

Spis treści

Część I Podstawy zabezpieczeń Windows

1 Podmioty, użytkownicy i inni aktorzy	3
Trójka podmiot/obiekt/akcja	3
Rodzaje podmiotów zabezpieczeń	4
Użytkownicy	4
Komputery	7
Grupy	7
Pojęcia abstrakcyjne (grupy logowania)	10
Usługi	11
Podmioty zabezpieczeń	12
Komponenty SID	12
Uwierzytelnienia SID	13
SID usług	14
Dobrze znane SID	15
Podsumowanie	16
Dodatkowe źródła	16
2 Jednostki i protokoły uwierzytelniające	17
Co wiemy, co mamy, czym jesteśmy	17
Coś, co wiemy	18
Coś, co mamy	18
Coś, czym jesteśmy	18
Istota magazynów jednostek uwierzytelniających	20
Skrót hash LM	21
Skrót Hash NT	23
Weryfikator hasła	24
W pamięci	25
Szyfrowanie możliwe do odwrócenia	27
Protokoły uwierzytelniające	28
Uwierzytelnienie Basic	29
Protokoły wyzwanie-odpowiedź	29
Uwierzytelniające karty inteligentne	37
Karty inteligentne i hasła	38
Ataki na hasła	38
Zdobywanie haseł	38
Wykorzystanie przechwyconych informacji	42
Ochrona haseł	44
Zarządzanie hasłami	46
Korzystajmy z innych jednostek uwierzytelniających	46
Zapisujmy hasła bezpiecznie	46
Przestańmy myśleć o słowach	47
Ustalmy zasady dotyczące haseł	47
Szczegółowe zasady dotyczące haseł	48
Podsumowanie	54

Dodatkowe źródła.....	54
3 Obiekty: to, czego potrzebujemy	55
Terminologia kontroli dostępu.....	55
Obiekty podlegające zabezpieczeniom	56
Deskryptory bezpieczeństwa	56
Lista kontroli dostępu.....	58
Wpisy listy kontroli dostępu.....	59
Maski dostępu.....	61
Zależności pomiędzy strukturami kontroli dostępu.....	66
Dziedziczenie.....	66
Żetony zabezpieczeń	69
Proces sprawdzania dostępu.....	71
Etykiety integralności	73
DACL puste i NULL.....	74
Język SDDL	75
Narzędzia zarządzania uprawnieniami.....	79
cacls i icacls.....	79
SC	80
subinacl.....	80
Główne zmiany w kontroli dostępu w systemie Windows Server 2008.....	81
Uprawnienia TrustedInstaller	81
SID lokalizacji sieciowej	81
Zmiany przestrzeni nazw systemu plików	81
Usunięcie uprawnień użytkowników zaawansowanych	82
OWNER_RIGHT a prawa właściciela	82
Prawa użytkownika i przywileje	83
RBAC/AZMAN	89
Podsumowanie.....	89
Dodatkowe źródła.....	90
4 Istota kontroli dostępu użytkownika (UAC)	91
Czym jest UAC?	92
Filtrowanie żetonu.....	92
Części składowe kontroli UAC	94
Zapytanie o podniesienie uprawnień użytkownika przez kontrolę UAC	95
Usługa AIS	99
Wirtualizacja plików i rejestru.....	99
Manifesty i żądane poziomy wykonywania	101
Mechanizm wykrywania instalatorów.....	102
Mechanizm UIPI.....	103
Zapytania o podniesienie uprawnień bezpiecznego pulpitu	103
Wykorzystanie pomocy zdalnej	104
Ograniczenia administracyjne zdalnej kontroli UAC	104
Mapowanie dysków sieciowych podczas pracy w trybie	
Admin Approval Mode	105
Blokowanie podnoszenia uprawnień aplikacji podczas logowania	107

Konfigurowanie aplikacji powstały przed systemem Windows Vista	
do współpracy z kontrolą UAC	108
Ustawienia zasad grupy kontroli UAC.....	109
Ustawienia zasady kontroli UAC zlokalizowane w opcjach zabezpieczeń	109
Inne zasady kontroli UAC	111
Nowości w kontroli UAC w systemach Windows Server 2008 i Windows Vista SP1	112
Nowe ustawienia zasad grupy	112
Najlepsze rozwiązania kontroli UAC	113
Podsumowanie.....	114
Dodatkowe źródła.....	114
5 Zapory i ochrona dostępu do sieci	115
Platforma filtrowania systemu Windows	116
Zapora Windows z zabezpieczeniami zaawansowanymi	118
Udoskonalenia Windows Firewall	118
Zarządzanie Windows Firewall.....	122
Usługa RRAS.....	131
Udoskonalenia w usłudze RRAS	131
Protokół IPsec	134
Podstawy protokołu IPsec	134
Nowe funkcje systemu Windows Server 2008	136
Usługa NAP	139
Architektura	140
Wdrożenie usługi NAP	144
Rodzaje działania usługi NAP	147
Podsumowanie.....	149
Dodatkowe źródła.....	149
6 Usługi	151
Wprowadzenie do usług	151
Czym są usługi?	152
Konto logowania się usługi	152
Porty nasłuchiwanie	154
Konfigurowanie usług.....	155
Usługi według roli w systemie Windows Server 2008.....	161
Ataki na usługi.....	161
Robak Blaster	161
Najczęstsze kierunki ataków na usługi.....	163
Wzmacnianie zabezpieczeń usług.....	165
Zasada najmniejszych przywilejów.....	165
Identyfikatory SID usługi	169
Identyfikatory SID ograniczające zapis	172
Ograniczony dostęp sieciowy	174
Izolacja sesji 0	176
Obowiązkowe poziomy integralności	176
Zapobieganie wykonywaniu danych	176
Inne nowe funkcje menedżera SCM.....	177

Zabezpieczanie usług.....	178
Tworzenie listy usług	178
Zmniejszanie liczby uruchamianych usług.....	178
Stosowanie zasady najmniejszych przywilejów dla pozostałych usług	179
Pilnowanie wykonywania aktualizacji.....	179
Tworzenie i używanie niestandardowych kont usług	180
Używajmy Windows Firewall i protokołu IPsec do izolacji sieciowej.....	181
Sprawdzanie błędów usług	181
Promujmy bezpieczne usługi	182
Podsumowanie.....	182
Dodatkowe źródła.....	182
7 Zasady grupy	183
Nowości w systemie Windows Server 2008	183
Podstawy zasad grupy	184
Lokalny obiekt GPO	184
Obiekty GPO oparte na usłudze Active Directory	185
Przetwarzanie zasad grupy.....	191
Nowości w zasadach grupy	194
Usługa zasad grupy.....	194
Szablony ADMX i katalog centralny	195
Obiekty początkowe GPO	196
Komentarze obiektu GPO	199
Ulepszenia filtrowania	200
Nowe zarządzanie zasadami zabezpieczeń	201
Zapora Windows z zabezpieczeniami zaawansowanymi	204
Zasady sieci przewodowych i bezprzewodowych	205
Zarządzanie ustawieniami zabezpieczeń	208
Podsumowanie.....	213
Dodatkowe źródła.....	213
8 Inspekcja.....	215
Czemu służy inspekcja?.....	215
Działanie inspekcji w systemach Windows	216
Konfiguracja zasad inspekcji	218
Opcje zasad inspekcji	223
Tworzenie dobrych zasad inspekcji	225
Nowe zdarzenia w systemie Windows Server 2008	228
Analiza zdarzeń za pomocą wbudowanych narzędzi	233
Event Viewer	233
WEvtUtil.exe.....	238
Podsumowanie.....	239
Część II Implementacja kontroli tożsamości i dostępu za pomocą Active Directory	
9 Projektowanie usług katalogowych pod kątem zabezpieczeń.....	243

Nowy interfejs użytkownika	244
Nowy kreator instalacji AD DS	246
Kontrolery domeny tylko do odczytu	248
Baza danych AD DS tylko do odczytu	249
Filtrowane zestawy atrybutów kontrolera RODC	249
Replikacja jednokierunkowa	250
Buforowanie poświadczzeń	250
DNS tylko do odczytu	252
Instalacja etapowa kontrolerów RODC	252
Restartowalne usługi AD DS	254
Narzędzie instalacji bazy danych Active Directory	255
Inspekcja usług AD DS	257
Inspekcja dostępu do AD DS	257
Przegląd usług AD LDS	261
Przegląd usług AD FS	264
Czym są usługi AD FS?	264
Co nowego w systemie Windows Server 2008?	265
Podsumowanie	266
Dodatkowe źródła	266
10 Implementowanie usług certyfikatów	267
Nowości w PKI w systemie Windows Server 2008	267
Zagrożenia związane z usługą certyfikatów i opcje zmniejszające ryzyko	268
Skompromitowanie pary kluczy urzędu certyfikacji CA	269
Zapobieganie sprawdzaniu odwołania	269
Próby zmiany konfiguracji urzędu CA	272
Próby zmiany szablonu certyfikatów	274
Dodanie niezaufanych urzędów certyfikatów CA do magazynu zaufanego głównego CA	274
Agenci rejestrowania wydający nieautoryzowane certyfikaty	276
Skompromitowanie urzędu CA przez administratora	277
Nieautoryzowane odzyskanie prywatnego klucza użytkownika z bazy danych urzędu certyfikacji	278
Zabezpieczanie usług certyfikatów	279
Wdrażanie fizycznych środków ochrony	279
Najlepsze rozwiązania	280
Podsumowanie	281
Dodatkowe źródła	282
Część III.....Typowe scenariusze zabezpieczeń	
11 Zabezpieczanie ról serwerowych	285
Role a funkcje	286
Domyślne role i funkcje	287
Serwer przed instalacją ról	295
Domyślne miejsce zajmowane przez usługę	296
Instalacja typu Server Core	296

Role obsługiwane przez Server Core	298
Funkcje obsługiwane przez Server Core	298
Co nie jest zawarte w instalacji typu Server Core	299
Narzędzia zarządzające rolami serwera	300
Wstępne zadania konfiguracyjne	300
Kreatory dodawania ról i funkcji	301
Menedżer serwera	301
Kreator konfiguracji zabezpieczeń	304
Serwery o wielu rolach	313
Podsumowanie.....	313
12 Zarządzanie poprawkami	315
Cztery fazy zarządzania poprawkami.....	315
Faza 1: Oszacowanie.....	316
Faza 2: Identyfikacja.....	317
Faza 3: Ocena i plan	319
Faza 4: Wdrażanie.....	321
Anatomia aktualizacji zabezpieczeń	322
Obsługiwane parametry dostępne poprzez wiersz poleceń	322
Integracja plików MSU do pliku obrazu Windows.....	323
Narzędzia w arsenale zarządzania poprawkami.....	323
Centrum pobierania Microsoft.....	323
Katalog Microsoft Update	323
Windows Update i Microsoft Update	325
Automatyczne aktualizowanie systemu Windows	326
Microsoft Baseline Security Analyzer	328
Usługa WSUS.....	332
System Center Essentials 2007	340
Podsumowanie.....	341
Dodatkowe źródła.....	342
13 Zabezpieczanie sieci	343
Wprowadzenie do zależności zabezpieczeń	345
Akceptowalne zależności	346
Nieakceptowane zależności.....	347
Analiza zależności z punktu widzenia ataku	349
Rodzaje zależności.....	350
Zależności użytkowania	350
Zależności oparte na dostępie	350
Zależności administracyjne	353
Zależności konta usługowego.....	353
Zależności funkcjonalne	354
Ograniczanie zależności	354
Krok 1: Utworzenie schematu klasyfikacji	355
Kroki 2 i 3: Modelowanie zagrożeń sieciowych.....	357
Krok 4: Przeanalizować, poprawić, w razie potrzeby powtórzyć	361
Krok 5: Projektowanie strategii izolacji.....	362

Krok 6: Wyprowadzanie strategii roboczej	363
Krok 7: Ograniczenia implementacji	364
Podsumowanie.....	367
Dodatkowe źródła.....	367
14 Zabezpieczanie biura oddziałowego.....	369
Wprowadzenie do kwestii biur oddziałowych.....	369
Dlaczego biura oddziałowe są tak istotne?	370
Co odróżnia biura oddziałowe?	370
Projektowanie biur oddziałowych	371
System Windows Server 2008 w biurze oddziałowym	372
Funkcje niezwiązane z bezpieczeństwem	373
Funkcje zabezpieczające dla biura oddziałowego	375
Inne czynności zabezpieczające.....	389
Podsumowanie.....	390
Dodatkowe źródła.....	390
15 Rozwiązań dla małych firm	391
Utrzymywanie serwerów niskim kosztem	392
Wybór odpowiedniej platformy i ról.....	392
Serwery przeznaczone dla małych firm	395
System Windows Server 2008 Web Edition	395
System Windows Server kryptonim „Cougar”	395
Windows Essential Business Server	399
Utrzymywane serwery	400
Wirtualizacja	400
Złamanie wszystkich zasad przez serwery o wielu rolach	401
Akceptowalne role	402
Komponenty serwera.....	402
Przemyślenie ryzyka	403
Problemy serwerów brzegowych	405
Zapewnianie wsparcia i obsługa aktualizacji.....	406
Zapewnianie odzyskiwania serwera	408
Najlepsze rozwiązania dla małych przedsiębiorstw	409
Postępowanie zgodnie z poradnikiem wzmacniania.....	410
Zasady.....	413
Najlepsze rozwiązania dla dostawców	416
Problemy z dostępem zdalnym	417
Monitorowanie i zarządzanie dodatkami	418
Rola serwera w zarządzaniu i kontroli komputerów biurowych	420
Zalecenia dla dodatkowych konfiguracji serwera.....	423
Podsumowanie.....	428
Dodatkowe źródła.....	428
16 Zabezpieczanie aplikacji serwerowych.....	431
Wprowadzenie.....	431
Serwer IIS 7: Rodowód zabezpieczeń	432
Konfigurowanie serwera IIS 7	433

Delegowanie funkcji.....	434
Zabezpieczenia oparte o protokół TCP/IP	436
Zabezpieczanie adresu IP	436
Zabezpieczanie portów	438
Zabezpieczanie nagłówka hosta.....	439
Zabezpieczenia oparte na prostych ścieżkach.....	439
Definiowanie i ograniczanie fizycznej ścieżki.....	439
Domyślne dokumenty czy przeszukiwanie katalogu?	443
Uwierzytelnienie i autoryzacja	444
Uwierzytelnianie anonimowe.....	445
Uwierzytelnianie podstawowe	446
Mapowanie certyfikatu klienta.....	447
Uwierzytelnianie skrótowe	449
Personifikacja platformy ASP.Net	450
Uwierzytelnianie za pomocą formularzy	451
Uwierzytelnianie systemu Windows	452
Zaufanie do serwera	453
Przyszłe kwestie zabezpieczeń dla serwera IIS	455
Podsumowanie.....	460
Dodatkowe źródła.....	460
Indeks	461