
Obsah

Kapitola 1

Úvod

1

Kapitola 2

Co je to vůbec bezpečnost?

3

2.1 Rozdílné chápání pojmu bezpečnost

3

2.1.1 Bezpečnost dříve

3

2.1.2 Zabezpečení dnes

4

2.2 Bezpečnost přihlášení pod Windows 2000

7

2.2.1 Kerberos a NTLM

7

2.2.2 Autentizace pomocí Smart Card

9

2.2.3 Vzdálený přístup

10

2.3 Šifrování dat pod Windows 2000

11

2.4 Spolehlivost dat pod Windows 2000

13

2.5 Bezpečnost přístupu pod Windows 2000

14

2.6 Zabezpečení sledování pod Windows 2000

15

2.7 Zálohování dat se systémem Windows 2000

17

2.8 Zabezpečení proti výpadku a rozložení zátěže pod Windows 2000

18

2.9 Redundance dat ve Windows 2000

19

2.10 „Reliability of Service“ pod Windows 2000

20

Kapitola 3

Známé standardy bezpečnosti

23

3.1 Publikace NCSC

23

3.2 Publikace BSI

24

3.3 Kritéria bezpečnosti pro hodnocení systémů IT

25

Kapitola 4

Proces implementace bezpečnosti	27
4.1 Základní úvahy o ITSM	27
4.2 Přehled disciplín managementu ITSM	28
4.3 Vzájemná závislost jednotlivých disciplín managementu	30
4.4 Realizace ITSM v praxi	31
4.5 Microsoft Operations Framework	33
4.5.1 Procesní model MOF	33
4.5.2 Týmový model MOF	36
4.6 Závislost MOF a MSF	39
4.7 Proces managementu bezpečnosti	39
4.7.1 Prvotní implementace a styl práce managementu bezpečnosti	39
4.7.2 Rozhraní managementu bezpečnosti k managementu změn	41
4.7.3 Úkoly release managementu	42
4.7.4 Úplný plán procesu implementace nového bezpečnostního standardu	44
4.7.5 Jednotlivé úkoly managementu bezpečnosti	44
4.8 Další informace k tématu ITSM a MOF	47

Kapitola 5

Rozpoznání zdrojů nebezpečí a jejich rozbor na základě analýzy skutečného stavu (kroky č. 1 a 2 managementu bezpečnosti)	49
5.1 Znamé mezery v zabezpečení	50
5.1.1 Přístup k Internetu	50
5.1.2 Internetový server	54
5.1.3 Server RAS	56
5.1.4 Poštovní server	59
5.1.5 Zneužití dat zaměstnanci	60
5.2 Klasické metody útoku	62
5.2.1 Co je útok?	62
5.2.2 Viry, červi a trojské koně	64
5.2.3 Rozluštění hesla (password cracking)	67
5.2.4 Zneužití e-mailu	70
5.2.5 Zneužití sítě	70

5.3 Klasické metody ztráty dat	71
5.3.1 Ztráta a obnovení dat	71
5.3.2 Ztráta dat u aplikačních serverů	73
5.3.3 Dostupnost dat aplikačních serverů	73
5.4 Vzorové analýzy skutečného stavu	74
5.4.1 Analýza skutečného stavu bezpečnosti přístupu k datům	74
5.4.2 Analýza skutečného stavu bezpečnosti hesel	76
5.4.3 Analýza skutečného stavu serveru pro vzdálený přístup (RAS)	78
5.4.4 Analýza skutečného stavu přímého přístupu k Internetu	79
5.4.5 Analýza skutečného stavu přístupu na Internet přes směrovač	81
5.4.6 Analýza skutečného stavu přístupu na Internet přes server proxy	82
5.4.7 Analýza skutečného stavu připojeného internetového serveru	83
5.4.8 Analýza skutečného stavu vlastního poštovního serveru	85
5.4.9 Analýza skutečného stavu rizika ztráty dat	86
5.5 Zjištění, vyhodnocení a krok č. 3 managementu bezpečnosti	88

Kapitola 6

Administrátorské nástroje managementu bezpečnosti

91

6.1 Konzola MMC ve Windows 2000 (Microsoft management console)	92
6.1.1 Oblasti použití MMC	92
6.1.2 Součásti MMC	92
6.1.3 Moduly snap-in	93
6.1.4 Zobrazení panelu úloh	100
6.1.5 Možnosti MMC	103
6.1.6 Dokumenty MS Common Console	104
6.1.7 Zabezpečení MMC proti neoprávněnému použití	106
6.2 Zásady skupiny	108
6.2.1 Oblasti použití zásad skupiny	108
6.2.2 Způsob fungování zásad skupiny	109
6.2.3 Pořadí přiřazování zásad skupiny	109
6.2.4 Typy zásad skupiny a možnosti nastavení	110
6.2.5 Základní pravidla pro zacházení se zásadami skupin	113
6.2.6 Praktický příklad přiřazení zásad skupiny	114
6.2.7 Dědičnost zásad skupiny	120
6.2.8 Manuální urychlení přiřazení zásad skupiny	128
6.2.9 Filtrování zásad skupiny	129

6.3 Registr a jeho úpravy	129
6.3.1 Struktura souborů registru	129
6.3.2 Úpravy registru pomocí editoru registru	131
6.3.3 Logická struktura registru	133
6.3.4 Možnosti úprav registru	136
6.4 Konfigurace zabezpečení pod Windows 2000	141
6.4.1 Oblasti použití a úkoly správce konfigurace zabezpečení	141
6.4.2 Vymezení Správce konfigurace zabezpečení vůči ostatním nástrojům	142
6.4.3 Snap-in „Šablony zabezpečení“	143
6.4.4 Konfigurace a analýza zabezpečení	153
6.4.5 Nástroj příkazového řádku SECEDIT	155
6.4.6 Přiřazení definovaných šablon zabezpečení	156

Kapitola 7**Zabezpečení z hlediska uživatelů** **159**

7.1 Požadavky na zabezpečení uživatelů	159
7.2 Autentizace pod Windows	160
7.2.1 Autentizace přes NTLM	161
7.2.2 Autentizace Kerberos	162
7.2.3 Autentizace pomocí karet Smart Card	168
7.3 Možnosti zabezpečení přihlášení	182
7.3.1 Stanovení zásad účtů	182
7.3.2 Použití zásad skupiny pro přidělení uživatelských práv a možností zabezpečení	186
7.3.3 Dodatečné zálohování hesel	192
7.4 Skupiny se zabezpečením pod Windows	193
7.4.1 Struktura skupin v kombinovaném režimu	193
7.4.2 Přejít do nativního režimu	196
7.4.3 Skupiny v nativním režimu	197
7.5 Zásady auditu pro sledování uživatelů	199
7.5.1 Přehled možných zásad auditu pro sledování uživatelů	200
7.5.2 Strategie auditování v rámci sledování uživatelů	201

Kapitola 8**Zabezpečení z hlediska zdrojů** **205**

8.1 Požadavky na zabezpečení zdrojů	205
--	------------

8.2 Zabezpečení dat	206
8.2.1 Klasifikace datových aktiv	206
8.2.2 Zabezpečení místního přístupu k souborům pomocí oprávnění NTFS	208
8.2.3 Zabezpečení přístupu ze sítě prostřednictvím sdílení v síti a NTFS	217
8.2.4 Strategie sledování přístupu k datům	227
8.3 Zabezpečení konfiguračních nastavení	235
8.3.1 Přímé zabezpečení registru	236
8.3.2 Zabezpečení přístupu k registru prostřednictvím zásad skupiny	238
8.4 Zabezpečení systémových služeb	240
8.5 Zabezpečení tiskáren	242
8.5.1 Řízení bezpečnosti přístupu	242
8.5.2 Zásady zabezpečení tiskáren	244
8.6 Zabezpečení objektů Active Directory	246
8.6.1 Delegování administrátorských úkolů	246
8.6.2 Explicitní a zděděná oprávnění	251
8.6.3 Zabezpečení objektů vůči globálnímu katalogu	256

Kapitola 9

Šifrování dat pod Windows	259
9.1 Požadavky vedoucí k použití EFS	259
9.2 Metody šifrování dat a zabezpečení spolehlivosti dat	259
9.2.1 Symetrické šifrování	260
9.2.2 Asymetrické šifrování	260
9.2.3 Digitální podpisy	261
9.3 EFS (Encrypting File System) – Šifrování souborů a adresářů	261
9.4 Příprava použití EFS	263
9.4.1 Systémové předpoklady pro použití EFS	263
9.4.2 Vymezení dat určených k šifrování	264
9.5 Aspekty šifrování dat	265
9.5.1 Šifrování souborů a složek	265
9.5.2 Přístup k zašifrovaným souborům a složkám	271
9.5.3 Kopírování a přesouvání zašifrovaných dat	271
9.6 Zálohování a obnova zašifrovaných dat	273
9.6.1 Zálohování zašifrovaných dat	273
9.6.2 Agent obnovení	273
9.6.3 Konfigurace zásad zabezpečení	274

9.6.4 Zálohování certifikátů	281
9.6.5 Obnova zašifrovaných dat	287

Kapitola 10

Certifikáty a digitální podpisy pro „důvěrnou“ komunikaci **289**

10.1 Požadavky vedoucí k používání digitálních certifikátů	289
10.2 Public Key Infrastructure (Infrastruktura veřejných klíčů)	290
10.2.1 Základní složky PKI	290
10.2.2 Hierarchie a typy certifikačních úřadů	291
10.2.3 Předpoklady pro vytvoření PKI	294
10.3 Instalace certifikačních služeb	295
10.3.1 Instalace prvního certifikačního úřadu v podniku	295
10.3.2 Nainstalované komponenty	298
10.3.3 Instalace podřízeného certifikačního úřadu	299
10.3.4 Zálohování a obnova stávajícího certifikačního úřadu	302
10.4 Proces přidělování certifikátů	305
10.4.1 Podávání žádostí o certifikát	306
10.4.2 Různé druhy šablon certifikátů	311
10.4.3 Kontrola žádostí o certifikát	316
10.5 Další administrátorské úkoly v rámci správy certifikátů	317
10.5.1 Ruční vystavování certifikátů v samostatných certifikačních úřadech	318
10.5.2 Obnova certifikátů	319
10.5.3 Odvolávání certifikátů	324
10.5.4 Zacházení se seznamem odvolaných certifikátů	326
10.5.5 Import a export certifikátů	333
10.5.6 Zásady skupiny pro certifikáty	337
10.5.7 Spolupráce s jinými certifikačními úřady	338

Kapitola 11

Zabezpečení různých síťových služeb **341**

11.1 Požadavky na bezpečnou komunikaci v síti LAN	341
11.2 Umístění síťových služeb v infrastruktuře sítě	342
11.3 Zabezpečení služby DHCP	347
11.3.1 Zamezení neautorizovaných serverů DHCP	348
11.3.2 Zamezení přidělování adres IP neautorizovaným klientům	350

11.3.3 Ochrana databáze DHCP	354
11.3.4 Navázání odpovědi DHCP na segmenty sítě	355
11.4 Zabezpečení služby DNS	356
11.4.1 Zabezpečení serveru DNS	357
11.4.2 Zabezpečení serverů DNS proti neautorizované registraci	360
11.4.3 Další ochranné mechanismy	362
11.5 Zabezpečení terminálových služeb	364
11.5.1 Šifrování dat terminálového serveru	365
11.5.2 Nastavení zabezpečení pro zajištění terminálových serverů	366
11.6 Zabezpečení komunikačních kanálů prostřednictvím protokolu IPSec	369
11.6.1 Síťový model a různé varianty šifrování dat	369
11.6.2 Jednoduché použití protokolu IPSec	371
11.6.3 Konfigurace uživatelských zásad protokolu IPSec	373
11.7 Zabezpečená komunikace v síti prostřednictvím směrování	382
11.7.1 Instalace Network Address Translation	382
11.7.2 Instalace reverzního překladu adres (Reverse NAT)	386
11.7.3 Zamezení komunikace tras	394
11.8 Vzdálený přístup prostřednictvím RAS a VPN	401
11.8.1 Požadavky při připojení vzdálených uživatelů a vzdálených stanovišť	402
11.8.2 Konfigurace zabezpečení autentizace vzdáleného přístupu	402
11.8.3 Konfigurace zabezpečení přenosu dat	405
11.8.4 Stanovení zabezpečení přístupu pomocí zásad vzdáleného přístupu	410
11.8.5 Stanovení zabezpečení pomocí zásad a profilů	412
11.8.6 Doplnkové funkce zabezpečení serverů RAS a VPN	413
11.9 Internet Authentication Service (IAS)	418
11.9.1 RADIUS a IAS	418
11.9.2 Instalace IAS	419

Kapitola 12

Internet a zabezpečení **421**

12.1 Požadavky na přístup na Internet a prezentace na Internetu	421
12.2 Internet Explorer 6.0	422
12.2.1 Definice různých zón zabezpečení	422
12.2.2 Ovlivnění používání souborů cookie (funkce utajení)	425
12.2.3 Využití upřesněných nastavení zabezpečení	429
12.2.4 Používání certifikátů	431

12.3 Zásady skupiny pro využívání Internetu	434
12.3.1 Zásady skupiny pro konfiguraci zabezpečení	434
12.3.2 Schválené prvky ActiveX a moduly plug-in	437
12.3.3 Instalace nastavení Authenticode	438
12.4 IEAK	439
12.5 Zabezpečení při prezentacích na Internetu	440
12.5.1 Služby poskytované IIS	440
12.5.2 Zabezpečovací bariéry IIS	442
12.5.3 Zabezpečení IIS	448

Kapitola 13

Kontrolní fáze (Krok č. 4 managementu bezpečnosti)

455

13.1 Vytvoření katalogu zabezpečení	457
13.2 Nástroje kontroly a varianty testování	458
13.2.1 Manuální testy neboli skripty	458
13.2.2 Dávkové soubory (Batch Jobs)	459
13.2.3 Protokol zabezpečení (Protokol událostí)	463
13.2.4 Konfigurace a analýza zabezpečení	466
13.2.5 HFNetChk	468
13.3 Reakce na kontrolu implementace	472

Příloha

475

P.1 „Class ID“ standardních modulů snap-in pod Windows 2000	475
P.1.1 Samostatné moduly snap-in	475
P.1.2 Rozšíření modulů snap-in	477
P.1.3 Moduly snap-in zásad skupiny	479
P.2 Užitečné internetové adresy	479
P.3 Kontrolní seznamy konfigurace zabezpečení	480
P.4 Pomůcka pro plánování implementace standardů zabezpečení	481
P.5 Seznam všech RFC použitých v této knize	482
P.6 Znamé porty pod Windows 2000	483

Rejstřík

487