Księgarnia PWN: Jan De Clercq, Guido Grillenmeier - Bezpieczeństwo Microsoft Windows. Podstawy praktyczne

# *Spis treści*

**Przedmowa Tony'ego Redmonda ..... 11**
**Przedmowa Marka Mortimore'a ..... 13**
**Przedmowa Stevena Adlera ..... 17**
**Przedmowa ..... 19**
**Podziękowania ..... 23**

**Część I. Wprowadzenie ..... 25**

**1. Zaufane infrastruktury zabezpieczeń jako wyzwanie ..... 27**
1.1. Wprowadzenie ..... 27
1.2. Rozmieszczenie zaufanych infrastruktur zabezpieczeń ..... 29
1.3. Fundamentalna rola zaufania ..... 32
1.4. Role zaufanej infrastruktury bezpieczeństwa ..... 32
1.4.1. Infrastruktury uwierzytelniania ..... 32
1.4.2. Infrastruktury autoryzacji ..... 35
1.4.3. Infrastruktury zarządzania kluczami ..... 38
1.4.4. Infrastruktury zarządzania zabezpieczeniami ..... 41
1.5. Kolejny etap: federacja ..... 46
1.5.1. Definicja ..... 47
1.5.2. Standardy ..... 48
1.6. Zarządzanie tożsamością i zaufane infrastruktury zabezpieczeń ..... 50
1.6.1. Definicja tożsamości i zarządzania tożsamością ..... 50
1.6.2. Składniki infrastruktury zarządzania tożsamością ..... 52
1.7. Microsoft jako producent zaufanych infrastruktur zabezpieczeń ..... 53
1.7.1. Windows Server 2003 R2 jako blok konstrukcyjny ..... 54
1.7.2. Inne bloki konstrukcyjne firmy Microsoft ..... 55
1.8. Podsumowanie ..... 58

**2. Urzędy i zwierzchnicy zabezpieczeń Windows ..... 59**
2.1. Urzędy zabezpieczeń ..... 59
2.1.1. Lokalne i domenowe urzędy zabezpieczeń ..... 60
2.1.2. Lokalny urząd zabezpieczeń ..... 60
2.1.3. Domenowy urząd zabezpieczeń ..... 66
2.2. Zwierzchnicy zabezpieczeń ..... 75
2.2.1. Identyfikatory zwierzchników ..... 77
2.2.2. Zarządzanie kontami ..... 90
2.2.3. Najważniejsze konta w systemie Windows ..... 95

2.2.4. Poświadczenia w postaci haseł ... 98
2.2.5. Blokowanie kont ... 121

**3. Relacje zaufania Windows ... 131**

3.1. Definicja relacji zaufania ... 131
3.2. Właściwości, typy i cechy zaufania ... 133
3.2.1. Nowe cechy zaufania ... 137
3.2.2. Zaufanie lasu ... 139
3.3. Ograniczanie relacji zaufania ... 143
3.3.1. Filtrowanie identyfikatorów SID ... 144
3.3.2. Uwierzytelnianie selektywne ... 148
3.3.3. Routing sufiksów nazw i ograniczenia nazw najwyższego poziomu ... 154
3.4. Relacje zaufania w praktyce ... 160
3.4.1. Wybór odpowiedniego typu relacji zaufania ... 160
3.4.2. Włączanie rozwiązywania nazw ... 164
3.4.3. Tworzenie relacji zaufania ... 166
3.4.4. Przypisywanie uprawnień w zaufanym środowisku ... 168
3.5. Relacje zaufania: pod maską ... 170
3.6. Zaufanie i bezpieczne kanały ... 175
3.6.1. Kontrolowanie konfiguracji bezpiecznych kanałów ... 176
3.6.2. Sprawdzanie bezpiecznych kanałów ... 176
3.6.3. Dostrajanie usług zabezpieczeń bezpiecznych kanałów ... 177
3.6.4. Narzędzia do zarządzania relacjami zaufania i bezpiecznymi kanałami ... 178
3.7. Relacje zaufania i zapory ogniowe ... 181

**4. Aspekty bezpieczeństwa klientów Windows ... 185**

4.1. Zarys zabezpieczeń klientów ... 185
4.2. Zasada minimalnych przywilejów ... 186
4.2.1. Uruchom jako... ... 189
4.2.2. Szybkie przełączanie użytkowników ... 193
4.2.3. Narzędzia od innych producentów ... 196
4.2.4. Zalety minimalizmu ... 197
4.3. Udoskonalenia zabezpieczeń w Windows XP SP2 ... 198
4.3.1. Zapora systemu Windows ... 199
4.3.2. Ułatwione zarządzanie zabezpieczeniami ... 203
4.3.3. Inne ważne zmiany ... 205
4.4. Zabezpieczenia przeglądarki internetowej ... 206
4.4.1. Nowe zabezpieczenia Internet Explorera w Windows XP SP2 ... 207
4.4.2. Strefy zabezpieczeń w Internet Explorerze ... 214
4.5. Ochrona przed złośliwym kodem mobilnym ... 225
4.5.1. Obrońca Windows (Windows Defender) ... 226
4.5.2. Podsumowanie i ogólne zalecenia dotyczące ochrony przed spyware ... 234
4.6. Używanie zabezpieczeń TPM ... 235
4.6.1. Wymagania urządzeń i oprogramowania TPM ... 238
4.6.2. Embedded Security for HP ProtectTools: implementacja techniczna ... 239
4.6.3. Aplikacje obsługujące HP TPM ... 247
4.7. Ważne zabezpieczenia systemu Windows Vista i przeglądarki IE 7.0 ... 248

**Część II. Uwierzytelnianie ... 251**

**5. Wprowadzenie do uwierzytelniania w systemie Windows ... 253**

5.1. Podstawy uwierzytelniania ... 253
5.1.1. Terminologia ... 253
5.1.2. Podział uwierzytelniania ... 255
5.2. Podstawy uwierzytelniania w systemie Windows ... 258
5.2.1. Założenia teoretyczne ... 258
5.2.2. Architektura uwierzytelniania ... 262
5.2.3. Uwierzytelnianie w czasie startu komputera i logowania użytkownika ... 270
5.3. Prawa logowania ... 275
5.3.1. Zarządzanie prawami logowania Windows ... 279
5.3.2. Sprawdzone rozwiązania ... 280
5.4. Uwierzytelnianie NTLM ... 281
5.4.1. Protokół NTLM ... 281
5.4.2. Odmiany NTLM ... 283
5.4.3. Kontrolowanie podprotokołów NTLM ... 285
5.4.4. Wyłączanie przechowywania wartości mieszania LM ... 287
5.5. Dostęp anonimowy ... 291
5.6. Buforowanie poświadczeń ... 297
5.7. Ograniczanie liczby jednoczesnych sesji logowania ... 301
5.7.1. Działanie programu LimitLogin ... 302
5.7.2. Architektura i komponenty LimitLogin ... 303
5.7.3. Instalacja LimitLogin ... 305
5.7.4. Konfiguracja programu LimitLogin ... 307
5.8. Ogólne zasady rozwiązywania problemów z uwierzytelnianiem ... 311
5.8.1. Dzienniki zdarzeń związanych z uwierzytelnianiem ... 311
5.8.2. Dzienniki usługi Netlogon ... 317
5.9. Co znajduje się w innych rozdziałach na temat uwierzytelniania? ... 319

**6. Kerberos ... 321**

6.1. Wprowadzenie do protokołu Kerberos ... 321
6.1.1. Zalety protokołu Kerberos ... 322
6.1.2. Porównanie uwierzytelniania Kerberos z NTLM ... 325
6.2. Kerberos: protokół podstawowy ... 326
6.2.1. Założenia projektu Kerberos ... 327
6.2.2. Krok 1: Uwierzytelnianie Kerberos opiera się na kryptografii klucza symetrycznego ... 328
6.2.3. Krok 2: Centrum KDC Kerberos jest skalowalne ... 330
6.2.4. Krok 3: Bilet zapewnia bezpieczny transport klucza sesji ... 332
6.2.5. Krok 4: Centrum KDC rozprowadza klucze sesji, wysyłając je do klienta ... 334
6.2.6. Krok 5: Bilet TGT ogranicza używanie kluczy głównych ... 336
6.2.7. Wszystkie elementy układanki ... 340
6.2.8. Usługi poufności, uwierzytelniania i integralności danych Kerberos ... 342
6.2.9. Uwierzytelnianie użytkownik-użytkownik ... 342

6.2.10. Numery wersji klucza ... 344
6.3. Logowanie się do systemu Windows za pomocą protokołu Kerberos ... 345
6.3.1. Logowanie w środowisku jednodomenowym ... 345
6.3.2. Logowanie w środowisku wielodomenowym ... 350
6.3.3. Logowanie w środowiskach z wieloma lasami ... 360
6.4. Kerberos dla zaawansowanych ... 362
6.4.1. Delegacja uwierzytelniania ... 362
6.4.2. Od uwierzytelniania do autoryzacji ... 376
6.4.3. Analiza biletu i wartości uwierzytelniającej Kerberos ... 385
6.4.4. Znaczenie czasu w uwierzytelnianiu Kerberos ... 402
6.4.5. Aplikacje obsługujące protokół Kerberos ... 403
6.5. Konfiguracja protokołu Kerberos ... 406
6.5.1. Ustawienia GPO ... 406
6.5.2. Właściwości kont ... 408
6.5.3. Protokoły transportu i porty ... 409
6.6. Rozwiązywanie problemów z działaniem protokołu Kerberos ... 410
6.6.1. Przeglądanie zdarzeń ... 410
6.6.2. Narzędzia do rozwiązywania problemów ... 412
6.7. Współdziałanie protokołu Kerberos ... 413
6.7.1. Implementacje innych producentów ... 413
6.7.2. Porównanie protokołu Kerberos w systemie Windows z innymi implementacjami ... 414
6.7.3. Scenariusze współdziałania ... 415

**7. Uwierzytelnianie IIS ... 425**

7.1. Domyślne zabezpieczenia w IIS 6.0 ... 425
7.2. Wprowadzenie do uwierzytelniania IIS ... 427
7.3. Uwierzytelnianie HTTP ... 430
7.3.1. Dostęp anonimowy ... 431
7.3.2. Uwierzytelnianie podstawowe ... 434
7.3.3. Uwierzytelnianie digest ... 438
7.4. Zintegrowane uwierzytelnianie Windows ... 441
7.5. Uwierzytelnianie Passport ... 443
7.5.1. Passport i Windows Live ID ... 444
7.5.2. Technologie WWW obsługujące Passport ... 445
7.5.3. Infrastruktura usługi Passport ... 446
7.5.4. Wymiana podstawowych komunikatów w uwierzytelnianiu Passport ... 447
7.5.5. Zmiany użytkownika Passport w systemach Windows XP i Windows Server 2003 ... 449
7.5.6. Pliki cookie ... 451
7.5.7. Passport a informacje personalne ... 456
7.5.8. Integracja uwierzytelniania Passport z systemem Windows Server 2003 ... 457
7.6. Uwierzytelnianie za pomocą certyfikatów ... 459
7.6.1. Konfiguracja SSL ... 462
7.6.2. Obsługa SSL w przeglądarce internetowej ... 476
7.6.3. Sprawdzanie ważności certyfikatów ... 477

7.6.4. Uwagi na temat wdrażania ... 481
7.7. Porównanie metod uwierzytelniania IIS ... 488

**8. Integracja uwierzytelniania w systemach UNIX/Linux i Windows ... 489**

8.1. Porównanie uwierzytelniania w systemach UNIX/Linux i Windows ... 490
8.2. Technologie umożliwiające współdziałanie ... 491
8.2.1. LDAP ... 491
8.2.2. Kerberos ... 494
8.3. Pojęcia związane z zabezpieczeniami systemów UNIX/Linux ... 495
8.3.1. PAM ... 496
8.3.2. Usługi nazw ... 499
8.3.3. NSS ... 500
8.3.4. Pliki lokalne ... 502
8.3.5. NIS ... 503
8.3.6. NIS+ ... 504
8.3.7. Integracja NIS i LDAP ... 505
8.3.8. Samba ... 507
8.4. Propozycje integracji zarządzania kontami i uwierzytelniania w systemach UNIX/Linux i Windows ... 509
8.4.1. Rozwiązania umożliwiające koegzystencję infrastruktur NIS i AD ... 510
8.4.2. Rozwiązania umożliwiające scentralizowane zarządzanie użytkownikami za pomocą repozytorium AD/LDAP ... 522
8.5. Podsumowanie ... 540

**9. Jednokrotne logowanie (SSO) ... 543**

9.1. SSO: Zalety i wady ... 543
9.2. SSO w sieci WWW a SSO w firmie ... 544
9.3. Architektury SSO ... 545
9.3.1. Proste architektury SSO ... 545
9.3.2. Złożone architektury SSO ... 547
9.3.3. Architektury SSO: podsumowanie ... 558
9.4. Zwiększanie zasięgu SSO ... 560
9.4.1. Obejmowanie zasięgiem SSO różnych organizacji ... 560
9.4.2. Obejmowanie zasięgiem SSO różnych aplikacji ... 562
9.5. Technologie SSO firmy Microsoft ... 562
9.5.1. Menedżer poświadczeń ... 563
9.5.2. BizTalk Server i Host Integration Server – SSO dla firm ... 568
9.5.3. SSO w SPS 2003 ... 578
9.5.4. Active Directory Federation Services ... 581
9.5.5. IAS (Internet Authentication Service) ... 585
9.6. Podsumowanie ... 587

**Część III. Autoryzacja ... 589**

**10. Autoryzacja w systemie Windows Server 2003 ... 591**

10.1. Podstawy autoryzacji ... 591
10.2. Model autoryzacji Windows ... 592

10.3. Pośrednicy autoryzacji ... 598
10.3.1. Grupy ... 599
10.3.2. Prawa użytkowników ... 630
10.4. Zmiany w autoryzacji w systemie Windows 2000 ... 632
10.4.1. Nowy edytor ACL ... 634
10.4.2. Szczegółowa kontrola dziedziczenia ... 635
10.4.3. Wpisy ACE dla typów obiektów ... 643
10.4.4. Proces przetwarzania list ACL ... 659
10.4.5. Historia identyfikatorów SID ... 664
10.5. Zmiany w autoryzacji w systemie Windows Server 2003 ... 667
10.5.1. Bardziej restrykcyjne ustawienia autoryzacji ... 667
10.5.2. Uprawnienia czynne ... 669
10.5.3. Zmiany domyślnego deskryptora zabezpieczeń AD ... 669
10.5.4. Replikacja wartości połączonych AD i aktualizacja przynależności do grup ... 672
10.5.5. Kwoty dla obiektów AD ... 673
10.5.6. Bit poufności dla atrybutów AD ... 675
10.5.7. Ukrywanie danych w systemie plików i udziałach ... 680
10.5.8. Menedżer autoryzacji ... 687
10.6. Narzędzia ... 697

**11. Delegacja Active Directory ... 699**

11.1. Wprowadzenie ... 699
11.1.1. Uwagi na temat poziomu uprzywilejowania ... 700
11.1.2. Uwagi na temat środowisk wielodomenowych ... 704
11.1.3. Jednostki organizacyjne ... 707
11.2. Ogólne wskazówki na temat delegacji Active Directory ... 711
11.2.1. Honorowanie zasady minimalnych przywilejów w zarządzaniu AD ... 712
11.2.2. Kontrolowanie zarządzania hasłami ... 713
11.2.3. Projektowanie ról dla delegacji AD ... 716
11.3. Konfiguracja delegacji administracyjnej ... 725
11.3.1. Kreator delegacji AD ... 726
11.3.2. Przykłady delegacji administracyjnej ... 730
11.4. Ukrywanie obiektów w Active Directory ... 739
11.4.1. Trudności z ukrywaniem danych w Active Directory ... 739
11.4.2. Ukrywanie danych za pomocą „normalnych" uprawnień obiektów i atrybutów AD ... 745
11.4.3. Włączanie trybu wyświetlania obiektów w lesie ... 751
11.4.4. Dostosowywanie domyślnych zabezpieczeń obiektów w AD ... 761
11.4.5. Dostosowywanie wbudowanego zbioru właściwości ... 766
11.4.6. Używanie bitu poufności ... 774
11.5. Narzędzia od innych producentów ... 778

**Skorowidz ... 781**