

# Stručný obsah

## Část I

<b>Začínáme</b>	<b>1</b>
1 Budování zabezpečení	3
2 Implementace zabezpečení na platformě Oracle	31
3 Vytvoření plánu zabezpečení	63

## Část II

<b>Zabezpečení operačního systému</b>	<b>91</b>
4 Zabezpečení databáze na operačním systému Unix	93
5 Oracle a zabezpečení Windows NT/2000	127
6 Ověřování uživatelů operačním systémem	157

## Část III

<b>Zabezpečení databáze Oracle</b>	<b>181</b>
7 Hesla a uživatelé	183
8 Oprávnění, práva, role a pohledy	207
9 Databázová propojení	231
10 Zabezpečení a vývojové nástroje	251

## Část IV

<b>Zabezpečení komunikace na síti</b>	<b>277</b>
11 Kontrola integrity dat, ověřování a šifrování v síti	279
12 Možnosti zabezpečení v Oracle	305
13 Firewally a Oracle	331

---

14 Zabezpečení HTTP serveru Apache	349
15 Správa zabezpečení v Oracle Portal	369

## Část V

---

**Hackeri a řešení problémů** **411**

16 Implementace auditu	413
17 Zabezpečení databáze před hackery	439

## Část VI

---

**Dodatky** **463**

A Slovníček	465
B Kontrolní seznamy pro posouzení bezpečnostních rizik	471
C Zabezpečení systému po krocích	485
D Systémová oprávnění a možnosti auditu	493
E Nové možnosti zabezpečení v Oracle9i	497
Rejstřík	505

# Obsah

<b>0 autorech</b>	<b>xvii</b>
<b>Předmluva</b>	<b>xix</b>

## Část I Začínáme 1

### 1 Budování zabezpečení 3

<b>Vývoj zabezpečení</b>	<b>3</b>
Nástup počítačů	4
Bezpečnost ve virtuálním světě	5
<b>Poznejte útočníky</b>	<b>6</b>
Útočníci zevnitř	8
Hrozby přicházející zvenku	11
Jak vznikají díry v zabezpečení	13
<b>Určení, kdo co může dělat</b>	<b>16</b>
Ověřování (authentication)	16
Přístupová práva	23
Integrita systému	24
Různé způsoby ověřování identity	25

### 2 Implementace zabezpečení na platformě Oracle 31

<b>Základy zabezpečení v Oracle</b>	<b>34</b>
O zálohách	35
Posun k lepšímu zabezpečení	37
Verze 6 a nový pohled na zabezpečení	41
Oracle7	44
Uvedení Oracle8	50
<b>Oracle 8i a Internet</b>	<b>54</b>
Pohled na vylepšené možnosti zabezpečení Oracle8i	55

### 3 Vytvoření plánu zabezpečení 63

<b>Definování plánu zabezpečení</b>	<b>63</b>
Kompromisy zabezpečení	65
Úkol plánu zabezpečení	66

Globální a lokální politiky	67
Stanovení odpovědnosti	69
<b>Vyhodnocování rizik</b>	<b>82</b>
Jak jste zranitelní	82
Ocenění majetku	84
Alternativní řešení	86
<b>Životní cyklus databáze</b>	<b>86</b>
Používané systémy	86
Nové systémy	88
Hodnocení databázového softwaru	89

## Část II

# Zabezpečení operačního systému 91

## 4 Zabezpečení databáze na operačním systému Unix 93

<b>K čemu je potřeba operační systém</b>	<b>93</b>
Typy operačních systémů	94
<b>Zabezpečení Unixu</b>	<b>97</b>
Základní rysy zabezpečení Unixu	97
Zajištění operačního systému	105
<b>Bezpečnost Oracle na Unixu</b>	<b>108</b>
Jak pracuje databáze Oracle	109
Instalace Oracle na Unixu	110
Používání bezpečného adresáře pro dočasné soubory	118
Zabezpečení přímých zařízení	119
Soubory Oracle s nastaveným bitem SUID	119
OSDBA, OSOPER a Internal	123
Varování ohledně používání SQL*Plus	124
Zápis protokolu auditu do operačního systému	125

## 5 Oracle a zabezpečení Windows NT/2000 127

Základy Windows NT/2000	127
Otázky ohledně zabezpečení Windows NT	128
Windows NT a Oracle	144
Zobrazení vláken Oracle	148
Oracle a registr Windows	151
<b>Nastavení zabezpečení Oracle na systémech Windows NT/2000</b>	<b>154</b>
Ochrana software Oracle	155

<b>6</b>	<b>Ověřování uživatelů operačním systémem</b>	<b>157</b>
	<b>Konfigurace procesu ověřování</b>	<b>158</b>
	Nastavení parametrů	158
	Protokol TNS	160
	Proces ověřování ve Windows	161
	Zasílání údajů pro přihlášení přes síť	165
	Vytvoření databázového uživatele na Windows	165
	Vytvoření uživatele ve Windows	168
	Role v operačním systému Windows	174
	<b>Proces ověřování v operačním systému Unix</b>	<b>178</b>
	Vytvoření databázového uživatele na Unixu	179

## Část III

# Zabezpečení databáze Oracle **181**

<b>7</b>	<b>Hesla a uživatelé</b>	<b>183</b>
	Možnosti Oracle pro správu hesel	184
	<b>Implicitně vytváření uživatelé Oracle</b>	<b>191</b>
	Zjištění implicitně vytvořených uživatelských účtů	192
	<b>Externí a vzdálená identifikace uživatelů</b>	<b>201</b>
	Orapwd	202
<b>8</b>	<b>Oprávnění, práva, role a pohledy</b>	<b>207</b>
	<b>Objekty a oprávnění</b>	<b>207</b>
	<b>0 uživatelích</b>	<b>210</b>
	Řízení přístupu uživatelů	210
	Přidělování oprávnění	216
	Používání rolí	218
	Role, které jsou součástí Oracle	222
	Implicitní role uživatele	224
	<b>Používání pohledů</b>	<b>227</b>
	Vytváření pohledů	227
	<b>Triggery</b>	<b>230</b>
<b>9</b>	<b>Databázová propojení</b>	<b>231</b>
	Základní architektura databázových propojení	232
	Vytvoření databázového propojení	235
	Sdílená databázová propojení	244
	Globální databázová propojení	244

<b>10 Zabezpečení a vývojové nástroje</b>	<b>251</b>
<b>Zabezpečení aplikace</b>	<b>251</b>
Databázoví a aplikační uživatelé	252
Implementace zabezpečení aplikace v databázi	253
Postupy při návrhu aplikací	255
Rozhraní OCI	259
Audit a monitorování činností v databázi	264
<b>Virtuální privátní databáze</b>	<b>266</b>
Jemné řízení přístupu k datům	267
Aplikační kontext	269
<b>Práva vlastníka a práva volajícího</b>	<b>271</b>
Procedury s právy vlastníka	272
Procedury s právy volajícího	273
<b>Balíky PL/SQL</b>	<b>274</b>
DBMS_OBFUSCATION_TOOLKIT	275
Balík UTL_FILE	276

## Část IV

<b>Zabezpečení komunikace na síti</b>	<b>277</b>
---------------------------------------	------------

<b>11 Kontrola integrity dat, ověřování a šifrování v síti</b>	<b>279</b>
--	------------

<b>Produkt Oracle Advanced Security</b>	<b>279</b>
Sniffing a spoofing	280
Odcizení spojení	282
Ochrana dat v síti	283
<b>Nativní rysy OAS</b>	<b>288</b>
Konfigurace ověřování identity	291
Konfigurace ověřování integrity	292
Konfigurace šifrování	293
Protokol SSL	294
Konfigurace SSL	295
Ladění připojení pomocí SSL	302
Enterprise User Security	303
<b>Doporučené protokoly</b>	<b>304</b>

<b>12 Možnosti zabezpečení v Oracle</b>	<b>305</b>
---	------------

<b>Virtuální privátní databáze</b>	<b>306</b>
Vytvoření VPD	308
<b>Produkt Oracle Label Security</b>	<b>317</b>

<b>Oracle Internet Directory</b>	<b>319</b>
O architektuře LDAP	320
Implementace Oracle Internet Directory	324

## **13 Firewally a Oracle 331**

<b>Jak fungují firewally</b>	<b>331</b>
Možnosti použití firewallů	333
Čemu firewall nezabrání	336
Typy firewallů	337
<b>Používání Oracle přes firewall</b>	<b>338</b>
Problém	339
Jak zjistit, že problém s připojením je ve firewallu	340
Použití zprostředkovatele na firewallu	341
Služba listener	343
Connection Manager	344

## **14 Zabezpečení HTTP serveru Apache 349**

<b>O webových serverech</b>	<b>349</b>
Úkoly webového serveru	349
<b>Implementace serveru Apache od firmy Oracle</b>	<b>355</b>
Instalace a konfigurace serveru Apache	355
Konfigurační soubor pro Oracle HTTP	366
Zabezpečení serveru Apache	367

## **15 Správa zabezpečení v Oracle Portal 369**

<b>Oracle Portal – od začátku</b>	<b>369</b>
Uživatelé portálu Oracle	370
Správa ověřování uživatelů v portálu	373
Typy uživatelských účtů	374
<b>Správa uživatelů</b>	<b>375</b>
Vytváření uživatelů	375
Úprava uživatele	381
Údržba údajů o vlastním účtu	388
Konfigurace přihlašovacího serveru	389
Nastavení politik pro hesla	390
Ověřování uživatelů	394
<b>Správa přístupu k objektům</b>	<b>399</b>
Vytváření skupin	399
Přidělení přístupu uživatelům nebo skupinám	402
Nastavení veřejného přístupu ke stránkám a aplikacím	408

<b>Část V</b>	
<b>Hackeri a řešení problémů</b>	<b>411</b>
<b>16 Implementace auditu</b>	<b>413</b>
<b>0 auditu</b>	<b>414</b>
Otázky pro nastavení auditu	414
Přizpůsobení databázového auditu	425
<b>Způsob auditu tabulek</b>	<b>427</b>
Skripty pro audit tabulek	428
<b>17 Zabezpečení databáze před hackery</b>	<b>439</b>
<b>Útočníci</b>	<b>440</b>
Nespokojení zaměstnanci	440
Profesionální hackeři	446
Vandalové	449
Uživatel, který se snaží získat vyšší oprávnění	450
<b>Další typy útoků</b>	<b>451</b>
Přetečení vyrovnávacích pamětí	452
Útok typu vložení SQL	453
Jak hlásit objevená zranitelná místa databáze	456
<b>Nástroje na ochranu databáze</b>	<b>458</b>
Vyhodnocování zabezpečení	458
Šifrování	459
Strategie pro výběr produktu	461
<b>Část VI</b>	
<b>Dodatky</b>	<b>463</b>
<b>A Slovníček</b>	<b>465</b>
<b>B Kontrolní seznamy pro posouzení bezpečnostních rizik</b>	<b>471</b>
<b>Fyzická bezpečnost hardwaru</b>	<b>471</b>
<b>Zařízení, pásky a disky</b>	<b>473</b>
<b>Bezpečnost operačního systému a sítě</b>	<b>474</b>
<b>Správa hesel a účtů</b>	<b>476</b>
<b>Zálohování a obnova dat</b>	<b>477</b>
<b>Právní problémy</b>	<b>479</b>

Politiky a postupy	480
Otázky týkající se Oracle	481
Další otázky týkající se zabezpečení	482
<b>C Zabezpečení systému po krocích</b>	<b>485</b>
Změna implicitních hesel	485
Povolení možnosti pro správu hesel	486
Odstranění oprávnění daných rolí PUBLIC, která nejsou nezbytně nutná	487
Nastavení parametrů na bezpečné hodnoty	488
Umístění databáze za firewall	488
Nastavení hesla pro službu listener	489
Povolení SSL pro šifrování přenosů po síti	490
Zlepšení zabezpečení operačního systému	490
Stažení a aplikace bezpečnostních oprav	491
<b>D Systémová oprávnění a možnosti auditu</b>	<b>493</b>
<b>E Nové možnosti zabezpečení v Oracle9i</b>	<b>497</b>
Zabezpečení dat	497
Bezpečné aplikační role	498
Ověřování přes zprostředkovatele	498
Zabezpečení Javy	499
Podpora pro PKI	499
Produkt Oracle Advanced Security	500
Oracle9i Data Guard	500
Jemné nastavení auditu	501
Oracle Net	502
Implicitní účty a hesla	502
<b>Rejstřík</b>	<b>505</b>