

Inhaltsverzeichnis

Über dieses Buch	xxiii
Zielgruppe	xxiii
Voraussetzungen	xxiii
Referenzmaterial	xxiv
Die Begleit-CD-ROM	xxiv
Features dieses Buches	xxiv
Anmerkungen	xxiv
Konventionen	xxv
Typografische Konventionen	xxv
Tastaturkonventionen	xxv
Übersicht über die Kapitel und den Anhang	xxvi
Auffinden spezifischer Informationen zu den geprüften Kenntnissen	xxvii
Implementierung, Verwaltung und Fehlerbehebung grundlegender Sicherheitsmaßnahmen	xxviii
Implementierung, Verwaltung und Fehlerbehebung von Service Packs und Sicherheitsaktualisierungen	xxviii
Implementierung, Verwaltung und Fehlerbehebung von sicheren Kommunikationskanälen	xxix
Implementierung, Verwaltung und Fehlerbehebung der Authentifizierung und des sicheren Remotezugriffs	xxix
Implementierung und Verwaltung einer Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure, PKI) und des verschlüsselnden Dateisystems (Encrypting File System, EFS)	xxx
Überwachung und Reaktion auf sicherheitsrelevante Zwischenfälle	xxxi
Erste Schritte	xxxi
Hardwarevoraussetzungen	xxxii
Softwarevoraussetzungen	xxxii
Installationsanweisungen	xxxii
Über die Onlineversion des Buches	xxxiii
Der Onlinetest	xxxiii
Das Microsoft Certified Professional-Programm	xxxiv
Vorteile des Microsoft Certified Professional-Programms	xxxiv
Vorteile für den Einzelnen	xxxv
Vorteile für Arbeitgeber und Unternehmen	xxxvi

Voraussetzungen für den Erhalt eines MCP-Zertifikats	xxxvi
Technische Schulung für Computerspezialisten	xxxvii
Selbststudium	xxxvii
Microsoft Certified Technical Education Centers (CTECs)	xxxvii
Technischer Support	xxxvii
E-Mail	xxxvii
Per Post	xxxvii
 Kapitel 1 Gruppenrichtlinien	 1
Über dieses Kapitel	1
Bevor Sie beginnen	2
Lektion 1: Active Directory und Gruppenrichtlinien	3
Die Struktur von Active Directory	3
Praktische Übung: Entwerfen einer Hierarchie für Active Directory	5
Lernzielkontrolle	7
Zusammenfassung der Lektion	8
Lektion 2: Konfigurieren von Gruppenrichtlinien	9
Grundlagen von Gruppenrichtlinien	9
Verknüpfen von Gruppenrichtlinien mit Active Directory-Containern	10
Lokale Gruppenrichtlinien	10
Gruppenrichtlinien in Active Directory	10
Die Anwendungsreihenfolge von Gruppenrichtlinien	11
Die physische Struktur von Gruppenrichtlinienobjekten	12
Die logische Struktur von Gruppenrichtlinienobjekten	13
Verwalten von Gruppenrichtlinien	14
Erstellen von Gruppenrichtlinienobjekten	14
Verknüpfen von Gruppenrichtlinien- mit Active Directory-Objekten	14
Einstellungen für Gruppenrichtlinienobjekte	15
Delegieren der Verwaltung	15
Filtern von Gruppenrichtlinien	16
Praktische Übungen: Verwalten von Gruppenrichtlinien	16
Übung 1: Erstellen von Gruppenrichtlinienobjekten	17
Übung 2: Einstellungen für Gruppenrichtlinienobjekte	18
Übung 3: Steuern des administrativen Zugriffs auf Gruppenrichtlinienobjekte	19
Übung 4: Filtern der Anwendung von Gruppenrichtlinienobjekten	20
Übung 5: Verknüpfen eines Active Directory- mit einem Gruppenrichtlinienobjekt	21
Übung 6: Entfernen einer Verknüpfung	22
Übung 7: Löschen eines Gruppenrichtlinienobjekts	23
Übung 8: Erstellen einer Verwaltungskonsole für Gruppenrichtlinien	23
Lernzielkontrolle	26
Zusammenfassung der Lektion	27
Lektion 3: Konfigurieren der Sicherheitsrichtlinien für Clientcomputer	28
Clientseitige Konfiguration von Gruppenrichtlinien	28

Konfigurieren von Gruppenrichtlinien nach dem Benutzertyp	29
Konfigurieren von Internet Explorer über Gruppenrichtlinien	30
Steuern der Einstellungen für Internet Explorer	30
Grenzen der Gruppenrichtlinien	30
Praktische Übungen: Einrichten der Gruppenrichtlinien für Clients	32
Übung 1: Konfigurieren eines Computers für Knowledge Worker	32
Übung 2: Verwenden von Skripts zum Aufbau einer einheitlichen Umgebung	34
Übung 3: Konfigurieren eines Computers für Task Worker	37
Übung 4: Einrichten der Sicherheit für MMC-Clients	39
Übung 5: Einrichten der Sicherheit für Internet Explorer	40
Lernzielkontrolle	43
Zusammenfassung der Lektion	44
Lektion 4: Beheben von Fehlern bei der Anwendung von Gruppenrichtlinien	45
Typische Probleme bei der Anwendung von Gruppenrichtlinien	45
Die Auswirkung der DNS-Auflösung auf Gruppenrichtlinien	46
Sonderfälle	46
Probleme bei der Migration von Windows NT 4.0-Domänen	47
Probleme aufgrund von Windows NT 4.0-Vertrauensstellungen	48
Praktische Übungen: Beheben von Fehlern bei der Anwendung von Gruppenrichtlinien	48
Übung 1: Aktivieren der Protokollierung in Windows 2000	48
Übung 2: Verifizieren der Konfiguration eines Domänencontrollers	49
Übung 3: Überprüfen der Clientverbindung	49
Lernzielkontrolle	51
Zusammenfassung der Lektion	52
Lektion 5: Grenzen von Sicherheitseinstellungen	53
Die Rolle der Gruppenrichtlinien für die Netzwerksicherheit	53
Praktische Übung: Umgehen der Sicherheitseinstellungen von Gruppenrichtlinien	54
Lernzielkontrolle	56
Zusammenfassung der Lektion	57
Kapitel 2 Benutzerkonten und Sicherheitsgruppen	59
Über dieses Kapitel	59
Bevor Sie beginnen	59
Lektion 1: Anlegen von lokalen Benutzerkonten und Sicherheitsgruppen	60
Verwalten von Benutzerkonten	60
Verwalten von Sicherheitsgruppen	62
Optimieren der Sicherheitsprüfung	63
Verwalten der Gruppen	63
Authentifizieren eines Benutzers auf einem lokalen Computer	64
Der lokale Anmeldevorgang	64
Zugriff auf lokale Ressourcen	65
Integrierte lokale Gruppen	66
Systemgruppen	66

Arbeitsgruppenauthentifizierung im Hintergrund	67
Praktische Übungen: Anlegen von Benutzerkonten und Sicherheitsgruppen	68
Übung 1: Verwalten von Benutzerkonten auf einem lokalen Computer	68
Übung 2: Verwalten von Sicherheitsgruppen auf einem lokalen Computer	71
Lernzielkontrolle	72
Zusammenfassung der Lektion	73
Lektion 2: Active Directory-Domänenkonten und Sicherheitsgruppen	74
Domänen	74
Authentifizieren von Domänenbenutzerkonten	74
Kerberos	75
Domänenübergreifende Vertrauensstellung	78
Anmeldung an einer Domäne	78
Zugriff auf Ressourcen einer Domäne	79
Effizienter Einsatz von Domänensicherheitsgruppen	80
Verwenden von Sicherheitsgruppen zum Festlegen von Berechtigungen	80
Erstellen von wirksamen Domänensicherheitsgruppen	81
Optimieren von Gruppen in großen Organisationen	82
Praktische Übungen: Anlegen von Benutzerkonten und Sicherheitsgruppen	83
Übung 1: Verwalten von Domänenbenutzerkonten in Active Directory	83
Übung 2: Verwalten von Domänensicherheitsgruppen	86
Lernzielkontrolle	88
Zusammenfassung der Lektion	89
 Kapitel 3 Einschränkungen für Konten, Benutzer und Gruppen	 91
Über dieses Kapitel	91
Bevor Sie beginnen	92
Lektion 1: Kontorichtlinien	93
Anwenden von Kontorichtlinien	93
Welche Kontorichtlinieneinstellungen sind möglich?	93
Kennwortchronik erzwingen	93
Maximales Kennwortalter	94
Minimales Kennwortalter	94
Minimale Kennwortlänge	94
Kennwörter müssen den Komplexitätsanforderungen entsprechen	95
Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	96
Kontosperrungsdauer	96
Kontosperrungsschwelle	97
Kontosperrungszähler zurücksetzen nach	97
Benutzeranmeldeeinschränkungen erzwingen	97
Maximale Gültigkeitsdauer des Diensttickets	97
Maximale Gültigkeitsdauer des Benutzertickets	98
Maximaler Zeitraum für die Erneuerung von Benutzertickets	98
Maximale Toleranz für die Synchronisation des Computertakts	98

Praktische Übung: Einrichten von Kontorichtlinien	99
Lernzielkontrolle	103
Zusammenfassung der Lektion	104
Lektion 2: Verwalten von Benutzerrechten	105
Zuweisen von Benutzerrechten	105
Praktische Übung: Ändern von Benutzerrechten	106
Lernzielkontrolle	109
Zusammenfassung der Lektion	110
Lektion 3: Zugriffssteuerung durch eingeschränkte Gruppen	111
Einstellungen für eingeschränkte Gruppen	111
Praktische Übung: Erstellen einer eingeschränkten Gruppe	111
Lernzielkontrolle	114
Zusammenfassung der Lektion	115
Lektion 4: Verwalten von Sicherheitsvorlagen	116
Der Zweck von Sicherheitsvorlagen	116
Vorteile vordefinierter Sicherheitsvorlagen	117
Verwalten von Sicherheitsvorlagen	119
Empfohlene Vorgehensweisen	119
Bereitstellen von Sicherheitsvorlagen	119
Praktische Übungen: Verwalten von Sicherheitsvorlagen	120
Übung 1: Erstellen einer Verwaltungskonsole für Sicherheitsvorlagen	120
Übung 2: Erstellen einer Sicherheitsvorlage	122
Übung 4: Ändern einer vordefinierten Sicherheitsvorlage	125
Übung 5: Die Verwaltungskonsole Lokale Sicherheitseinstellungen	126
Übung 6: Die Verwaltungskonsole Sicherheitskonfiguration und -analyse	127
Übung 7: Bereitstellen einer Sicherheitsvorlage über Gruppenrichtlinienobjekte	127
Übung 8: SecEdit.exe	128
Lernzielkontrolle	131
Zusammenfassung der Lektion	132
Kapitel 4 Sicherheit auf der Grundlage von Konten	133
Über dieses Kapitel	133
Bevor Sie beginnen	133
Lektion 1: Verwalten von Dateisystemberechtigungen	134
Verwalten von Berechtigungen	134
Die Wichtigkeit der Zugriffssteuerung	134
Wie funktionieren Berechtigungen?	135
Bestimmen der Sicherheitsanforderungen	136
Verwenden der standardmäßigen Berechtigungen des Dateisystems	136
Empfohlene Vorgehensweisen	140
Vergeben von grundlegenden Berechtigungen	140
Verwalten von Berechtigungsänderungen in einem einzigen Ordner	140

Wiedergeben des Organisationsaufbaus in der Struktur der Ordner und Sicherheitsgruppen	141
Bearbeiten vorhandener Berechtigungen	141
Erstellen einer Sicherheitsgruppe mit Vollzugriff auf alle Ressourcen	142
Beheben von Problemen aufgrund von Berechtigungen	142
Liegt ein durch Berechtigungen verursachtes Problem vor?	142
Auffinden der problembehafteten Ressource	142
Bestimmen des Problems	143
Praktische Übungen: Schützen von Dateien und Ordnern	143
Übung 1: Festlegen von Berechtigungen für Dateien und Ordner	144
Übung 2: Beheben von Problemen aufgrund von Berechtigungen	147
Lernzielkontrolle	150
Zusammenfassung der Lektion	151
Lektion 2: Freigabesicherheit	152
Was bedeutet Freigabesicherheit?	152
Verwalten von Freigaben unter Sicherheitsaspekten	153
Bewährte Verfahren	154
Praktische Übungen: Freigaben und Freigabeberechtigungen	155
Übung 1: Anlegen von Freigaben	155
Übung 2: Verwalten der Sicherheit von Freigaben	157
Lernzielkontrolle	159
Zusammenfassung der Lektion	160
Lektion 3: Überwachungsrichtlinien	161
Sicherheitsmechanismen für die Überwachung	161
Wie funktioniert die Überwachung?	161
Überwachungskategorien	162
Verwalten der Überwachung	163
Vermeiden von Problemen	164
Verwalten der Überwachungstätigkeiten	164
Praktische Übungen: Durchführen der Überwachung	164
Übung 1: Überwachen von An- und Abmeldeversuchen	164
Übung 2: Überwachung von Datei- und Ordnerberechtigungen	166
Übung 3: Einsehen des Überwachungsprotokolls	168
Lernzielkontrolle	170
Zusammenfassung der Lektion	171
Lektion 4: Einbeziehen der Registrierung	172
Warum ist die Sicherheit der Registrierung wichtig?	172
Bearbeiten der Registrierung	172
Praktische Übung: Erkunden der Registrierung	174
Lernzielkontrolle	176
Zusammenfassung der Lektion	177

Kapitel 5 Zertifizierungsstellen	179
Über dieses Kapitel	179
Bevor Sie beginnen	179
Lektion 1: Grundlagen zu Zertifikaten	180
Verschlüsselung	180
Verschlüsselung mit geheimen Schlüsseln	180
Verschlüsselung mit öffentlichen Schlüsseln	181
Überprüfen von Identitäten mit digitalen Signaturen	182
Gemeinsamer Einsatz von Verschlüsselung und Zertifikaten	182
Zertifikatshierarchien	183
Stammzertifizierungsstellen	184
Ablauf von Zertifikaten	185
Zertifikatssperreliste	186
Verwendungszwecke für Zertifikate	187
Lernzielkontrolle	189
Zusammenfassung der Lektion	190
Lektion 2: Installieren der Windows 2000-Zertifikatsdienste	191
Installieren von Zertifizierungsstellen	191
Organisationszertifizierungsstellen	191
Eigenständige Zertifizierungsstellen	192
Stamm- und untergeordnete Zertifizierungsstellen	193
Kryptografiedienstanbieter	194
Empfohlene Vorgehensweisen	195
Praktische Übungen: Aufbau einer Zertifizierungsstellenhierarchie	196
Übung 1: Installieren der Zertifikatsdienste für die Stammzertifizierungsstelle der Organisation	196
Übung 2: Installieren der Zertifikatsdienste für eine eigenständige untergeordnete Zertifizierungsstelle	199
Lernzielkontrolle	202
Zusammenfassung der Lektion	203
Lektion 3: Warten von Zertifizierungsstellen	204
Widerrufen von Zertifikaten	204
Ausstellen von Zertifikaten	205
Sichern und Wiederherstellen von Zertifizierungsstellen	205
Routinemäßige Sicherung der Zertifizierungsstellen-Datenbank	205
Sichern der Zertifikatsdatenbank mit der Verwaltungskonsole Zertifizierungsstelle	205
Praktische Übungen: Verwalten von Zertifizierungsstellen	207
Übung 1: Widerrufen eines Zertifikats	207
Übung 2: Verwalten der Zertifikatssperreliste	208
Übung 3: Sichern einer Zertifizierungsstelle	210
Übung 4: Wiederherstellen einer Zertifizierungsstelle	211
Lernzielkontrolle	212
Zusammenfassung der Lektion	213

Kapitel 6 Verwalten einer Struktur öffentlicher Schlüssel	215
Über dieses Kapitel	215
Bevor Sie beginnen.....	215
Lektion 1: Computerzertifikate	216
Der Zweck von Computerzertifikaten	216
Wie wird ein Zertifikat eingesetzt?	216
Verwenden von Zertifikatsvorlagen.....	217
Bereitstellen von Computerzertifikaten	218
Manuelle Bereitstellung.....	218
Automatisierte Bereitstellung	219
Praktische Übungen: Zwei Methoden zum Bereitstellen von Computerzertifikaten	220
Übung 1: Computerzertifikate manuell bereitstellen	220
Übung 2: Bereitstellen von Computerzertifikaten mit Hilfe von Gruppenrichtlinien	221
Lernzielkontrolle.....	225
Zusammenfassung der Lektion	226
Lektion 2: Bereitstellen von Benutzerzertifikaten.....	227
Bereitstellen von Zertifikaten für die Benutzer.....	227
Anfordern und Installieren von Zertifikaten.....	227
Automatisierte Bereitstellung von Benutzerzertifikaten	229
Manuelles Erstellen von Zertifikaten	229
Verschieben von Zertifikaten	230
Sichern und Wiederherstellen des Betriebssystems	230
Verwenden von servergespeicherten Profilen	230
Ex- und Import von Zertifikaten	230
Praktische Übungen: Bereitstellen und Verschieben von Zertifikaten	231
Übung 1: Bereitstellen von Zertifikaten über die Website der Zertifikatsdienste	232
Übung 2: Verschieben von Zertifikaten von einer Arbeitsstation zur anderen	235
Lernzielkontrolle.....	239
Zusammenfassung der Lektion	240
Lektion 3: Verwenden von Smartcard-Zertifikaten	241
Verwenden von Smartcards	241
Speicherung von öffentlichen und privaten Schlüsseln	241
Verwenden einer PIN	242
Gewährleisten der Sicherheit.....	242
Arten von Smartcard-Zertifikaten	242
Ausgeben von Smartcards	243
Entfernen von Smartcards	245
Beheben von Fehlern bei der Registrierung von Smartcards	246
Keine Initialisierung möglich	246
Fehler während der Initialisierung von Smartcards	246
Praktische Übungen: Einführen von Smartcards	247
Übung 1: Bereitstellen von Zertifikaten für Smartcards	247
Übung 2: Registrieren von Smartcards	248
Lernzielkontrolle.....	254

Zusammenfassung der Lektion	255
Lektion 4: Bereitstellen von S/MIME-Zertifikaten	256
S/MIME-Zertifikate.....	256
Beheben von Fehlern bei der S/MIME-Bereitstellung	256
Praktische Übung: Senden von digital signierten E-Mails	257
Lernzielkontrolle.....	262
Zusammenfassung der Lektion	263
Kapitel 7 Verbesserte Authentifizierung	265
Über dieses Kapitel	265
Bevor Sie beginnen.....	265
Lektion 1: Unterstützung von Clients mit älteren Windows-Versionen	266
Grundlagen der Authentifizierung	266
Authentifizierung in Windows 2000-Netzwerken	267
Authentifizierung mit LAN Manager.....	267
NTLM-Authentifizierung	268
Authentifizierung mit NTLM 2	268
Aufbau einer sicheren Umgebung.....	268
Praktische Übungen: Aufbau einer sicheren Umgebung mit verschiedenen Clients	269
Übung 1: Aufheben der Unterstützung für ältere Authentifizierungsprotokolle	269
Übung 2: Aktivieren von NTLM 2 auf älteren Windows-Clients.....	272
Lernzielkontrolle.....	274
Zusammenfassung der Lektion	275
Lektion 2: Unterstützung von Macintosh-Clients	276
Lektion 2: Sichere Unterstützung von Macintosh-Rechnern.....	276
Praktische Übungen: Gewähren des Zugriffs auf Windows 2000-Server	277
Übung 1: Vorbereiten eines Windows 2000-Servers auf die Unterstützung von Macintosh-Clients	277
Übung 2: Herstellen einer Verbindung von einem Macintosh zu einem Windows 2000-Server.....	279
Lernzielkontrolle.....	284
Zusammenfassung der Lektion	285
Lektion 3: Vertrauensstellungen.....	286
Grundlagen von Vertrauensstellungen	286
Verwalten von externen Vertrauensstellungen	287
Praktische Übung: Einrichten einer externen Vertrauensstellung	287
Herstellen einer Vertrauensstellung.....	287
Lernzielkontrolle.....	292
Zusammenfassung der Lektion	293
Kapitel 8 IPSec	295
Über dieses Kapitel	295
Bevor Sie beginnen.....	295

Lektion 1: Einrichten von IPSec in einer Domäne	297
Grundlagen von IPSec	297
ESP-Modi	298
Der Einsatz von IPSec	298
Einrichten von IPSec mit IKE	299
IPSec in Windows 2000	299
Verteilen von geheimen IKE-Schlüsseln	299
IPSec in privaten Netzwerken	300
Festlegen der IPSec-Methode nach der Serverrolle	300
Praktische Übungen: Einrichten von IPSec zwischen den Mitgliedern einer Domäne	301
Übung 1: Einrichten der IPSec-Protokollierung und -Überwachung	302
Übung 2: Aktivieren von IPSec auf Servern	303
Übung 3: Aktivieren von IPSec auf Clients	305
Übung 4: Aktivieren von IPSec auf Domänencontrollern	307
Lernzielkontrolle	310
Zusammenfassung der Lektion	311
Lektion 2: Einrichten von IPSec zwischen Netzwerken ohne Vertrauensstellung	312
Bereitstellen eines geheimen Schlüssels	312
Festlegen einer IPSec-Richtlinie in Windows 2000	313
Erstellen von IPSec-Filtern	313
IPSec-Ausnahmen	313
Praktische Übungen: Aufbau eines einfachen, verschlüsselten Tunnels zwischen Domänen	314
Übung 1: Konfigurieren eines fremden Servers für IPSec	314
Übung 2: Konfigurieren der Server einer Domäne für die IPSec-Kommunikation mit einem fremden Server	322
Lernzielkontrolle	328
Zusammenfassung der Lektion	329
Lektion 3: Einrichten von IPSec auf Internetservern	330
Verwenden von Zertifikaten zur Verteilung von geheimen IPSec-Schlüsseln	330
Praktische Übungen: Verwenden von Zertifikaten zum Austausch von geheimen IKE-Schlüsseln	331
Übung 1: Konfigurieren der Organisationszertifizierungsstelle zur Bereitstellung von IPSec-Zertifikaten	331
Übung 2: Bereitstellen von Zertifikaten für die IPSec-Verschlüsselung	333
Lernzielkontrolle	339
Zusammenfassung der Lektion	340
Lektion 4: Beheben von Fehlern der IPSec-Konfiguration	341
Mögliche Ursachen für das Versagen von IPSec	341
Die Kommunikation zwischen den Endsystemen funktioniert nicht richtig	342
Die Filter sind falsch konfiguriert	342
IKE verfügt nicht über einen passenden Satz von geheimen Schlüsseln	342
IPSec kann keinen kompatiblen Verschlüsselungssatz oder Authentifizierungsalgorithmus aushandeln	343
Ein Zwischensystem verändert die Pakete	343

Praktische Übungen: Beheben von Fehlern bei der IPSec-Kommunikation	344
Übung 1: Aktualisieren der IPSec-Sicherheitsrichtlinie einer Domäne.....	344
Übung 2: Enthält das Zertifikat einen privaten Schlüssel?	344
Übung 3: Neustarten des IPSec-Richtlinien-Agents	346
Übung 4: Aktivieren der IKE-Protokollierung.....	346
Lernzielkontrolle.....	347
Zusammenfassung der Lektion	348
Kapitel 9 Remotezugriff und VPNs.....	349
Über dieses Kapitel	349
Bevor Sie beginnen.....	350
Lektion 1: Schützen von RRAS-Servern.....	351
Grundlagen der RRAS-Sicherheit.....	351
Gesichtspunkte der RAS-Sicherheit	351
Folgen von Single Sign-On für die Sicherheit	353
Konfigurieren eines neuen RRAS-Servers	353
Die voreingestellte RRAS-Konfiguration	354
Konfigurationsoptionen für RRAS	354
Verwalten der RRAS-Sicherheitsoptionen	355
Konfigurieren der RRAS-Servereigenschaften	355
Konfigurieren der Benutzereigenschaften	355
Praktische Übungen: Schützen von RRAS-Servern	355
Übung 1: Konfigurieren eines Servers für RRAS.....	355
Übung 2: Verwalten eines RRAS-Servers.....	358
Lernzielkontrolle.....	361
Zusammenfassung der Lektion	362
Lektion 2: Verwalten der RRAS-Authentifizierung	363
Konfigurieren der RRAS-Authentifizierung von Windows.....	363
PAP und CHAP.....	363
EAP	364
Zugriff ohne Authentifizierung	364
Verwenden von RADIUS und IAS	364
Wie funktioniert IAS?	365
Konfigurieren der RADIUS-Authentifizierung	366
Praktische Übungen: Konfigurieren der RRAS-Authentifizierung und eines IAS-Servers	366
Übung 1: Auswählen der Windows-Authentifizierung	366
Übung 2: RADIUS und IAS.....	368
Lernzielkontrolle.....	375
Zusammenfassung der Lektion	376
Lektion 3: Schützen von Remoteclients	377
Verwalten der RAS-Richtlinien	377
Zugriff auf die RAS-Richtlinien	377
Erstellen und Bearbeiten von RAS-Richtlinien.....	378

Verwalten des Profils für eine Richtlinie	379
Verwenden des Verbindungs-Manager-Verwaltungskits	380
Arbeiten mit Dienstprofilen	381
Angeben von Dienstnamen und Supportinformationen	381
Netzwerk und DFÜ-Verbindungen	381
Unterstützung für VPNs.	381
Vorgänge und Anwendungen	382
Ändern von Grafiken und Symbolen	382
Software und Dokumentation	382
Verwenden des Verbindungs-Managers	382
Praktische Übungen: Schützen von Remoteclients.....	383
Übung 1: Verwalten der RAS-Richtlinien	383
Übung 2: Der Verbindungs-Manager.....	388
Lernzielkontrolle	392
Zusammenfassung der Lektion	393
Lektion 4: Schützen der Kommunikation über ein VPN.....	394
Was sind virtuelle private Netzwerke?.....	394
PPTP	394
L2TP	395
Festlegen des VPN-Protokolls	395
Aktivieren der L2TP-Filterung auf dem Server	395
Konfigurieren der VPN-Einstellungen des Clients	395
Praktische Übungen: Konfiguration und Fehlerbehebung bei VPN-Protokollen	396
Übung 1: Konfigurieren eines RRAS-Servers	396
Übung 2: Herstellen einer sicheren Verbindung zum L2TP-VPN-Server.....	405
Lernzielkontrolle	408
Zusammenfassung der Lektion	409
Kapitel 10 Sicherheit in drahtlosen Netzwerken.....	411
Über dieses Kapitel	411
Bevor Sie beginnen	411
Lektion 1: Einrichten eines drahtlosen Netzwerks	413
Drahtlose Technologien	413
Aufsetzen eines Infrastruktur-WLANs	414
Häufige Angriffe auf drahtlose Netzwerke	415
Praktische Übungen: Verbinden eines Zugriffspunkts und eines Clients mit dem Netzwerk	415
Übung 1: Konfigurieren eines drahtlosen Zugriffspunkts	416
Übung 2: Konfigurieren eines Clientcomputers für die Verbindung zu einem drahtlosen Netzwerk	420
Lernzielkontrolle	422
Zusammenfassung der Lektion	423
Lektion 2: Schützen von drahtlosen Netzwerken.....	424
Grundlagen von Wired Equivalent Privacy (WEP)	424

Die Sicherheitsprobleme von WEP	425
Verwalten von WEP auf dem Client	426
Praktische Übungen: Einrichten der WEP-Verschlüsselung	426
Übung 1: Sicherheitskonfiguration eines drahtlosen Zugriffspunkts	426
Übung 2: Konfigurieren von WEP auf dem Client	429
Lernzielkontrolle	432
Zusammenfassung der Lektion	433
Lektion 3: Konfigurieren der Clients	434
Sicherer Zugang	434
Erkennen von Sicherheitsproblemen einer 802.1x-Implementierung	436
Fehlerbehebung bei 802.1x-Verbindungen	436
Praktische Übungen: Einrichten eines Netzwerks für die 802.1x-Authentifizierung	437
Übung 1: Installieren von IAS	437
Übung 2: Konfigurieren des Zugriffspunkts für 802.1x	448
Übung 3: Konfigurieren von Windows XP für 802.1x	448
Lernzielkontrolle	452
Zusammenfassung der Lektion	453
Kapitel 11 Sicherheit von öffentlichen Anwendungsservern	455
Über dieses Kapitel	455
Bevor Sie beginnen:	455
Lektion 1: Sicherheit im Internet	456
Die Anforderungen	456
Bedrohungen der Sicherheit	457
Angriffsarten	457
Angriffsmethoden	457
Angriffswege	458
Schützen von öffentlichen Diensten	459
Sicherheit durch Firewalls	459
Firewalltypen	462
Firewall-Router	462
Sicherheitsproxys	463
ISA Server	464
Praktische Übungen: Konfigurieren einer Firewall	464
Übung 1: Installieren und Konfigurieren von ISA Server	465
Lernzielkontrolle	472
Zusammenfassung der Lektion	473
Lektion 2: Konfigurieren von Microsoft SQL Server	474
Schützen von öffentlichen Datenbankservern	474
Der richtige Platz für Datenbankserver	475
Schützen von Microsoft SQL Server	475
Praktische Übungen: Einrichten der SQL Server-Sicherheit für das Internet	476
Übung 1: Veröffentlichen des SQL-Servers	476

Übung 2: Aktivieren der SSL-Verschlüsselung auf dem SQL-Server	478
Übung 3: Überprüfen der SQL-Verbindung über eine Firewall hinweg.....	480
Lernzielkontrolle	483
Zusammenfassung der Lektion	484
Lektion 3: Schützen von Microsoft Exchange Server für die Arbeit im Internet.....	485
Ausnutzen von offenen Relays	485
Angemessener Schutz für Exchange Server.....	486
Schützen von Exchange Server mit einem Relay-Mailserver.....	487
Schützen von Exchange Server mit einem starken Sicherheitsproxy.....	487
Schützen der Anmeldeinformationen mit SSL	487
Praktische Übungen: Schützen von Microsoft Exchange für die Verwendung im Internet.....	488
Übung 1: Weiterleiten von Ports an Exchange	488
Übung 2: Einrichten einer sicheren Kennwortauthentifizierung	490
Übung 3: Überprüfen der Sicherheit von Exchange Server.....	495
Lernzielkontrolle	499
Zusammenfassung der Lektion	500
 Kapitel 12 Sicherheit von Webdiensten	501
Über dieses Kapitel	501
Bevor Sie beginnen.....	501
Lektion 1: Schützen von öffentlichen Webservern.....	502
Was sind die Internet-Informationsdienste?.....	502
Einrichten der IIS-Sicherheit	502
Festlegen von Sicherheitseinstellungen	503
Verwalten von Eigenschaften der Verzeichnissicherheit	503
Einschränkungen von IP-Adressen und Domäennamen.....	504
Aufrechterhalten der Sicherheit von IIS	504
Praktische Übungen: Einrichten der IIS-Sicherheit	505
Übung 1: Einstellen der Sicherheitsoptionen	505
Lernzielkontrolle.....	508
Zusammenfassung der Lektion	509
Lektion 2: Authentifizierung im Web	510
Grundlagen der Authentifizierung im Web.....	510
Anonyme Anmeldung	511
Standardauthentifizierung.....	511
Digestauthentifizierung	512
Integrierte Windows-Authentifizierung	512
Zertifikate	512
Konfiguration für die Authentifizierung im Web	513
Praktische Übungen: Auswählen von Authentifizierungsmethoden.....	513
Übung 1: Einrichten der anonymen Anmeldung	513
Übung 2: Festlegen der Authentifizierungsmethode.....	515
Lernzielkontrolle	518

Zusammenfassung der Lektion	519
Lektion 3: Verwenden von SSL	520
Wie funktioniert SSL?	520
Erwerb und Installation von SSL-Zertifikaten	520
Installieren von Serverzertifikaten	521
Anfordern von Zertifikaten von einer externen Zertifizierungsstelle	521
Verwalten von Serverzertifikaten	521
Einstellen von SSL-Optionen	521
Einsehen der Einzelheiten von Zertifikaten	522
Erneuern und Entfernen von Zertifikaten	522
Authentifizieren von Clients	522
Aktivieren von Clientzertifikaten	522
Installieren von Clientzertifikaten	523
Verwalten der Einstellungen für Clientzertifikate	523
Zuordnen von Clientzertifikaten	523
Verwenden einer Zertifikatsvertrauensliste	524
Praktische Übungen: SSL	524
Übung 1: Einrichten von SSL in IIS	524
Übung 2: Verwenden von Clientzertifikaten	530
Lernzielkontrolle	542
Zusammenfassung der Lektion	543
Kapitel 13 Intrusion Detection und Ereignisüberwachung	545
Über dieses Kapitel	545
Bevor Sie beginnen	545
Lektion 1: Einrichten eines Intrusion-Detection-Systems für öffentliche Server	546
Häufige Arten von Netzwerkeinbrüchen	546
Erkennen von Netzwerkeinbrüchen	547
Erkennen von Denial-of-Service-Angriffen	547
Erkennen von Angriffen auf Schwachstellen	548
Erkennen von Angriffen mit falscher Identität	548
Verwenden eines Decoy-Servers	549
Die Psychologie der Intrusion Detection mit Decoy-Systemen	550
Festlegen der Ports für den „Lockvogel“	551
Der richtige Platz für einen Decoy-Server	552
Grenzen der Intrusion Detection mit Decoy-Systemen	552
Durchführen der Ereignisanalyse und Sicherstellen der Beweise	552
Praktische Übungen: Aufspüren von Eindringlingen	553
Übung 1: Konfigurieren eines Decoy-Servers	554
Lernzielkontrolle	558
Zusammenfassung der Lektion	559
Lektion 2: Ereignisüberwachung in privaten Netzwerken	560
Intrusion Detection in privaten Netzwerken	560

Erkennen eines Angriffs	560
Der schlimmste Fall	561
Administratoren und Kennwörter	562
Sicherstellen der Beweise	563
Durchsuchen von Überwachungsprotokollen mit EventComb	563
Erwerb und Installation von EventComb	563
Verwendung von EventComb	564
Konfigurieren der Ereignisprotokolle für EventComb	565
Praktische Übungen: Verwalten von Ereignisprotokollen	565
Übung 1: Konfigurieren von Ereignisprotokollen	565
Übung 2: Verwenden von EventComb	566
Lernzielkontrolle	569
Zusammenfassung der Lektion	570
 Kapitel 14 Softwarewartung	 571
Über dieses Kapitel	571
Bevor Sie beginnen	571
Lektion 1: Service Packs und Hotfixes	572
Was sind Service Packs und Hotfixes?	572
Ermitteln der zurzeit installierten Service Packs und Hotfixes	572
Befehlszeilenoptionen für Qfecheck.exe	573
Verwalten von Service Packs und Hotfixes	573
Installieren eines Service Packs	573
Extrahieren eines Service Packs	574
Installieren eines Hotfixes	574
Entfernen eines Service Packs oder Hotfixes	574
Slipstreaming von Service Packs und Hotfixes	575
Hinzufügen eines Service Packs zu einer Installationsfreigabe	575
Hinzufügen von Hotfixes zu einer Installationsfreigabe	575
RIS	576
Installieren von RIS	576
Erstellen eines RIS-Installationsabilds	576
Installieren von Clients mit RIS	577
Praktische Übungen: Verwalten von Service Packs und Hotfixes	577
Übung 1: Manuelle Installation von Service Packs und Hotfixes	577
Übung 2: Slipstreaming von Service Packs und Hotfixes	579
Übung 3: Verwenden von RIS	582
Lernzielkontrolle	587
Zusammenfassung der Lektion	588
Lektion 2: Automatische Aktualisierungen mit Microsoft Software Update Services	589
Verwenden von Windows Update	589
Zugang zu Windows Update	589
Verwenden des Windows Update-Katalogs	590

Automatische Updates	590
Installieren der Funktion Automatische Updates	591
Konfigurieren des Clients für Automatische Updates	591
Installieren und Konfigurieren der Software Update Services	591
Installieren der Software Update Services	591
Konfigurieren der Software Update Services	591
Synchronisieren von Aktualisierungen	591
Akzeptieren von automatischen Aktualisierungen	592
Konfigurieren des Clients für Automatische Updates	592
Praktische Übungen: Verwenden der Software Update Services	592
Übung 1: Verwalten von automatischen Aktualisierungen	593
Übung 2: Verwenden der Software Update Services	598
Lernzielkontrolle	606
Zusammenfassung der Lektion	607
Lektion 3: Bereitstellen von Aktualisierungen im Unternehmen	608
Verwenden von Gruppenrichtlinien zur Bereitstellung von Software	608
Funktionsweise von MSI-Installationspaketen	608
Erstellen des Gruppenrichtlinienobjekts	609
Installieren mehrerer Hotfixes	609
Verwenden von Qchain.exe	609
Verwenden von Batchdateien	609
Werkzeuge für das Sicherheitsmanagement	610
Microsoft Baseline Security Analyzer	610
HFNetChk	610
SMS	611
Praktische Übungen: Bereitstellen mehrerer Hotfixes im Unternehmen	611
Übung 1: Bereitstellen von Aktualisierungen mit Hilfe von Gruppenrichtlinien	611
Übung 2: Verwenden von Qchain und Batchdateien	613
Lernzielkontrolle	614
Zusammenfassung der Lektion	615
Anhang A Fragen und Antworten	617
Kapitel 1: Gruppenrichtlinien	617
Lektion 1: Active Directory und Gruppenrichtlinien	617
Lektion 2: Konfigurieren von Gruppenrichtlinien	617
Lektion 3: Konfigurieren der Sicherheitsrichtlinien für Clientcomputer	618
Lektion 4: Beheben von Fehlern bei der Anwendung von Gruppenrichtlinien	618
Lektion 5: Grenzen von Sicherheitseinstellungen	619
Kapitel 2: Benutzerkonten und Sicherheitsgruppen	619
Lektion 1: Anlegen von lokalen Benutzerkonten und Sicherheitsgruppen	619
Lektion 2: Active Directory-Domänenkonten und Sicherheitsgruppen	620
Kapitel 3: Einschränkungen für Konten, Benutzer und Gruppen	620
Lektion 1: Kontorichtlinien	620

Lektion 2: Verwalten von Benutzerrechten.....	621
Lektion 3: Zugriffssteuerung durch eingeschränkte Gruppen.....	621
Lektion 4: Verwalten von Sicherheitsvorlagen	622
Kapitel 4: Sicherheit auf der Grundlage von Konten	622
Lektion 1: Verwalten von Dateisystemberechtigungen	622
Lektion 2: Freigabesicherheit	623
Lektion 3: Überwachungsrichtlinien.....	624
Lektion 4: Einbeziehen der Registrierung	624
Kapitel 5: Zertifizierungsstellen	625
Lektion 1: Grundlagen zu Zertifikaten	625
Lektion 2: Installieren der Windows 2000-Zertifikatsdienste.....	625
Lektion 3: Warten von Zertifizierungsstellen	626
Kapitel 6: Verwalten einer Infrastruktur öffentlicher Schlüssel	626
Lektion 1: Computerzertifikate	626
Lektion 2: Bereitstellen von Benutzerzertifikaten	627
Lektion 3: Verwenden von Smartcard-Zertifikaten	627
Lektion 4: Bereitstellen von S/MIME-Zertifikaten	628
Kapitel 7: Verbesserte Authentifizierung	628
Lektion 1: Unterstützung von Clients mit älteren Windows-Versionen	628
Lektion 2: Unterstützung von Macintosh-Clients	629
Lektion 3: Vertrauensstellungen.....	629
Kapitel 8: IPSec	630
Lektion 1: Einrichten von IPSec in einer Domäne	630
Lektion 2: Einrichten von IPSec zwischen Netzwerken ohne Vertrauensstellung.....	631
Lektion 3: Einrichten von IPSec auf Internetservern	631
Lektion 4: Beheben von Fehlern der IPSec-Konfiguration	631
Kapitel 9: Remotezugriff und VPNs	632
Lektion 1: Schützen von RRAS-Servern	632
Lektion 2: Verwalten der RRAS-Authentifizierung	633
Lektion 3: Schützen von Remoteclients	633
Lektion 4: Schützen der Kommunikation über ein VPN	634
Kapitel 10: Sicherheit in drahtlosen Netzwerken.....	634
Lektion 1: Einrichten eines drahtlosen Netzwerks	634
Lektion 2: Schützen von drahtlosen Netzwerken.....	635
Lektion 3: Konfigurieren der Clients	635
Kapitel 11: Sicherheit von öffentlichen Anwendungsservern.....	636
Lektion 1: Sicherheit im Internet	636
Lektion 2: Konfigurieren von Microsoft SQL Server	637
Lektion 3: Schützen von Microsoft Exchange Server für die Arbeit im Internet.....	637
Kapitel 12: Sicherheit von Webdiensten	638
Lektion 1: Schützen von öffentlichen Webservern.....	638
Lektion 2: Authentifizierung im Web	638
Lektion 3: Verwenden von SSL	639
Kapitel 13: Intrusion Detection und Ereignisüberwachung	639

Lektion 1: Einrichten eines Intrusion-Detection-Systems für öffentliche Server	639
Lektion 2: Ereignisüberwachung in privaten Netzwerken	640
Kapitel 14: Softwarewartung	640
Lektion 1: Service Packs und Hotfixes	640
Lektion 2: Automatische Aktualisierungen mit Microsoft Software Update Services ..	641
Lektion 3: Bereitstellen von Aktualisierungen im Unternehmen	641
Glossar	643
Index	655
Systemvoraussetzungen	667