/SQL	410
5.5	Zusätzliche Untersuchungen	412
5.5.1	Abfrage 5001: Übersicht verschlüsselter Tablespaces	412
5.5.2	Abfrage 5002: Übersicht verschlüsselter Spalten	413
5.5.3	Abfrage 5003: Übersicht der Data Labels	415
5.5.4	Abfrage 5004: Übersicht von Objekten mit speziellen Datentypen	416
5.5.5	Abfrage 5005: Übersicht aller Libraries	417
5.5.6	Abfrage 5006: gefilterte Übersicht aller Libraries	420

5.5.7	Abfrage 5007: Übersicht aller Fehler (RMAN)	421
5.5.8	Abfrage 5008: Übersicht aller eingespielten Patchsets	423
5.5.9	Abfrage 5009: Übersicht aller eingespielten Patches	424
5.5.10	Abfrage 5010: Übersicht der Database Vault-Sicherheitszonen	424
5.5.11	Abfrage 5011: Übersicht der Scheduler-Jobs innerhalb der letzten 24 Stunden	427
5.5.12	Abfrage 5012: Übersicht aller Scheduler-Programme	428
5.5.13	Abfrage 5013: Übersicht aller Scheduler-Credentials	429
5.5.14	Abfrage 5014: Java-Übersicht	430
5.6	Prüfung auf mögliche bekannte Schwachstellen	435
5.6.1	Abfrage 6001: Schwachstelle SCN-Headroom	435
5.6.2	Abfrage 6002: CVE-2012-3132: Get SYSDBA Rights	438
5.7	Datenbanksicherheitsprüfung durchführen	441
5.7.1	Ausführung einer automatischen Sicherheitsprüfung unter Windows ..	442
5.7.2	Ausführung einer automatischen Sicherheitsprüfung unter UNIX	443
5.8	Vereinfachte Auswertung der Zugriffskontrolle durch SQL	445
5.8.1	Oracle Software Appliance als Auswertungssystem nutzen	445
5.8.2	Daten der untersuchten Datenbank laden	446
5.8.3	Evaluierungsdashboard	450
5.8.4	Manuelle Auswertungsmöglichkeiten	452
5.9	Sicherheitszustand bewerten	460
5.9.1	Einzelne Untersuchungen bewerten	461
5.9.2	Bewertung nach CVSS	466
5.9.3	Toolbasierte Datenbanksicherheitsprüfung	467
6	Anhang: Fragenkatalog	469
6.1	Businessbeitrag der IT-Abteilung	470
6.2	Welche Konzepte existieren und sind implementiert?	471
6.3	Welche Daten befinden sich in der zu untersuchenden Datenbank?	473
6.4	Wie sehen die Architektur und das Deployment aus?	474
6.5	Wie installieren Sie Datenbanken?	475
6.6	Wer greift auf die Datenbank zu?	476
6.7	Welches Patching-Konzept wird verfolgt?	478
6.8	Wie wird die Datenbank bzw. das System überwacht?	479
6.9	Ist die Integrität der Datenbank und des Systems sichergestellt?	480
6.10	Wo steht der Datenbankserver?	482
6.11	Kann die Integrität der Daten sichergestellt werden?	482
6.12	Was tut der Betreiber für eine sichere Konfiguration?	483
Index	485	