Stručný obsah

Úvod 27

Část 1: Klíčové principy zabezpečení

Kapitola 1: Klíčové principy zabezpečení 33
Kapitola 2: Poznejte svého protivníka 43

Část 2: Zabezpečení služby Active Directory

Kapitola 3: Konfigurace zabezpečení uživatelských účtů a hesel 59
Kapitola 4: Konfigurace ověřování systémů Microsoft Windows 95
Kapitola 5: Konfigurace zabezpečení služby Active Directory 113
Kapitola 6: Implementace zásad skupiny s ohledem na bezpečnost 127
Kapitola 7: Návrhy domén a doménových struktur s ohledem na bezpečnost 143

Část 3: Zabezpečení jádra operačního systému

Kapitola 8: Řízení přístupu k datům 161
Kapitola 9: Správa zabezpečení systémových služeb 187
Kapitola 10: Implementace zabezpečení protokolu TCP/IP 217
Kapitola 11: Tvorba a konfigurace šablon zabezpečení 253
Kapitola 12: Správa zabezpečení a soukromí v Microsoft Internet Exploreru 293
Kapitola 13: Správa zabezpečení a soukromí v Microsoft Office XP 319
Kapitola 14: Správa zabezpečení a soukromí v Microsoft Office System 2003 327
Kapitola 15: Auditování událostí zabezpečení Microsoft Windows 337
Kapitola 16: Implementace zabezpečení přenosných počítačů 365

Část 4: Zabezpečení obvyklých služeb

Kapitola 17: Implementace zabezpečení řadičů domén 383
Kapitola 18: Implementace zabezpečení serveru DNS 405
Kapitola 19: Implementace zabezpečení terminálových služeb 419
Kapitola 20: Implementace zabezpečení serveru DHCP 433
Kapitola 21: Implementace zabezpečení serveru WINS 443
Kapitola 22: Implementace bezpečnosti při směrování a vzdáleném přístupu 451
Kapitola 23: Implementace zabezpečení certifikační služby 477
Kapitola 24: Implementace zabezpečení Microsoft IIS 491
Kapitola 25: Návrh infrastruktury pro ověřování v sítích 802.1x 527

Část 5: Správa bezpečnostních aktualizací

Kapitola 26: Řízení opravných aktualizací 557
Kapitola 27: Nástroje pro řízení oprav 573

Část 6: Plánování a posuzování bezpečnosti a reakce na incidenty

Kapitola 28: Posuzování zabezpečení sítě 605
Kapitola 29: Nástroje pro posuzování bezpečnosti 619
Kapitola 30: Příprava na bezpečnostní události 645
Kapitola 31: Reakce na bezpečnostní události 663
Rejstřík 685

Obsah

Úvod 27

Část 1: Klíčové principy zabezpečení

Kapitola 1

Klíčové principy zabezpečení 33

1.1 Principy řízení rizika 34
Učíme se řídit riziko 34
Strategie řízení rizik 36

1.2 Principy zabezpečení 38
Udělení minimálních potřebných oprávnění 38
Důkladná ochrana 38
Omezení plochy útoku 38
Vyhýbání se předpokladům 39
Ochrana, zjištění a reakce 39
Zabezpečení při vývoji, při výchozím nastavení a při implementaci 39
Deset neměnných zákonů zabezpečení 39
Deset neměnných zákonů bezpečné správy 41

Kapitola 2

Poznejte svého protivníka 43

2.1 Vědomosti o vlastní síti 44
Přesné ohodnocení vlastních odborných znalostí 44

2.2 Udržování podrobné dokumentace o síti organizace 45

2.3 Zjištění úrovně poskytované organizační podpory 45

2.4 Identifikace útočníka 46
Poznání vnějších útočníků 47
Poznání vnitřních útočníků 48

2.5 Motivace útočníků 48
Proslulost, přijetí a ego 49
Finanční zisk 50
Výzva 51
Aktivismus 52
Pomsta 52
Špionáž 52
Informační válka 53

2.6 Proč je obrana sítí složitá 53
Útočníci mají neomezené prostředky 53
Útočníci musí zvládnout pouze jediný útok 54
Obránci nemohou přejít do útoku 54
Obránci musí plnit obchodní cíle 54
Obránci musí vždy zvítězit 55

Část 2: Zabezpečení služby Active Directory

Kapitola 3

Konfigurace zabezpečení uživatelských účtů a hesel 59

3.1 Zabezpečení účtů 60
Principy identifikátorů zabezpečení 60
Principy přístupových tokenů 69
Konfigurace možností zabezpečení účtu 70
Zabezpečení účtů pro správu 72
Implementace zabezpečení hesla účtu 74
3.2 Přidělování práv a oprávnění prostřednictvím skupin 80
Uživatelská práva a oprávnění 81
Oprávnění ke službě Active Directory, k souborům a k registrům 87
Typy skupin a jejich rozsah 87
Implementace zabezpečení podle rolí 90
3.3 Doporučené postupy 92
3.4 Další informace 93

Kapitola 4

Konfigurace ověřování systémů Microsoft Windows 95

4.1 Uchování a přenos pověření 96
LAN Manager 97
NTLM 100
NTLMv2 100
Kerberos 102
4.2 Ukládání utajovaných informací v systému Windows 107
Utajovaná data místního úřadu zabezpečení 107
Rozhraní Data Protection API 109
Pověření uložená v mezipaměti 109
Správce pověření 110
4.3 Doporučené postupy 111
4.4 Další informace 111

Kapitola 5

Konfigurace zabezpečení služby Active Directory 113

5.1 Principy schématu služby Active Directory 114
Atributy 114
Třídy 115

5.2 Konfigurace seznamů DACL pro zabezpečení objektů služby Active Directory **116**
Co jsou to seznamy DACL? 117
Funkce seznamů DACL 119
5.3 Zabezpečení objektů a atributů služby Active Directory **120**
Konfigurace výchozích seznamů DACL u objektů a atributů 121
Zabezpečení objektů po vytvoření 121
Konfigurace seznamů DACL z příkazového řádku 123
5.4 Doporučené postupy **124**
5.5 Další informace **125**

Kapitola 6
Implementace zásad skupiny s ohledem na bezpečnost **127**
6.1 Principy zásad skupiny **128**
Zásady skupiny související s počítačem 129
Zásady související s uživateli 131
Použití objektů zásad skupiny 132
6.2 Zpracování objektů zásad skupiny **134**
Počáteční použití zásad skupiny 134
Aktualizace zásad skupiny 135
Vyžádané zpracování 135
6.3 Úpravy použití zásad skupiny **136**
Blokování dědičnosti 136
Potlačení přepisování nastavení 136
Filtrování objektů zásad skupiny 137
Režim zpětné smyčky 137
6.4 Správa zásad skupiny **138**
Výchozí oprávnění k zásadám skupiny 138
Delegování správy zásad skupiny 139
6.5 Doporučené postupy **140**
6.6 Další informace **140**

Kapitola 7
Návrhy domén a doménových struktur s ohledem na bezpečnost **143**
7.1 Autonomie a izolace ve službě Active Directory **144**
7.2 Návrh doménových struktur pro služby Active Directory **145**
Hranice správy rozlehlé sítě a izolace správy 145
Řízení výchozích oprávnění a schématu 146
Hranice globálního katalogu 146
Požadavky na důvěryhodnost domén 147
Izolace řadičů domén 148

Ochrana kořenové domény doménové struktury 149
7.3 Návrh domén pro zabezpečení služby Active Directory 151
7.4 Návrh služby DNS pro zabezpečení služby Active Directory 152
Jeden obor názvů 153
Delegovaný obor názvů 153
Interní obor názvů 154
Rozdělený obor názvů 154
7.5 Návrh delegování oprávnění 155
7.6 Doporučené postupy 156
7.7 Další informace 158

Část 3: Zabezpečení jádra operačního systému

Kapitola 8
Řízení přístupu k datům 161
8.1 Jak zabezpečit oprávnění k souborům a složkám 162
Jak fungují diskrétní seznamy řízení přístupu (DACL) 165
Přiřazení DACL v okamžiku vytvoření 167
Co se děje s DACL při kopírování a přesunu souborů a složek 167
Nástroje příkazového řádku 169
Zabezpečení přístupu k souborům a složkám pomocí oprávnění ke sdílení 173
8.2 Souborový systém EFS 174
Jak EFS funguje 174
Nástroje příkazového řádku pro systém EFS 176
Další funkce EFS v systémech Windows 2003 Server a Windows XP 179
Úvod do návrhu zásad pro Agenta obnovení dat 180
8.3 Jak zabezpečit oprávnění k systémovému registru 183
Konfigurace oprávnění k registru 184
8.4 Doporučené postupy 185
8.5 Další informace 185

Kapitola 9
Správa zabezpečení systémových služeb 187
9.1 Správa oprávnění ke službám 188
Konfigurace spouštěcí hodnoty služby 189
Zastavení, spuštění, pozastavení a obnovení služby 190
Konfigurace kontextu zabezpečení služeb 191
Konfigurace diskrétního přístupového seznamu služby DACL 192
9.2 Výchozí služby ve Windows 2003 Server, Windows 2000 a Windows XP 194
9.3 Doporučené postupy 213
9.4 Další informace 215

Kapitola 10
Implementace zabezpečení protokolu TCP/IP 217
10.1 Zabezpečení protokolu TCP/IP 218
Protokoly internetové vrstvy 218
Protokoly přenosové vrstvy 221
Nejběžnější hrozby vůči protokolu TCP/IP 223
Konfigurace zabezpečení TCP/IP ve Windows 226
10.2 Protokol IPSec 237
Zabezpečení přenosu dat pomocí protokolů IPSec 237
Výběr režimu činnosti IPSec 240
Výběr metody ověřování IPSec 240
Vytvoření zásady IPSec 241
Jak protokol IPSec funguje 245
Monitorování protokolu IPSec 247
10.3 Doporučené postupy 250
10.4 Další informace 251

Kapitola 11
Tvorba a konfigurace šablon zabezpečení 253
11.1 Nastavení šablon zabezpečení 254
Zásady účtů 255
Místní zásady 257
Protokoly událostí 275
Skupiny s omezeným členstvím 277
Systémové služby 277
Nastavení registru 277
Nastavení souborového systému 277
Zásady pro bezdrátovou síť (IEEE 802.11) 277
Zásady veřejného klíče 278
Zásady omezení softwaru 279
Zásady zabezpečení protokolu IP 281
11.2 Jak fungují šablony zabezpečení 282
Aplikace šablon zabezpečení na místní počítač 282
Aplikace šablon zabezpečení pomocí zásady skupiny 285
11.3 Výchozí šablony zabezpečení 286
11.4 Vytvoření vlastní šablony zabezpečení 287
Přidání položek registru do možností zabezpečení 287
Přidání služeb, hodnot registru a souborů do šablony zabezpečení 290
11.5 Doporučené postupy 290
11.6 Další informace 290

Kapitola 12

Správa zabezpečení a soukromí v Microsoft Internet Exploreru 293
12.1 Nastavení zabezpečení v Internet Exploreru 294
Nastavení soukromí 294
Blokování automaticky otevíraných oken 297
Zóny zabezpečení 298
Globální nastavení zabezpečení 313
Rozšířená konfigurace zabezpečení ve Windows Serveru 2003 314
Konfigurace nastavení soukromí a zabezpečení v Internet Exploreru 315
12.2 Doporučené postupy 316
12.3 Další informace 317

Kapitola 13

Správa zabezpečení a soukromí v Microsoft Office XP 319
13.1 Konfigurace zabezpečení ovládacích prvků ActiveX a maker 320
13.2 Ochrana dokumentů v Office XP 321
Ochrana dokumentu pro čtení 322
Ochrana metadat v dokumentu 322
Chránění obsahu dokumentu 323
13.3 Konfigurace zabezpečení v Outlooku 2002 324
Zabezpečení příloh 324
Ochrana zpráv ve formátu HTML 325
13.4 Doporučené postupy 325
13.5 Další informace 325

Kapitola 14

Správa zabezpečení a soukromí v Microsoft Office System 2003 327
14.1 Konfigurace zabezpečení ovládacích prvků ActiveX a maker 328
14.2 Ochrana dokumentů v Microsoft Office System 2003 330
Ochrana dokumentu pro čtení 330
Ochrana metadat v dokumentu 331
Chránění obsahu dokumentu 332
14.3 Konfigurace zabezpečení v Outlooku 2003 332
Zabezpečení příloh 333
Ochrana zpráv ve formátu HTML 333
14.4 Doporučené postupy 334
14.5 Další informace 334

Kapitola 15

Auditování událostí zabezpečení Microsoft Windows 337
15.1 Které události budou podléhat auditu 338
15.2 Práce s Prohlížečem událostí 339
Stanovení místa pro ukládání protokolu 340
Stanovení maximální velikosti souboru protokolu 341
Konfigurace chování při přepisování 341
15.3 Konfigurace zásad auditování 342
Auditování událostí přihlášení k účtu 343
Auditování událostí správy účtu 346
Auditování událostí přístupu k adresářové službě 348
Auditování událostí přihlášení 349
Auditování přístupu k objektům 351
Auditování změny zásad 354
Auditování používání oprávnění 355
Auditování sledování procesů 356
Auditování systémových událostí 357
Jak povolit zásady auditování 357
15.4 Monitorování auditovaných událostí 359
Práce s Prohlížečem událostí 359
Vlastní skripty 360
Nástroj Event Comb 360
15.5 Doporučené postupy 362
15.6 Další informace 363

Kapitola 16

Implementace zabezpečení přenosných počítačů 365
16.1 Vlastnosti přenosných počítačů 366
Zvýšené riziko ztráty a krádeže 366
Obtížná aplikace bezpečnostních aktualizací 368
Vystavení rizikovému prostředí nedůvěryhodných sítí 369
Riziko odposlechu v bezdrátové síti 369
16.2 Implementace doplňkového zabezpečení přenosných počítačů 370
Ochrana hardwaru 370
Ochrana spuštění systému 371
Ochrana dat 373
Školení uživatelů 375
16.3 Zabezpečení bezdrátových sítí ve Windows XP 375
Služba Wireless Zero Configuration ve Windows XP 375
Konfigurace zabezpečení připojení bezdrátové sítě 802.11 376
16.4 Doporučené postupy 379

16.5 Další informace 379

Část 4: Zabezpečení obvyklých služeb

Kapitola 17

Implementace zabezpečení řadičů domén 383

17.1 Jakým hrozbám jsou řadiče domén vystaveny 384
Modifikace nebo přidávání objektů služby Active Directory 384
Útoky na heslo 384
Útoky s odepřením služeb (DoS) 384
Útoky s vyřazením replikací 385
Zneužití známých zranitelných míst 385
17.2 Implementace zabezpečení na řadičích domény 385
Zajištění fyzické bezpečnosti 386
Zvýšení bezpečnosti uložených hesel 386
Vypnutí nepotřebných služeb 387
Aplikace bezpečnostních nastavení pomocí zásad skupiny 393
Ochrana proti výpadku řadiče domény 394
Implementace systémového klíče Syskey 394
Zabezpečení vestavěných účtů a skupin 395
Zapnutí auditování 396
Zabezpečení komunikace ve službě Active Directory 396
Omezení množiny uživatelů, kteří smí být ověřeni na konzole řadiče domény 399
17.3 Doporučené postupy 399
17.4 Další informace 402

Kapitola 18

Implementace zabezpečení serveru DNS 405

18.1 Jakým hrozbám jsou servery DNS vystaveny 407
Změny v záznamech služby DNS 407
Přenosy zón s daty DNS do neoprávněného serveru 408
Prozrazení vnitřního schématu adresování IP 408
Útoky s odepřením služeb (DoS) proti službám DNS 408
Vyřazení přístupu k záznamům prostředků DNS v kořenové doméně struktury 408
18.2 Zabezpečení serveru DNS 409
Implementace zón integrovaných se službou Active Directory 409
Implementace samostatného vnitřního a vnějšího názvového serveru DNS 411
Omezení přenosu zón 412
Implementace protokolu IPSec mezi klienty DNS a servery DNS 413
Omezení provozu DNS ve firewallu 414
Omezení správy DNS 414
Ochrana mezipaměti služby DNS 414
18.3 Doporučené postupy 415
18.4 Další informace 416

Kapitola 19
Implementace zabezpečení terminálových služeb 419
19.1 Jakým hrozbám jsou terminálové služby vystaveny 420
Udělování nadměrných oprávnění uživatelům 421
Obcházení firewallového zabezpečení 421
Nutnost mít uživatelské právo Přihlásit se místně 421
Útočník získá plný přístup k ploše Windows 422
19.2 Zabezpečení terminálových služeb 422
Výběr správného režimu činnosti terminálových služeb 422
Omezení množiny uživatelů a skupin, kterým je uděleno právo připojení k terminálovému serveru 424
Omezení množiny spouštěných aplikací 424
Implementace nejsilnějšího možného šifrování 426
Posílení bezpečnostní konfigurace terminálového serveru 427
Vyšší zabezpečení při ověřování ve Windows 2003 Server SP1 428
19.3 Doporučené postupy 430
19.4 Další informace 432

Kapitola 20
Implementace zabezpečení serveru DHCP 433
20.1 Jakým hrozbám jsou vystaveny servery DHCP 434
Neoprávněné servery DHCP 435
Když server DHCP přepíše platné záznamy prostředků ve službě DNS 435
Když server DHCP nepřebírá vlastnictví záznamů prostředků ve službě DNS 436
Neoprávněný klient DHCP 436
20.2 Zabezpečení serveru DHCP 436
Ponechání výchozího chování při registraci názvů 437
Které účty budou členem skupiny DnsUpdateProxy 437
Kontrola položek BAD_ADDRESS v databázi DHCP 438
Sledování členství ve skupině DHCP Administrators 439
Povolení auditování DHCP 439
20.3 Doporučené postupy 439
20.4 Další informace 441

Kapitola 21
Implementace zabezpečení serveru WINS 443
21.1 Jakým hrozbám jsou servery WINS vystaveny 445
Vyřazení replikací mezi servery WINS 445
Registrace falešných záznamů služby NetBIOS 445
Nesprávná registrace záznamů WINS 445
Zásahy do konfigurace služby WINS 446
Útoky s odepřením služeb (DoS) proti serveru WINS 446

21.2 Zabezpečení serveru WINS 446
Sledování členství ve skupinách pro správu 446
Ověřování konfigurace replikací ve službě WINS 447
Implementace statických položek WINS pro kriticky důležité aplikace NetBIOS 447
Vyřazení aplikací NetBIOS z provozu 447
Implementace podrobného záznamu služby WINS do protokolu událostí 448
21.3 Doporučené postupy 448
21.4 Další informace 450

Kapitola 22
Implementace bezpečnosti při směrování a vzdáleném přístupu 451
22.1 Součásti řešení vzdáleného přístupu 452
Ověřovací protokoly 452
Protokoly sítí VPN 454
Klientský software 454
Serverové služby a software 455
Karanténní služby 455
22.2 Jakým hrozbám je vzdálený přístup vystaven 456
Odposlech ověřování 456
Odposlech dat 457
Obcházení firewallu při vstupu do privátní sítě 457
Nestandardní uplatnění zásad 458
Rozšíření obvodu sítě o místo připojení vytáčeného uživatele 458
Odepření služeb (DoS) vzniklé nadměrným počtem pokusů o zadání hesla 458
Krádež přenosného počítače s uloženým pověřením 459
Připojení vzdáleného klienta, který nevyhovuje bezpečnostním požadavkům platným ve firemní síti 459
22.3 Zabezpečení serverů pro vzdálený přístup 460
Implementace ověřování a účtování s protokolem RADIUS 460
Zabezpečení provozu při ověřování RADIUS mezi serverem vzdáleného přístupu a serverem RADIUS 461
Konfigurace zásad vzdáleného přístupu 461
Zavedení povinných certifikátů v protokolu L2TP/IPSec 463
Omezení množiny serverů, které smí spouštět a zastavovat službu RRAS 465
Implementace uzamčení účtů při vzdáleném přístupu 466
Implementace karanténního řešení 466
22.4 Zabezpečení klientů se vzdáleným přístupem 471
Konfigurace balíků CMAK 471
Implementace silného ověřování 472
Zavedení povinných certifikátů 472
22.5 Doporučené postupy 473
22.6 Další informace 474

Kapitola 23

Implementace zabezpečení certifikační služby 477
23.1 Jakým hrozbám je certifikační služba vystavena 478
Ohrožení páru klíčů certifikačního úřadu 478
Útoky proti serverům, na kterých jsou uloženy seznamy odvolaných certifikátů (CRL) 479
Pokus o změnu konfigurace certifikačního úřadu 479
Pokus o změnu šablony certifikátů 479
Útoky, které vyřazují z činnosti kontrolu odvolaných certifikátů ze seznamu CRL 480
Přidání nedůvěryhodného certifikačního úřadu do důvěryhodného kořenového úložiště CÚ 480
Vydání falešných certifikátů 480
Publikování falešných certifikátů do služby Active Directory 481
Ohrožení certifikačního úřadu jediným správcem 481
Neoprávněné obnovení soukromého klíče uživatele z databáze certifikačního úřadu 481
23.2 Zabezpečení certifikační služby 482
Implementace fyzických bezpečnostních opatření 482
Implementace logických bezpečnostních opatření 483
Změna míst publikace seznamu odvolaných certifikátů (CRL) a certifikátů CÚ 486
Kontrola seznamu odvolaných certifikátů (CRL) ve všech aplikacích 486
Správa oprávnění k šablonám certifikátů 487
Oddělení rolí 487
23.3 Doporučené postupy 488
23.4 Další informace 489

Kapitola 24

Implementace zabezpečení Microsoft IIS 491
24.1 Implementace zabezpečení Windows 492
Provozování minimální množiny potřebných služeb 493
Definice uživatelských účtů pro anonymní přístup 493
Zabezpečení souborového systému 494
Aplikování konkrétních nastavení v registru 495
24.2 Společná bezpečnostní nastavení IIS ve Windows 2000 a 2003 Server 496
Ověřování 496
Oprávnění k webům 501
Komunikační kanály 502
24.3 Implementace dalších bezpečnostních opatření ve verzi IIS 5.0 506
Nástroj IIS Lockdown 506
Filtr URLScan 511
Instalace filtru URLScan 511
24.4 Implementace dalších bezpečnostních opatření ve verzi IIS 6.0 515
Snížení okruhu požadovaných oprávnění 516
Automatické monitorování provozního stavu systému 517
Izolace aplikací 518

Zlepšené zabezpečení součástí Http.sys 519
Podpora zabezpečení služby ASP.NET 519
Zabezpečení výchozích nastavení 520
Ochrana proti známým útokům 521
24.5 Konfigurace služby FTP 522
24.6 Doporučené postupy 523
24.7 Další informace 525

Kapitola 25
Návrh infrastruktury pro ověřování v sítích 802.1x 527
25.1 Jak funguje ověřování v sítích 802.1x 528
25.2 Jakým hrozbám je vystaveno síťové prostředí 530
25.3 Typy ověřování v síti 802.1x 532
Ověřování EAP-TLS 532
Ověřování PEAP 533
25.4 Ochrana komunikací 533
Ochrana bezdrátové komunikace 533
Ochrana komunikace v pevné síti 535
25.5 Příprava certifikátů pro ověřování 802.1x 536
Certifikáty počítačů u serverů RADIUS 536
Uživatelské certifikáty pro klienty 536
Certifikáty počítačů pro klienty 537
25.6 Zavedení certifikátů pro uživatele a počítače 537
Server RADIUS 537
Klientské počítače 538
Uživatelé 539
25.7 Implementace ověřování 802.1x 540
Konfigurace serveru RADIUS 540
Konfigurace bezdrátového přístupového bodu nebo přepínače 546
Konfigurace přepínače 546
Připojení k bezdrátové síti 547
Připojení k pevné síti 549
25.8 Doporučené postupy 551
25.9 Další informace 552

Část 5: Správa bezpečnostních aktualizací

Kapitola 26
Řízení opravných aktualizací 557
26.1 Typy oprav 558
26.2 Vývoj bezpečnostních aktualizací 560
26.3 Řízení oprav v šesti krocích 562

Krok 1: oznámení 562
Krok 2: posouzení 563
Krok 3: získání 564
Krok 4: přezkoušení 567
Krok 5: nasazení 568
Krok 6: ověření 570
26.4 Doporučené postupy 571
26.5 Další informace 571

Kapitola 27
Nástroje pro řízení oprav 573
27.1 Katalog oprav Security Patch Bulletin Catalog 575
27.2 Služba Windows Update 577
27.3 Automatické aktualizace 580
27.4 Služba Microsoft Software Update Services 581
Jak služba SUS funguje 581
Konfigurace serveru SUS 582
Konfigurace klientů SUS 585
27.5 Aktualizace sady Office 587
27.6 Služba Windows Update Services 588
Nové funkce služby Windows Update Services 588
Lepší hospodaření se šířkou pásma 590
Přechod ze služby Software Update Services 591
27.7 Nástroj Microsoft Baseline Security Analyzer 592
Hledání aktualizací v grafickém režimu 593
Kontrola aktualizací v textové verzi nástroje MBSA z příkazového řádku 594
27.8 SMS 2.0 Software Update Services Feature Pack 596
27.9 Microsoft System Management Server 2003 598
Jednodušší správa 598
Jednodušší práce koncových uživatelů 599
27.10 Doporučené postupy 600
27.11 Další informace 601

Část 6: Plánování a posuzování bezpečnosti a reakce na incidenty

Kapitola 28
Posuzování zabezpečení sítě 605
28.1 Typy bezpečnostních posudků 606
Hledání zranitelných míst 606
Penetrační testy 608
Audit bezpečnosti IT 609
28.2 Jak provádět posouzení bezpečnosti 609

Příprava na posouzení bezpečnosti 610
Provedení bezpečnostního posudku 610
Řešení problémů nalezených při posuzování bezpečnosti 611
28.3 Provádění penetračních testů 612
Krok 1: sběr informací 613
Krok 2: zkoumání zranitelných míst 615
Krok 3: záměrné napadení cílové aplikace nebo sítě 616
28.4 Doporučené postupy 617
28.5 Další informace 617

Kapitola 29
Nástroje pro posuzování bezpečnosti 619
29.1 Definice základního zabezpečení 620
Instalace průvodce Security Configuration Wizard 621
Činnosti průvodce Security Configuration Wizard 622
Možnosti průvodce Security Configuration Wizard 623
29.2 Posouzení konfigurace zabezpečení 624
Konzola Security Configuration and Analysis 625
Utilita příkazového řádku Secedit.exe 627
29.3 Provedení bezpečnostního posudku 627
Nástroj Microsoft Baseline Security Analyzer 628
Skenování portů 637
29.4 Doporučené postupy 641
29.5 Další informace 642

Kapitola 30
Příprava na bezpečnostní události 645
30.1 Vytvoření týmu pro reakci na incidenty 646
Výběr osobního garanta opatření 646
Vymezení účastníků 647
Kdo tým povede 648
30.2 Definice politiky reakce na incidenty 649
Rozdělení incidentů do kategorií 649
Návrh proaktivních a reaktivních opatření 650
Vytvoření zásad pro podporu reakcí na incidenty 652
30.3 Vytvoření plánu komunikací 655
Interní komunikace před incidentem 655
Komunikace v průběhu incidentu 657
Kontakt s útočníkem 659
Spolupráce s tiskem 660
30.4 Doporučené postupy 661
30.5 Další informace 661

Kapitola 31

Reakce na bezpečnostní události 663
31.1 Nejčastější projevy bezpečnostního incidentu 665
Neobvyklý provoz TCP/IP nebo UDP 665
Přítomnost jistých událostí v souboru systémového protokolu 666
Nedostupnost síťových prostředků 668
Nadměrné zatížení procesoru 668
Nepravidelný výkon služeb 669
Nepravidelné aktivity souborového systému 669
Změny v oprávněních 670
31.2 Analýza bezpečnostního incidentu 670
Stanovení příčiny 670
Jak zabránit dalšímu zneužívání systému 671
Jak zabránit šíření útoku a dalším incidentům 671
Obnova činnosti služeb 671
Doplnění bezpečnostní politiky o poučení z incidentu 672
Sledování útočníka 672
31.3 Provádění bezpečnostního šetření 673
Vyvolání právního postihu 673
Shromažďování důkazů 675
Sledování sítě 679
31.4 Implementace protiopatření po bezpečnostním incidentu 680
Posouzení rozsahu útoku 680
Nalezení vhodného kompromisu 681
31.5 Obnova činnosti služeb po bezpečnostním incidentu 681
31.6 Ponaučení z bezpečnostního incidentu 682
31.7 Doporučené postupy 683
31.8 Další informace 683
Rejstřík 685

Předmluva

Zabezpečení nemá binární charakter. Není to přepínač nebo dokonce sada přepínačů. Nelze jej popsat v absolutních pojmech. Nevěřte nikomu, kdo se pokouší přesvědčit vás o opaku. Zabezpečení je relativní – existuje pouze vyšší či nižší úroveň zabezpečení. Je navíc dynamické, jelikož vše se neustále mění – lidé, procesy i technologie. V konečném důsledku všechny tyto faktory znesnadňují správu zabezpečení.

Cílem této knihy je poskytnout pomoc při zvyšování, posuzování a správě zabezpečení počítačů se systémy Microsoft Windows 2003, Windows 2000 a Windows XP. Pomůže vám také lépe pochopit, že nedílnou součástí zabezpečení jsou lidé a procesy. Věříme, že uplatníte-li principy, postupy a doporučení, které jsou podrobně popsány v této knize, budete nejen lépe vybaveni pro správu zabezpečení, ale také pro úvahy o zabezpečení.

Hodně štěstí.

Ben Smith a Brian Komar

Březen, 2005

Poděkování

Jména autorů na obálce znamenají deset procent ledovce, který vidíte nad povrchem hladiny. V pozadí každé knihy stojí velké množství zanícených, vysoce kvalifikovaných lidí a tato kniha je ztělesněním této základní pravdy. Při psaní obou verzí tohoto svazku jsme měli štěstí a cítili se poctěni tím, že jsme byli obklopení lidmi s nejlepšími znalostmi v tomto oboru – kniha je také jejich výtvorem.

Od počátku bylo naším cílem napsat knihu, která by byla čtivá a užitečná. Čtenáři, kteří znají autory, zjistí, že Michelle Goodman a Christina Palaia – redaktorky prvního a druhého vydání měly jeden z nejtěžších úkolů: zkrotit naší výmluvnost. Pozornost, se kterou se věnovaly detailům, paměť a pozoruhodná schopnost minimalizovat počet příslovcí použitých ve větách se ukázaly jako neocenitelné. Elizabeth Hansford, Joel Panchot a William Teel odvedli ohromný kus práce na vynikajícím vzhledu knihy, což byl skutečně gargantuovský úkol. Index vytvořil Seth Maislin. Všem děkujeme.

I když z hlediska gramatiky lze považovat za naprosto bezchybné vyjádření, že knihy se píší, ve skutečnosti jsou vytvářeny. Jsme velmi vděčni Karen Szall za nesmírnou práci při sestavování knihy. Rádi bychom také poděkovali prvnímu člověku, který na knize pracoval v roce 2001 – redaktorovi Martinu DelReovi. Ještě jednou mu děkujeme za výdrž.

Obzvláště děkujeme našemu blízkému příteli Ronaldu Beekelaarovi, který přečetl každé slovo této verze a téměř celou první verzi. Jeho vliv na kvalitu knihy je bez přehánění obrovský. Neexistuje lepší odborný korektor nebo redaktor. Toto vydání bylo také posuzováno mnoha našimi kolegy ve společnosti Microsoft, mezi něž patří Andreas Luther, Ayman AlRashed, Allen Stewart, Bill Sisk, Chase Carpenter, Chris Reinhold, Claudio Vacalebre, Dallas Davis, Didier Vandenbroeck, Eric Fitzgerald, George Spanakis, Joel Schaeffer, Jose Luis Auricchio, Joe Davies, Kai Axford, Ken Anderson, Mark Kradel, Mark Pustilnik, Matt Clapham, Matt Kestian, Mike Greer, Ryan Vatne, Shain Wray a Shawn Rabourn. Naše poděkování a ocenění si zaslouží zejména Axman za pečlivé čtení a rady, díky kterým je tato kniha skutečně lepší, a dále Michael Glass za organizaci a pomoc při korektuře. Na závěr dodejme, že všechny chyby a opomenutí jsou pouze a jedině našimi chybami.

Naše poděkování si však hlavně a především zaslouží naše manželky: Beth Boatright a Krista Kunz. Velmi oceňujeme jejich mimořádnou podporu a toleranci – více, než umíme vyjádřit slovy. Děkujeme.

Ben Smith a Brian Komar

Únor, 2005

Úvod

Vítejte v knize Zabezpečení systému a sítě Microsoft Windows, jež je součástí sady Microsoft Windows Server 2003 Resource Kit. Tato kniha nabízí podrobné informace o funkcích zabezpečení v systémech Microsoft Windows Server 2003, Windows 2000 a Windows XP a postupy pro lepší zabezpečení těchto operačních systémů.

Informace o této knize

I když je samozřejmě možné knihu číst od počátku do konce, je kvůli většímu pohodlí čtenáře rozdělena na 6 částí. Každá část je věnována odlišné stránce zabezpečení systémů Windows Server 2003, Windows 2000 a Windows XP a jednotlivé části můžete prozkoumat před implementací zabezpečení do počítačů s těmito systémy nebo je můžete využít při vlastní implementaci jako referenční materiál.

Kniha je rozdělena na následujících šest dílů:

- **Část 1: Klíčové principy zabezpečení** nabízí přehled pro každodenní úvahy o zabezpečení. První část představuje také některé z nejdůležitějších potíží spojených se správou zabezpečení a nabízí postupy k jejich vyřešení.
- **Část 2: Zabezpečení služby Active Directory** poskytuje informace o zabezpečení adresářové služby Active Directory, od řešení otázek souvisejících s doménami a doménovými strukturami po řízení přístupu k objektům a atributům. Druhá část obsahuje podrobné informace o způsobech zabezpečení účtů a ověřování –

což jsou dvě základní součásti zabezpečení systémů Windows Server 2003, Windows 2000 a Windows XP. Tato část také popisuje způsob použití zásad skupiny pro zvýšení zabezpečení sítí používajících službu Active Directory.

- **Část 3: Zabezpečení jádra operačního systému** nabízí podrobné informace o možnostech zvýšení zabezpečení systémů Windows Server 2003, Windows 2000 a Windows XP. Popisuje také postupy pro lepší zabezpečení aplikací, jako je například Microsoft Office System 2003, Microsoft Office XP a Microsoft Internet Explorer, a také mobilních zařízení.
- **Část 4: Zabezpečení běžných služeb** popisuje způsoby zabezpečení běžných služeb spuštěných v systémech Windows Server 2003 a Microsoft Windows 2000 Server, včetně systému DNS (Domain Name System), protokolu DHCP (Dynamic Host Configuration Protocol (DHCP), služby WINS (Windows Internet Name Service) a služeb Terminal Services, Certificate Services, RRAS (Routing and Remote Access Service), Microsoft Internet Information Services 6.0.
- **Část 5: Správa aktualizací zabezpečení** zahrnuje podrobné informace o procesu správy aktualizací zabezpečení, včetně aktualizací Service Pack, aktualizací softwaru a oprav Hotfix a vysvětluje strategie zavádění aktualizací zabezpečení. Pátá část také popisuje metody posuzování zabezpečení počítačů se systémy Windows Server 2003, Windows 2000 a Windows XP.
- **Část 6: Plánování a posouzení zabezpečení a reakcí na události zabezpečení** podrobně vysvětluje posuzování zabezpečení, včetně prohledávání zranitelných míst, auditů IT a testování průniků a popisuje, jak je lze použít k posouzení zabezpečení sítě. Šestá část nabízí také informace týkající se plánování reakcí na události zabezpečení a představuje metody zkoumání těchto událostí.

Doprovodný disk CD-ROM ke knize Resource Kit

Doprovodný disk CD-ROM sady *Microsoft Windows Server 2003 Resource Kit* obsahuje různé nástroje a skripty umožňující efektivnější práci při implementaci a správě zabezpečení počítačů se systémy Windows Server 2003, Windows 2000 a Windows XP. Některé z těchto nástrojů jsou popsány v knize, avšak popis k mnohým z nich zde uveden není. Dokumentaci k jednotlivým nástrojům naleznete ve složce, která obsahuje daný nástroj. Mnoho nástrojů pochází ze sady Microsoft Windows Server 2003 Resource Kit, takže jsou navrženy k implementaci v operačních systémech Windows Server 2003. Zejména se jedná o nástroje a skripty, které se nacházejí v kořenové složce SecurityRKTools. Doprovodný disk CD-ROM obsahuje také elektronickou verzi anglického originálu (e-book) této knihy umožňující její úplné prohledávání.

Poznámka Společnost Microsoft nekontroluje software od jiných výrobců ani odkazy na stránky jiných společností a není tedy zodpovědná za jejich obsah, a proto ani z jejich zahrnutí na tento disk CD-ROM nelze vyvozovat záruku společnosti Microsoft za daný produkt či webový server.

Zásady podpory ke knize Resource Kit

Společnost Microsoft Corporation nepodporuje nástroje a skripty dodávané na doprovodném disku CD-ROM. Společnost Microsoft nezaručuje činnost nástrojů či příkladů skriptů ani žádných oprav chyb těchto nástrojů a skriptů. Nakladatelství Microsoft Press poskytuje zákazníkům, kteří si zakoupili knihu *Zabezpečení systému a sítě Microsoft Windows* nebo sadu *Microsoft Windows Server 2003 Resource Kit*, možnost oznámit případné potíže se softwarem a také získat názory a připomínky k těmto potížím. Chcete-li oznámit nějaké potíže nebo problémy, odešlete e-mailovou zprávu na adresu `rkinput@microsoft.com`. Tato e-mailová adresa je určena pouze pro potíže související se sadou *Microsoft Windows Server 2003 Resource Kit*. Nakladatelství Microsoft Press také prostřednictvím sítě WWW na adrese `http://www.microsoft.com/learning/support/` nabízí opravy ke knihám a doprovodným diskům CD-ROM. Jestliže se chcete připojit přímo k databázi Microsoft Knowledge Base a zadat dotaz týkající se určitého problému nebo potíží, přejděte na adresu `http://support.microsoft.com`. Řešíte-li potíže spojené s operačními systémy Windows, vyhledejte informace o odborné pomoci dodávané s patřičným produktem.

Systémové požadavky

Systémové požadavky na nástroje a skripty

Nástroje zahrnuté na doprovodném disku CD-ROM vyžadují instalaci systému Windows Server 2003, Windows 2000 nebo Windows XP.

Poznámka Doprovodný disk CD-ROM k sadě *Microsoft Windows Server 2003 Resource Kit* obsahuje různé nástroje a skripty. Mnohé z nich pocházejí ze sady Microsoft Windows Server 2003 Resource Kit. Další informace o požadavcích nástrojů naleznete v dokumentaci dodávané s jednotlivými nástroji.

Doporučená konfigurace systému pro elektronickou verzi knihy – eBook

Nejlepšího zobrazení elektronických verzí knih nakladatelství Microsoft Press (eBooks) dosáhnete použitím následující doporučené konfigurace systému:

- systém Microsoft Windows 2003, Windows 2000 nebo Windows XP;
- procesor Pentium II (nebo podobný) 266 MHz nebo rychlejší;
- 64 MB paměti RAM;
- jednotka CD-ROM 8× nebo rychlejší;
- nastavení rozlišení monitoru 800×600 v režimu High Color (16bit);
- aplikace Microsoft Internet Explorer 5.5 nebo novější.