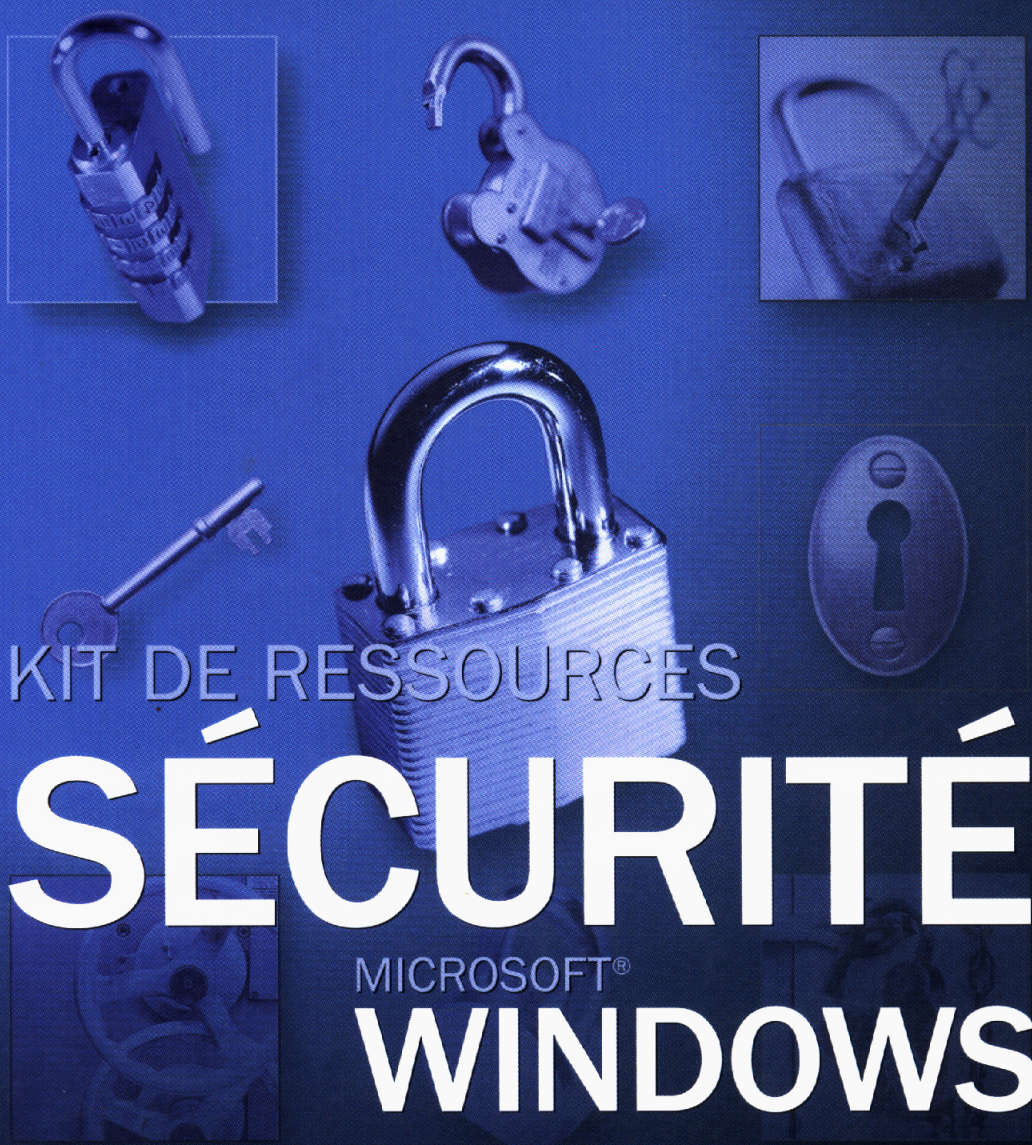
Microsoft®

Kit de Ressources



KIT DE RESSOURCES SÉCURITÉ MICROSOFT® WINDOWS

- Bénéficiez de l'expertise conceptuelle et méthodologique des ingénieurs Microsoft
- Implémentez une sécurité fiable, robuste et évolutive
- Accédez à des outils de sécurité spécifiques

B. Smith, B. Komar et l'équipe Sécurité de Microsoft

Microsoft®

KIT DE RESSOURCES SÉCURITÉ MICROSOFT® WINDOWS

Ben Smith
Brian Komar

Adapté de l'anglais par :
Xavier Guesnu

Titre U.S. : MICROSOFT WINDOWS SECURITY RESOURCE KIT
ISBN U.S. : 0-7356-1868-2

Édition et diffusion : Dunod
Distribution : Vivendi Universal Publishing Services
Couverture : Agence SAMOA
Traduction : Xavier Guesnu
Mise en page : IID
ISBN : 2 10 007249 8

Sommaire

Introduction

À propos du Kit de ressources i
À propos du site de téléchargement ii
Stratégie de support du Kit de ressources iii
Configuration requise iii
À propos de la couverture iii

Partie I Application des principes clés de la sécurité

1 Principes clés de la sécurité 3

Présentation de la gestion des risques 3
Apprendre à gérer les risques 4
Stratégies de gestion des risques 6
Comprendre la sécurité 7
Attribution du privilège minimal requis 8
Défense de chaque couche du réseau 8
Réduction de la surface d'attaque 8
Protection, détection et réponse 8
Conception, sécurité par défaut et déploiement 9
Les 10 commandements de la sécurité 9
Les 10 commandements de l'administration de la sécurité 11

2 Évaluer les forces en présence 13

Connaître ses propres forces 13
Évaluer avec rigueur ses propres compétences 14
Posséder une documentation détaillée du réseau 14
Maîtriser le niveau de prise en charge organisationnelle 15
Identifier l'agresseur 15
Agresseurs externes 16
Agresseurs internes 18
Motivations des agresseurs 19
Difficultés liées à la défense des réseaux 19
Ressources illimitées pour les agresseurs 20
Nécessité pour les agresseurs de maîtriser une seule attaque 20
Nécessité pour les défenseurs de réaliser leurs objectifs professionnels 20
Les défenseurs sont condamnés à gagner 21

Partie II Sécuriser Active Directory

3 Sécuriser les comptes d'utilisateurs et les mots de passe 25

Sécurisation des comptes 25
Identificateurs de sécurité 26
Présentation des jetons d'accès 28
Configurer les options de sécurité des comptes 30
Sécuriser les comptes administratifs 33
Implémenter la sécurité par mot de passe 36
Attribution de droits et d'autorisations à l'aide de groupes 43
Droits et autorisations utilisateur 43
Types de groupes et portée 49
Implémentation de la sécurité à base de rôles dans Windows 2000 59
Sécuriser les mots de passe 62
Présentation de l'authentification 62
Stocker des secrets dans Windows 73
Méthodes conseillées 77
Informations complémentaires 78

4 Sécuriser les objets et les attributs Active Directory 81

Schéma Active Directory 81
Attributs 82
Classes 82
Configurer les DACL pour sécuriser les objets Active Directory 84
Présentation des DACL 85
Fonctionnement des DACL 88
Sécuriser les objets et les attributs Active Directory 89
Configurer les DACL par défaut des objets et des attributs 90
Sécuriser les objets après leur création 91
Configurer les listes DACL à partir de la ligne de commande 93
Méthodes conseillées 94
Informations complémentaires 95

5 Implémenter la stratégie de groupe 97

Présentation de la stratégie de groupe 97
Stratégies de groupe ordinateur 99
Stratégies de groupe utilisateur 101
Utilisation des conteneurs de stratégie de groupe 103
Traitement des objets stratégie de groupe 105
Application initiale de la stratégie de groupe 105

Actualisation de la stratégie de groupe 106
Traitement à la demande 107
Modification de l'application de stratégie de groupe 107
Bloquer l'héritage 107
Aucun remplacement 108
Filtrage des objets de stratégie de groupe 108
Traitement en mode boucle de rappel 109
Gestion de la stratégie de groupe 110
Autorisations par défaut de la stratégie de groupe 111
Délégation de la gestion de la stratégie de groupe 111
Méthodes conseillées 112
Informations complémentaires 113

6 Définir la sécurité pour les forêts et domaines Active Directory 115

Autonomie et isolation dans Active Directory 115
Définition des forêts pour la sécurité Active Directory 117
Limites de l'administration d'entreprise et isolation d'autorité 117
Contrôle par défaut du schéma et des autorisations 118
Frontières du catalogue global 118
Exigences liées à l'approbation des domaines 119
Isolation du contrôleur de domaine 119
Protection du domaine racine de la forêt 120
Conception de domaines pour la sécurité Active Directory 122
Définition d'un DNS pour la sécurité d'Active Directory 124
Espace de noms unique 125
Espace de noms délégué 126
Espace de noms interne 126
Espace de noms segmenté 126
Concevoir la délégation d'autorité 128
Méthodes conseillées 130
Informations complémentaires 132

Partie III Sécuriser le système d'exploitation

7 Sécuriser les autorisations 137

Sécuriser les autorisations des fichiers et des dossiers 137
Fonctionnement des listes DACL 143
Assignation des listes DACL à la création 144
Gestion des listes DACL lors d'une copie ou d'un déplacement de fichiers et de dossiers 145

Outils de ligne de commande 146
Autorisations de fichier et de dossier par défaut 151
Sécuriser l'accès aux fichiers et dossiers en partageant les autorisations 159
Utilisation d'EFS (Encrypting File System) 160
Fonctionnement d'EFS 161
Outils de ligne de commande EFS 163
Fonctionnalités EFS supplémentaires dans Windows XP 166
Introduction à la conception d'une stratégie agent de récupération de données 169
Sécuriser les autorisations de Registre 171
Configurer les autorisations de Registre 173
Méthodes conseillées 174
Informations complémentaires 175

8 Sécuriser les services 179

Gestion des autorisations de service 179
Configuration de la valeur de démarrage d'un Service 181
Arrêter, démarrer, suspendre et reprendre des services 182
Configurer le contexte de sécurité des services 183
Configuration de la liste DACL du service 184
Services par défaut dans Windows 2000 et Windows XP 186
Méthodes conseillées 210
Informations complémentaires 212

9 Implémenter la sécurité TCP/IP 213

Sécuriser TCP/IP 213
Présentation des protocoles de la couche Internet 214
Présentation des protocoles de couche de transport 217
Menaces courantes contre le protocole TCP/IP 220
Configurer la sécurité TCP/IP dans Windows 2000 et Windows XP 224
Utilisation de la sécurité IP (IPSec) 234
Sécuriser la transmission des données avec les protocoles IPSec 235
Sélection du mode IPSec 238
Sélectionner une méthode d'authentification IPSec 238
Créer des stratégies IPSec 240
Fonctionnement d'IPSec 244
Surveillance d'IPSec 247
Méthodes conseillées 249
Informations complémentaires 250

10 Sécuriser Microsoft Internet Explorer 6 et Microsoft Office XP 253

Paramètres de sécurité dans Internet Explorer 6 253
Paramètres de confidentialité 254
Zones de sécurité 258
Configurer les paramètres de confidentialité et de sécurité dans Internet Explorer 6 273
Paramètres de sécurité dans Office XP 275
Configurer la sécurité ActiveX et la sécurité des macros 275
Configurer la sécurité pour Outlook 2002 277
Méthodes conseillées 278
Informations complémentaires 279

11 Configurer les modèles de sécurité 281

Utilisation des paramètres des modèles de sécurité 281
Stratégies de comptes 282
Stratégies locales 285
Journal des événements 301
Groupes restreints 302
Services système 302
Registre 302
Système de fichiers 303
Stratégies de clé publique 303
Stratégies de sécurité IP 304
Fonctionnement des modèles de sécurité 304
Application des modèles de sécurité à un ordinateur local 304
Application des modèles de sécurité à l'aide de la Stratégie de groupe 309
Modèles de sécurité par défaut 310
Création de modèles de sécurité personnalisés 312
Ajout d'entrées du Registre aux Options de sécurité 312
Ajout de services, de valeurs de Registre et de fichiers aux modèles de sécurité 315
Méthodes conseillées 315
Informations complémentaires 316

12 Auditer les événements de sécurité Microsoft Windows 317

Détermination des événements à auditer 318
Gestion de l'Observateur d'événements 319
Déterminer l'emplacement de stockage 320
Déterminer la taille maximale du fichier journal 320

Configurer le comportement de remplacement 320
Configurer les stratégies d'audit 322
Auditer les événements de connexion aux comptes 323
Auditer la gestion des comptes 327
Auditer l'accès au service d'annuaire 330
Auditer les événements de connexion 331
Auditer l'accès aux objets 334
Auditer les modifications de stratégie 336
Auditer l'utilisation des privilèges 337
Auditer le suivi des processus 338
Auditer les événements système 339
Activation des stratégies d'audit 340
Surveillance des événements audités 341
Utilisation de l'Observateur d'événements 342
Utilisation de scripts personnalisés 342
Utilisation d'Event Comb 343
Méthodes conseillées 347
Informations complémentaires 348

13 Sécuriser les ordinateurs mobiles 349

À propos des ordinateurs portables 349
Risque accru de vol ou de perte 349
Difficulté d'application des mises à jour de sécurité 351
Exposition aux réseaux non approuvés 351
Indiscrétion sur les connectivités sans fil 352
Implémenter une sécurité supplémentaire pour les ordinateurs portables 352
Protection matérielle 353
Protection de l'amorçage 354
Protection des données 355
Formation des utilisateurs 358
Sécuriser la gestion de réseau sans fil dans Windows XP 358
Utilisation de la configuration automatique sans fil dans Windows XP 358
Configurer la sécurité de la connectivité réseau sans fil 802.11 360
Configurer la sécurité 802.11 avec 802.1x 362
Méthodes conseillées 364
Informations complémentaires 365

Partie IV Sécuriser les services

14 Implémenter la sécurité pour les contrôleurs de domaine 369

Menaces contre les contrôleurs de domaine 369
Modification des objets Active Directory 370
Attaques contre les mots de passe 370
Attaques de refus de service 370
Attaques d'empêchement de réplication 370
Exploitation des vulnérabilités identifiées 371
Implémenter la sécurité sur les contrôleurs de domaine 371
Assurer la sécurité physique 371
Augmenter la sécurité des mots de passe stockés 372
Supprimer les services superflus 373
Appliquer les paramètres de sécurité à l'aide de la Stratégie de groupe 375
Protection contre l'échec d'un contrôleur de domaine 375
Implémenter Syskey 376
Sécuriser les groupes et les comptes intégrés 377
Activation de l'audit 378
Sécuriser les communications Active Directory 379
Méthodes conseillées 382
Informations complémentaires 384

15 Implémenter la sécurité des serveurs DNS 385

Menaces sur les serveurs DNS 386
Modification d'enregistrements DNS 387
Transfert de zone de données DNS par un serveur non autorisé 387
Exposition des schémas internes d'adresses IP 387
Attaques de refus de service contre les services DNS 388
Sécuriser les serveurs DNS 388
Implémenter les zones intégrées Active Directory 389
Implémenter des serveurs de noms DNS internes et externes distincts 389
Restreindre les transferts de zones 391
Implémenter IPSec entre clients DNS et serveurs DNS 392
Restreindre le trafic DNS sur le pare-feu 393
Limiter la gestion de DNS 394
Protéger le cache DNS 394
Méthodes conseillées 394
Informations complémentaires 395

16 Implémenter la sécurité pour les services Terminal Server 397

Menaces contre les services Terminal Server 398
Attribution d'autorisations excessives aux utilisateurs 398
Sécurité du pare-feu ignorée 399
Utilisation d'un port connu 399
Nécessité du droit utilisateur Ouvrir une session localement 399
Bureau Windows complet à la disposition de l'assaillant 399
Sécuriser les services Terminal Server 400
Choix du mode approprié de services Terminal Server 400
Restriction des utilisateurs et des groupes ayant le droit Ouvrir une session localement 401
Interdiction du contrôle distant sur les serveurs Terminal Server 402
Restriction sur les applications pouvant être exécutées 403
Implémentation de la forme de cryptage la plus robuste 404
Renforcement de la configuration de sécurité de Terminal Server 405
Méthodes conseillées 406
Informations complémentaires 407

17 Implémenter la sécurité pour les serveurs DHCP 409

Menaces contre les serveurs DHCP 410
Serveurs DHCP non autorisés 410
Remplacement par les serveurs DHCP des enregistrements de ressources DNS valides 411
Non appropriation par DHCP des enregistrements de ressources DNS 412
Clients DHCP non autorisés 412
Sécuriser les serveurs DHCP 412
Conservation du comportement par défaut d'inscription des noms 413
Déterminer si le groupe DNSUpdateProxy doit être utilisé 413
Éviter l'installation de DHCP sur les contrôleurs de domaines 414
Rechercher les entrées BAD_ADDRESS dans la base de données DHCP 415
Surveiller l'appartenance du groupe Administrateurs DHCP 416
Activation de l'audit DHCP 416
Méthodes conseillées 416
Informations complémentaires 417

18 Implémenter la sécurité pour les serveurs WINS 419

Menaces contre les serveurs WINS 421
Empêcher la réplication entre serveurs WINS 421
Inscription d'enregistrements NetBIOS erronés 421

Inscription incorrecte d'enregistrements WINS 422
Modification de la configuration WINS 422
Sécuriser les serveurs WINS 422
Surveiller l'appartenance du groupe WINS 422
Valider la configuration de la réplication WINS 422
Supprimer les applications NetBIOS 423
Méthodes conseillées 423
Informations complémentaires 424

19 Implémenter la sécurité pour le routage et l'accès distant 425

Composants d'une solution d'accès distant 425
Protocoles d'authentification 426
Protocoles VPN 427
Logiciels clients 428
Logiciels et services serveur 429
Menaces contre les solutions d'accès distant 430
Interception de l'authentification 430
Interception des données 431
Franchissement du pare-feu du réseau privé 431
Application de stratégies non normalisée 431
Extension du périmètre réseau à l'emplacement de l'utilisateur de la connexion distante 432
Refus de service consécutif à des attaques contre les mots de passe 432
Vol d'ordinateurs portables sur lesquels sont enregistrées les informations d'identification 433
Sécuriser les serveurs d'accès distant 433
Implémenter l'authentification RADIUS et la gestion de comptes 433
Sécuriser le trafic d'authentification RADIUS entre le serveur d'accès distant et le serveur RADIUS 434
Configurer une stratégie d'accès distant 434
Déployer les certificats requis pour L2TP/IPSec 437
Restriction des serveurs autorisés à exécuter le service RRAS 439
Implémenter le verrouillage de compte d'accès distant 440
Sécuriser les clients d'accès distant 441
Configurer les packages CMAK 441
Implémenter une authentification forte 441
Déployer les certificats requis 442
Méthodes conseillées 442
Informations complémentaires 443

20 Implémenter la sécurité pour les services de certificats 445

Menaces sur les Services de certificats 445
Mise en péril de la paire de clés de l'autorité de certification 446
Attaques contre les serveurs hébergeant des listes de révocation de certificats et des certificats d'autorités de certification 446
Tentatives de modification de la configuration des autorités de certification 447
Tentatives de modification des autorisations de modèles de certificats 447
Attaques désactivant le contrôle des listes de révocation de certificats 447
Ajout d'autorités de certification non approuvées au magasin des autorités de certification racines approuvées 447
Émission de certificats illicites 448
Publication de certificats erronés sur le service d'annuaire Active Directory 448
Sécuriser les Services de certificats 448
Implémenter des mesures de sécurité logiques 449
Modifier les listes de révocation de certificats et les points de publication des certificats d'autorités de certification 450
Activer le contrôle des listes de révocation dans toutes les applications 450
Gérer les autorisations de modèles de certificats 451
Méthodes conseillées 451
Informations complémentaires 451

21 Implémenter la sécurité pour Microsoft IIS 5.0 453

Implémenter la sécurité Windows 2000 454
Réduire les services 454
Définir les comptes d'utilisateurs 455
Sécuriser le système de fichiers 456
Appliquer des paramètres de Registre spécifiques 458
Configurer la sécurité d'IIS 459
Authentification 459
Autorisations de sites Web 463
Canaux de communication 464
Sécuriser IIS à l'aide d'outils 468
Outil IIS Lockdown 468
Filtre URLScan 474
Configurer le service FTP 480
Méthodes conseillées 482
Informations complémentaires 482

Partie V Gérer les mises à jour de la sécurité

22 Gestion des correctifs 487

Types de correctifs 488
Développement d'un correctif 490
Gestion des correctifs en six étapes 491
Étape 1. Notification 491
Étape 2. Évaluation 492
Étape 3. Acquisition 493
Étape 4. Tests 497
Étape 5. Déploiement 498
Étape 6. Validation 502
Méthodes conseillées 503
Informations complémentaires 504

23 Utiliser les outils de gestion des correctifs 505

Catalogue des bulletins de correctifs de sécurité 506
Windows Update 509
Mises à jour automatiques 512
Services Microsoft SUS (Software Update Services) 514
Fonctionnement des services SUS 514
Configurer le serveur SUS 515
Configurer les clients SUS 518
Microsoft Baseline Security Analyzer 520
Explorer les mises à jour en mode GUI 522
Explorer les mises à jour avec la version ligne de commande de MBSA 523
Pack de fonctionnalités des services SUS SMS 525
Méthodes conseillées 528
Informations complémentaires 529

24 Utiliser les outils d'évaluation de la sécurité 531

Évaluer la configuration de la sécurité 531
Console Configuration et analyse de la sécurité 533
Utilitaire Secedit.exe 535
Évaluations de sécurité 535
Microsoft Baseline Security Analyzer 536
Outils tiers 547
Analyse des ports 548
Méthodes conseillées 552
Informations complémentaires 553

Partie VI Planifier et exécuter les évaluations de sécurité et les réponses aux incidents

25 Évaluer la sécurité d'un réseau **557**

Types d'évaluations de sécurité 558
Analyse des vulnérabilités 558
Tests de pénétration 560
Audit de la sécurité informatique 561
Conduite des évaluations de sécurité 561
Planification de l'évaluation 562
Conduite de l'évaluation 562
Résolution des problèmes détectés pendant l'évaluation de la sécurité 563
Conduite de tests de pénétration 565
Étape 1. Recueillir les informations 565
Étape 2. Recherche des vulnérabilités 567
Étape 3. Mise en péril du réseau ou de l'application cible 569
Méthodes conseillées 570
Informations complémentaires 571

26 Planifier la réponse aux incidents **573**

Créer une équipe de réponse aux incidents 573
Obtenir l'approbation de la direction 574
Identifier les enjeux 574
Choisir un chef d'équipe 575
Définir une stratégie de réponse aux incidents 576
Catégoriser les types d'incidents 576
Réponses proactives et réactives 577
Stratégie d'utilisation acceptable 579
Créer un plan de communications 582
Communications internes avant incident 582
Communications pendant un incident 583
Communication avec la presse 585
Méthodes conseillées 586
Informations complémentaires 587

27 Répondre aux incidents de sécurité **589**

Indicateurs courants d'incidents de sécurité 590
Analyse des ports Internet 590
Impossibilité d'accéder aux ressources réseau 593

Utilisation excessive de l'unité centrale 593
Opérations irrégulières 594
Activité irrégulière du système de fichiers 594
Modifications des autorisations 595
Analyser un incident de sécurité 595
Déterminer la cause 596
Empêcher une exploitation future 596
Empêcher des incidents ultérieurs 596
Restaurer le service 597
Intégration des enseignements acquis à la stratégie 598
Suivre l'assaillant 598
Conduire les investigations sur la sécurité 598
Application de la loi 599
Recueillir les preuves 601
Surveiller le réseau 606
Implémenter des contre-mesures pour un incident de sécurité 607
Évaluer la portée d'une attaque 607
Recherche d'un compromis 608
Récupérer les services après un incident de sécurité 609
Conduire un incident de sécurité à titre rétrospectif 609
Méthodes conseillées 610
Informations complémentaires 611

Partie VI Appliquer les principes clés de la confidentialité

28 Comprendre l'importance de la confidentialité 615

Définir la confidentialité 616
Différences entre la confidentialité et la sécurité 617
Protéger les consommateurs contre les suivis et les contacts inappropriés 618
Origine de la législation sur la confidentialité 619
Organisation de développement et de coopération économique (ODCE) 619
Législation européenne sur la confidentialité 620
Formuler une stratégie de confidentialité d'entreprise 621
Créer un groupe responsable de la confidentialité 621
Répondre aux problèmes de confidentialité 621
Méthodes conseillées 623
Informations complémentaires 624

29 Définir la confidentialité pour un site Web d'entreprise 625

Définir une déclaration de confidentialité 626
Anatomie d'une déclaration de confidentialité 626
Remarques sur la déclaration de confidentialité 630
Autres règles de création et de publication d'une déclaration de confidentialité 632
Projet P3P 633
Intégration P3P pour Internet Explorer 6 634
Implémenter P3P pour un site Web 637
Méthodes conseillées 638
Informations complémentaires 639

30 Déployer la confidentialité en entreprise 641

Sélection des applications en fonction de leur degré de confidentialité 641
Protection de la confidentialité de vos employés 642
Protection de la confidentialité de vos clients et de vos partenaires commerciaux 642
Stockage sécurisé des données sur les clients 643
Collecte des données des clients et des préférences en matière de confidentialité 643
Contrôler la gestion des données client 643
Créer un système de contacts personnalisé 644
Créer un système de contacts avec Active Directory 644
Utiliser une base de données pour créer un système de contacts 646
Méthodes conseillées 647
Informations complémentaires 647

Index 649