



Inhaltsverzeichnis

Einleitung.....	XIII
Teil I Einstieg	1
1 Sicherheitsarchitektur	3
1.1 Entwicklungsgeschichte der Sicherheit	3
1.2 Sicherheit und Computer.....	5
1.2.1 Sicherheit in einer virtuellen Welt	6
1.3 Die Gefahrenquellen kennen	8
1.3.1 Gefahrenquellen von innen	9
1.3.2 Externe Gefahrenquellen	13
1.3.3 Warum gibt es Sicherheitslöcher?	16
1.4 Herausfinden, wer was tun kann	19
1.4.1 Authentifizierung.....	20
1.4.2 Autorisierung	29
1.4.3 Systemintegrität	30
1.4.4 Ein Blick auf verschiedene Authentifizierungsmodelle	31
2 Sicherheitsimplementierung bei Oracle	37
2.1 Hintergründe der Sicherheit bei Oracle	40
2.1.1 Über Backups	42
2.1.2 Die Sicherheit robuster machen.....	44
2.1.3 Version 6 und neue Sicherheitsansätze.....	50
2.1.4 Nun kommt Oracle7.....	53
2.1.5 Einführung von Oracle8	61
2.2 Oracle8i und das Internet	65
2.2.1 Neue Möglichkeiten für Standby-Datenbanken	66
2.2.2 Ein Blick auf die Features von Oracle8i Advanced Security	67

3	Planen Sie Ihre Sicherheit	77
3.1	Festlegen Ihres Sicherheitsplans	78
3.1.1	Der Sicherheitskompromiss	80
3.1.2	Die Rolle eines Sicherheitsplans	81
3.1.3	Globale versus lokale Richtlinien	82
3.1.4	Verantwortlichkeit zuweisen	85
3.1.5	Prozeduren	87
3.2	Risiken einschätzen	100
3.2.1	Wie angreifbar ist Ihr System?	100
3.2.2	Werte einschätzen	102
3.2.3	Alternative Lösungen	105
3.3	Lebenszyklen einer Datenbank	105
3.3.1	Ältere Systeme	105
3.3.2	Neue Systeme	107
3.3.3	Datenbank-Software-Pakete evaluieren	109
Teil II	Das Betriebssystem sicherer machen	111
4	Datenbanksicherheit unter Unix-Betriebssystemen	113
4.1	Warum wir ein Betriebssystem brauchen	114
4.1.1	Betriebssystemtypen	114
4.2	Unix absichern	118
4.2.1	Grundlegende Sicherheits-Features von Unix	118
4.2.2	Das Betriebssystem sichern	129
4.3	Oracle unter Unix sichern	132
4.3.1	Wie die Oracle-Datenbank arbeitet	133
4.3.2	Oracle unter Unix installieren	134
4.3.3	Ein sicheres temporäres Verzeichnis nutzen	144
4.3.4	Raw Devices sichern	145
4.3.5	Oracle-Dateien mit aktivem SUID-Bit	146
4.3.6	OSDBA, OSOPER und Internal	150
4.3.7	Eine Warnung zur Nutzung von SQL*Plus	151
4.3.8	Die Audit-Daten im Betriebssystem schreiben	152
5	Sicherheitsoptionen von Oracle und Windows NT/2000	155
5.1	Grundlagen von Windows NT/2000	155
5.1.1	Sicherheitsfragen zu Windows NT untersuchen	156
5.2	Überblick über Windows NT mit Oracle	174
5.2.1	Wie Windows NT funktioniert	175
5.2.2	Prozesse versus Threads	178
5.2.3	Die Oracle-Threads anzeigen	180
5.2.4	Oracle und die Windows-Registry	183

5.3	Oracle auf Ihrem Windows NT/2000-System schützen	187
5.3.1	Die Oracle-Software schützen	187
6	Authentifizierung im Betriebssystem	191
6.1	Authentifizierung konfigurieren.....	192
6.1.1	Parameter setzen	193
6.1.2	TNS-Protokoll.....	195
6.2	Authentifizierung mit Windows.....	198
6.2.1	Bestätigungen über das Netzwerk versenden	200
6.2.2	Einen Windows-Datenbankbenutzer erstellen	201
6.2.3	Einen Windows-Benutzer erstellen.....	204
6.2.4	Rollen im Betriebssystem Windows.....	211
6.3	Authentifizierung mit Unix	217
6.3.1	Einen Unix-Datenbankbenutzer erstellen	217
Teil III	Die Oracle-Datenbank sichern.....	221
7	Kennwörter und Benutzer	223
7.1	Die Passwortmanagement-Features von Oracle	224
7.1.1	Über Passwort-Verbesserungen	225
7.2	Standardbenutzer unter Oracle	233
7.2.1	Die Standardbenutzer untersuchen	234
7.3	Identifikation externer und entfernter Benutzer	246
7.3.1	Über Orapwd.....	247
8	Privilegien, Berechtigungen, Rollen und Views.....	253
8.1	Über Objekte und Berechtigungen	254
8.2	Über Benutzer	256
8.2.1	Benutzerzugriff kontrollieren.....	257
8.2.2	Über die Vergabe von Berechtigungen	264
8.2.3	Wie Rollen verwendet werden	267
8.2.4	Von Oracle mitgelieferte Rollen.....	271
8.2.5	Über Standardrollen für Benutzer	274
8.3	Einsatz von Views	277
8.3.1	Views erstellen.....	278
8.4	Über Trigger.....	281
9	Oracle und Datenbank-Links.....	283
9.1	Grundlegender Aufbau von Datenbank-Links	285
9.1.1	Einen Datenbank-Link anlegen.....	288
9.1.2	Sicherheitsprobleme bei Datenbank-Links	295

9.1.3	Über gemeinsam genutzte Datenbank-Links.....	299
9.1.4	Mehr über globale Datenbank-Links	300
9.1.5	Datenbank-Links auditieren	307
10	Entwickler-Tools und Sicherheit.....	309
10.1	Applikationssicherheit	310
10.1.1	Datenbank- versus Applikationsbenutzer.....	310
10.1.2	Applikationssicherheit über die Datenbank umsetzen.....	312
10.1.3	Entwurfspraktiken für Applikationen	315
10.1.4	Oracle Call Interface.....	319
10.1.5	Auditing zur Überwachung der Datenbankaktivitäten.....	327
10.2	Virtual Private Database	329
10.2.1	Detaillierte Zugriffskontrolle	330
10.2.2	Applikationskontext	332
10.3	Rechte des Aufrufenden versus Rechte des Erstellers	335
10.3.1	Rechte des Erstellers	336
10.3.2	Rechte des Aufrufenden	336
10.4	PL/SQL-Pakete	338
10.4.1	DBMS_OBFUSCATION_TOOLKIT	339
10.4.2	Das Paket UTL_FILE.....	340
Teil IV	Sichere Netzwerkkommunikation	343
11	Netzwerkintegrität, Authentifizierung und Verschlüsselung.....	345
11.1	Einführung in die Option Oracle Advanced Security	346
11.1.1	Sniffing und Spoofing	346
11.1.2	Eine Verbindung kidnappen.....	350
11.1.3	Daten im Netzwerk schützen	350
11.2	Proprietäre Features von OAS.....	357
11.2.1	Konfigurieren der Authentifizierung	359
11.2.2	Die Integritätsprüfung konfigurieren.....	361
11.2.3	Die Verschlüsselung konfigurieren	362
11.3	Das Secure Sockets Layer-Protokoll.....	363
11.3.1	SSL konfigurieren	364
11.3.2	Eine SSL-Verbindung debuggen.....	373
11.3.3	Enterprise User Security.....	375
11.4	Empfohlene Protokolle	376

12 Sicherheitsoptionen bei Oracle.....	377
12.1 Virtual Private Databases	379
12.1.1 Eine VPD erstellen	380
12.2 Ein Blick auf die Oracle Label Security.....	391
12.3 Oracle Internet Directory	394
12.3.1 Über die LDAP-Architektur	395
12.3.2 Implementierung des Oracle Internet Directory	401
13 Firewalls und Oracle.....	409
13.1 Wie Firewalls arbeiten	410
13.1.1 Vorgehensweise einer Firewall	411
13.1.2 Was eine Firewall nicht verhindert	415
13.1.3 Firewall-Typen	416
13.2 Oracle mit einer Firewall verwenden.....	417
13.2.1 Das Problem.....	418
13.2.2 Feststellen, ob ein Verbindungsproblem durch eine Firewall verursacht wird	420
13.2.3 Firewall Proxies	421
13.2.4 Listener-Dienst.....	423
13.2.5 Connection Manager	425
13.2.6 Port-Umleitung verhindern	428
14 Sicherheit des Apache HTTP-Servers	431
14.1 Über Web-Server	431
14.1.1 Aufgaben des Web-Servers	432
14.2 Oracles Apache-Implementierung	438
14.2.1 Installation und Konfiguration von Apache	439
14.2.2 HTTP-Konfigurationsdatei von Oracle.....	451
14.2.3 Sicherheit des Apache	453
15 Sicherheitsmanagement mit Oracle Portal.....	455
15.1 Oracle Portal – Von Anfang an.....	456
15.1.1 Standardkennungen von Oracle Portal	456
15.2 Authentifizierungsmanagement in Portal.....	461
15.2.1 Typen von Benutzerkonten	462
15.3 Benutzerverwaltung.....	463
15.3.1 Benutzer hinzufügen.....	463
15.3.2 Einen Benutzer bearbeiten	469
15.3.3 Eigenständige Benutzerverwaltung.....	479
15.4 Konfigurieren des Login Servers.....	480
15.4.1 Management der Passwortrichtlinien.....	482
15.4.2 Benutzer authentifizieren	486

15.5	Management des Objektzugriffs.....	491
15.5.1	Gruppen erstellen	492
15.5.2	Benutzern und Gruppen Zugriff erteilen	495
15.5.3	Öffentlichen Zugriff für Seiten und Applikationen erteilen	503
Teil V	Hacker und Fehlersuche.....	505
16	Implementierung des Auditings.....	507
16.1	Über das Auditing	508
16.1.1	Fragebogen zum Auditing.....	509
16.1.2	Das Auditing der Datenbank anpassen	522
16.2	Ein Ansatz zum Auditieren von Tabellen	525
16.2.1	Audit-Skripte für Tabellen.....	526
17	Ihre Datenbank gegen Hacker sichern.....	539
17.1	Angreifer	541
17.1.1	Verärgerte Mitarbeiter.....	541
17.1.2	Professionelle Hacker	549
17.1.3	Vandalen	552
17.1.4	Autorisierte Benutzer, die höhere Berechtigungen erlangen wollen.....	553
17.2	Angriffsarten.....	555
17.2.1	Buffer Overflows.....	555
17.2.2	SQL Injection-Angriff	557
17.2.3	Eine Sicherheitslücke melden	561
17.2.4	Unabhängige Sicherheitsüberprüfungen	562
17.3	Tools zum Schutz Ihrer Datenbank	563
17.3.1	Sicherheitsprüfungen	563
17.3.2	Intrusion Detection	564
17.3.3	Verschlüsselung	564
17.3.4	Eine Produktstrategie wählen	567
A	Glossar	569
B	Checklisten zum Prüfen des Sicherheitsrisikos	577
B.1	Physische Sicherheit der Hardware	578
B.2	Ausstattung, Bänder und Festplatten.....	579
B.3	Betriebssystem- und Netzwerksicherheit.....	581
B.4	Kennwort- und Kontoverwaltung.....	583
B.5	Datensicherung und Wiederherstellung.....	585
B.6	Rechtliche Aspekte	587
B.7	Richtlinien und Prozeduren	588

B.8	Spezifische Aspekte bei Oracle	589
B.9	Weitere Punkte	591
C	Schritte zum Sichern Ihres Systems	593
C.1	Standardkennwörter ändern	594
C.2	Features für das Passwortmanagement aktivieren	595
C.3	Nicht benötigte Berechtigungen für PUBLIC entziehen	596
C.4	Parameter auf sichere Werte setzen	596
C.5	Ihre Oracle-Datenbank(en) hinter einer Firewall unterbringen	597
C.6	Das Kennwort des Listeners setzen	598
C.7	SSL für die Netzwerkverschlüsselung aktivieren	599
C.8	Das Betriebssystem sicherer machen	600
C.9	Sicherheits-Patches herunterladen und einspielen	600
D	Systemberechtigungen und Audit-Optionen	601
E	Sicherheits-Features von Oracle9i	607
E.1	Datensicherheit	608
E.2	Sichere Applikationsrollen	608
E.3	Proxy-Authentifizierung	609
E.4	Java-Sicherheit	609
E.5	PKI-Unterstützung	610
E.6	Optionen der Oracle Advanced Security	611
E.7	Oracle9i Data Guard	611
E.8	Detailliertes Auditieren	612
E.9	Oracle Net	613
E.10	Standardmäßige Konten und Kennwörter	614
	Schlagwortregister	615