

Dr. Tobias Weltner, Kai Wilke, Björn Schneider

# **Windows-Sicherheit**

## **Das Praxisbuch**

***Microsoft***

# Inhaltsverzeichnis

<b>Vorwort</b> .....	<b>XXI</b>
Die Autoren .....	XXI
... und die vielen Helfer .....	XXII
In letzter Minute .....	XXII
<b>TeilA</b>	
<b>Was ist Sicherheit?</b> .....	<b>1</b>
<b>1 Probleme erkennen</b> .....	<b>3</b>
Ein ganz normaler Tag .....	3
Risiken erkennen .....	4
Was ist Sicherheit? .....	5
Risiken quantifizieren .....	7
Sicherheitsstrategien .....	8
Worauf es Angreifer absehen .....	9
Einschätzung und Sicherheitsstufen .....	12
Die Bedrohung konkretisieren .....	14
Wir hier drinnen und die da draussen .....	15
Verletzlichkeiten identifizieren .....	19
Schwachpunkte erkennen .....	20
Exploits und ihre Gemeinsamkeiten .....	20
Risiken managen .....	23
Sicherheitsrichtlinien etablieren .....	23
Reaktionspläne definieren .....	24
Fazit: Die Elemente Ihrer Sicherheitsstrategie .....	25
<b>2 Angriffe auf Ihr System</b> .....	<b>27</b>
Ein Webserver verabschiedet sich .....	27
Footprinting: eine Landkarte des Internets wird erstellt .....	28
Systeme identifizieren .....	28
Der Coup: Angreifer springen auf den Zug .....	32
Eine Epidemie breitet sich aus .....	34
»Code Red« wird entdeckt .....	34
Augenzeuge: Angriffe, die gerade stattfinden .....	35
Weltweite Erschütterungen .....	37
Analyse des Beispiels .....	38
Technikschwäche .....	38
Konfigurationsschwäche .....	38
Richtlinienschwäche .....	39

## TeilB

### Grundlagen der Hostsicherheit

41

<b>3</b>	<b>Sicherheits-Mechanismen</b> .....	<b>43</b>
	Die Team Player des Sicherheitssystems .....	44
	Gesicherte Ressourcen und Systemfunktionen .....	44
	Die Anwender: Security Principals .....	45
	Sicherheitsarchitektur aufbauen .....	45
	Planungsphase .....	46
	Sicherheit im Alltag gewährleisten .....	48
<b>4</b>	<b>Die Anmeldung</b> .....	<b>49</b>
	Arten der Anmeldung .....	49
	Interaktive Anmeldung .....	50
	Netzwerkanmeldung .....	51
	Anmeldung über Terminal Dienste .....	51
	Sonderfall SmartCards .....	52
	SmartCard-Standards .....	53
	SmartCard-Integration .....	53
	Der Authentifizierungsvorgang .....	53
	Wahl der Authentifizierungsmethode .....	54
	Die SAM-Datenbank .....	55
	Was in der SAM-Datenbank lagert .....	55
	SAM-Datenbank in der Registrierungsdatenbank öffnen .....	56
	Was im Active Directory lagert .....	58
<b>5</b>	<b>Benutzerkonten</b> .....	<b>59</b>
	Lokale Benutzerkonten .....	59
	Netzwerke ohne Domänencontroller .....	60
	Netzwerke mit Domänencontroller .....	60
	Domänen-Benutzerkonten .....	61
	Am Domänencontroller anmelden .....	61
	Macht der Benutzerkonten .....	63
	Rechte und Berechtigungen .....	63
	Gruppenmitgliedschaften .....	63
<b>6</b>	<b>Gruppen</b> .....	<b>65</b>
	Lokale Gruppen .....	66
	Vordefinierte lokale Gruppen .....	66
	Neues Windows 2000 Sicherheitsmodell .....	67
	Softwareinstallation im Benutzerprofil .....	68
	Gruppe »Administratoren« .....	68
	Gruppe »Hauptbenutzer« .....	69
	Gruppe »Benutzer« .....	70
	Automatisch verwaltete Gruppen .....	70
	Domänen-Gruppen .....	71
	Gruppentypen: Lokal, Global, Universal .....	72

Verteilergruppen	73
Mit Gruppen Berechtigungen verteilen	73
A-G-P-Prinzip: Einzelne Domäne	74
A-G-L-P-Prinzip: Domänengrenzen sprengen	75
A-G-DL-P-Prinzip: Native Mode ausnutzen	76
Universal Groups einsetzen	77
<b>Zugriffsberechtigungen</b>	<b>79</b>
Elektronische Schlüssel und SIDs	79
Ein Access Token genauer untersuchen	80
SIDs: Eindeutige Sicherheitsobjekte	81
Der Aufbau einer SID	82
Inhalt des Access Tokens analysieren	86
Verletzbarkeiten	87
Berechtigungen erteilen	89
Das elektronische Schloss: Security Descriptor	90
Wie Schlüssel elektronische Schlösser öffnen	93
Vererbare Berechtigungen verstehen	95
Vererbungsverfahren	95
Berechnung der effektiven Berechtigungen	96
<b>Systemrechte</b>	<b>97</b>
Systemrechte verstehen	97
Lokale Rechte festlegen	97
Zentrale Verwaltung	98
Konflikte zwischen Rechten und Berechtigungen	100
Übersicht über Systemrechte	100
Anmelde-Rechte	100
Sicherheitsrechte	101
Ressourcenverteilung	102
Herunterfahren und Ausdocken	103
Domänenverwaltung	103
Allgemeine Systemfunktionen	103
<b>Registrierungsdatenbank</b>	<b>105</b>
Die Registrierungsdatenbank verstehen	106
Hives: die Registrierungsdatenbank-Zweige	106
Policies: die ADM-Dateien	108
Registrierungsdatenbank-Einstellungen dokumentieren	108
Maßgeschneiderte Registrierungsdatenbank-Editoren	109
ADM-Dateien verwalten	111
Automatisch eingebundene ADM-Dateien	111
Zusätzliche ADM-Dateien einbinden	112
Sicherheitsoptionen	113
Sicherheitsvorlagen definieren die Optionen	114
Sensible Bereiche der Registrierungsdatenbank	115
Policy-Zweige in der Registrierungsdatenbank	116

<b>10 Gruppenrichtlinien</b> .....	<b>117</b>
Gruppenrichtlinien verstehen .....	118
Lokale GPO .....	118
GPOs im Active Directory .....	120
Einstellungen, die GPOs transportieren .....	121
Technische Umsetzung der Gruppenrichtlinien .....	122
Group Policy Container (GPC) .....	122
Group Policy Templates (GPT) .....	124
Umsetzung auf den Clients .....	125
Anwendung der Gruppenrichtlinien .....	126
Prüfungsintervall der Gruppenrichtlinien .....	127
Wie Gruppenrichtlinien verarbeitet werden .....	127
Vererbung von Gruppenrichtlinien .....	128
Kumulation von Gruppenrichtlinien-Eigenschaften .....	129
GPOs an Gruppenmitgliedschaften knüpfen .....	130
Gruppenrichtlinien verwalten .....	131
Neue Gruppenrichtlinien anlegen .....	131
Bestehende Gruppenrichtlinien anpassen .....	133
Sicherheitseinstellungen und Vorlagen verwenden .....	133
Sicherheitsvorlagen verstehen .....	133
Sicherheitsvorlagen in Gruppenrichtlinien kopieren .....	134
Sicherheitsvorlagen manuell anwenden .....	136
Systemsicherheit analysieren .....	136
Eigene Sicherheitsvorlagen anlegen .....	141
Fragen und Antworten .....	145

## Teilt

<b>Grundlagen der Kryptografie</b> .....	<b>149</b>
--	------------

<b>11 Kryptografie</b> .....	<b>151</b>
Kryptografische Verfahren .....	152
Symmetrische Verschlüsselung .....	153
Asymmetrische Verschlüsselung .....	156
Hash - Digitale Fingerabdrücke .....	160
Digitale Unterschriften .....	163
Verschlüsselungsalgorithmen .....	164
Wie kryptografische Algorithmen entstehen .....	164
Sichere Algorithmen und proprietäre Ansätze .....	164
Algorithmen für die symmetrische Verschlüsselung .....	165
Algorithmen für die asymmetrische Verschlüsselung .....	166
Risiken und Angriffsflächen .....	166
Einsatz von Algorithmen in Windows .....	168
Die CryptoAPI verstehen .....	169
Die Rolle der CryptoAPI .....	169
SmartCards und andere Erweiterungen .....	170
Skriptzugriff auf die CryptoAPI .....	170

<b>12 Public Key Infrastruktur (PKI)</b>	<b>171</b>
Die Rolle der Public Key Infrastruktur	171
Bestandteile einer PKI	172
Zertifikate	172
Öffentliche Schlüssel	173
Der Private Schlüssel	174
Zertifikate überprüfen	175
Vertrauenswürdige Zertifikate	176
Der Zertifikatspeicher	179
Empfehlungen	181
Zertifizierungsstellen	181
Die Rolle des Zertifikatherausgebers	181
Selbstsignierte Zertifikate	182
Zertifizierungsstellen	183
Zertifikate beantragen	183
Mit makecert.exe Zertifikate erstellen	184
Eigene Zertifizierungsstelle betreiben	191
Testzertifizierungsstelle verwenden	191
Eigene Zertifizierungsstelle installieren	191
<b>13 Kerberos</b>	<b>197</b>
Kerberos verstehen	197
Warum Kerberos?	197
Wie Kerberos funktioniert	198
Kerberos als PKI verstehen	198
Ein Anwender meldet sich an	199
Der Anwender greift auf Ressourcen zu	201
Kennwortübertragungen mit Kerberos	201
<b>TeilD</b>	
<b>Grundlagen Active Directory und Netzwerk</b>	<b>205</b>
<b>14 Netzwerk-Grundlagen</b>	<b>207</b>
Netzwerktransport und Protokolle	207
Die Anwendungsschicht	209
HTTP & Co: Anwendungsprotokolle	209
Die Transportschicht	211
Ports - die Dienste eines Servers	211
Die Transportprotokolle: TCP oder UDP	212
UDP - schnell, aber sorglos	213
Die Internetschicht	215
Das IP-Protokoll	215
DNS-Namensauflösungen	215
Wie IP-Adressen funktionieren	216
Die Routing Tabelle	216
Die Netzwerkkartenschicht	218
Das ARP-Protokoll	218

Hubs - Netzwerk-Mehrfachsteckdosen .....	220
Switches - »intelligente« Hubs .....	221
Router trennen Netzwerksegmente .....	222
Firewalls selektieren Pakete nach Inhalt .....	222
<b>15 Drahtlose Netzwerke .....</b>	<b>225</b>
Die Standards .....	225
Die Kanäle .....	226
Die Betriebsmodi .....	227
Der Ad Hoc Mode .....	227
Infrastructure Mode .....	227
Authentifizierung .....	228
Open System Authentication .....	228
<b>16 Active Directory-Grundlagen .....</b>	<b>231</b>
Active Directory Einführung .....	231
Vorteile des Active Directory .....	232
Neue Sicherheitsgrenzen .....	232
Welche Macht haben fremde Domänen? .....	233
Vertrauensstellungen verstehen .....	233
Sicherheitsrisiko Vertrauensstellung .....	233
Sicherheitsrisiko Replikation .....	235
Organisationseinheiten .....	235
Sicherheitsaspekte .....	235
<b>TeilE</b>	
<b>Praxis Hostverteidigung .....</b>	<b>237</b>
<b>17 Sicherheitsscanner .....</b>	<b>239</b>
Sicherheits-Analyse-Werkzeuge .....	239
Kostenlose Microsoft-Werkzeuge .....	239
Analysetools von Drittherstellern .....	240
Der Baseline Security Analyzer .....	241
Baseline Security Analyzer offline verwenden .....	241
Sicherheitstest durchführen .....	242
Sicherheitsanalyse von der Konsole starten .....	243
Sicherheitsreport verstehen .....	244
Sektion Vulnerabilities .....	245
Sektion Additional Systeminformation .....	248
Sektion Internet Information Services .....	249
Sektion Additional System Information .....	251
Sektion SQL Server Scan Results .....	252
Sektion Desktop Application Scan Results .....	254
<b>18 Kennwort- und Anmeldesicherheit .....</b>	<b>257</b>
Sicherheitsrisiken .....	258
Risiken von Kennwörtern .....	258

SmartCard-Anmeldungen . . . . .	259
Biometrische Verfahren . . . . .	259
Anmeldedaten im Netzwerk schützen . . . . .	260
Master-Datenbank mit Benutzerkontoinformationen . . . . .	260
Anmeldevorgang absichern . . . . .	261
Anmeldehinweis anzeigen . . . . .	261
Benutzernamen anzeigen . . . . .	261
Secure Attention Sequence (SAS) . . . . .	262
Zwischengespeicherte Anmeldungen . . . . .	263
EntSperrung nur über Domänencontroller . . . . .	264
Unsichere Authentifizierungsmethoden deaktivieren . . . . .	264
NTLMv2 für Windows 9x Clients . . . . .	266
Kennworte mit Kennwortrichtlinien absichern . . . . .	267
Kennwortrichtlinien konfigurieren . . . . .	268
Kontosperrungsrichtlinien . . . . .	274
Kerberos-Richtlinie . . . . .	276
Leere Kennworte im Netzwerk verbieten . . . . .	277
SmartCard-Anmeldung verwenden . . . . .	278
<b>19 Benutzerverwaltung . . . . .</b>	<b>285</b>
Eingebaute Benutzerkonten sichern . . . . .	286
Eingebautes Administratorkonto entschärfen . . . . .	286
Administrator-Konto umbenennen . . . . .	287
Dummy-Administrator einrichten . . . . .	289
EFS-Zertifikat sichern . . . . .	290
Administrator-Konto deaktivieren . . . . .	290
Veraltete Konten identifizieren . . . . .	290
Konten sperren . . . . .	292
Konten löschen . . . . .	295
Administrative Macht einschränken . . . . .	295
Einer für alle - alle auf einen! . . . . .	297
Administratorstatus als universeller »Problemloser« . . . . .	298
Administrative Macht dosieren . . . . .	298
Administration delegieren . . . . .	303
»Ausführen als« einsetzen . . . . .	304
Automatische Benutzeranmeldung . . . . .	306
Automatikanmeldungen über die Registrierungsdatenbank . . . . .	307
Sichere Automatik-Anmeldung . . . . .	307
Sichere Rechte für Benutzer . . . . .	308
Abwärtskompatibilität zu NT 4.0 herstellen . . . . .	308
Sicherheitsvorlage compatws.inf verwenden . . . . .	309
Sicherheitslücken bei der Windows NT 4.0-Migration . . . . .	313
Sicherheitseinstellungen der Benutzerkonten . . . . .	314
Sicherheitsoptionen für Konten festlegen . . . . .	315
Benutzerkonto-Vorlagen verwenden . . . . .	317
Neue Konten auf Vorlagenbasis einrichten . . . . .	318
Konto-Verwaltungstools einsetzen . . . . .	318



Eingeschränkte Gruppen verwenden .....	333
Administrative Gruppen über Eingeschränkte Gruppen verwalten .....	334
Fragen und Antworten .....	336
<b>20 Dienste konfigurieren .....</b>	<b>339</b>
Installierte Dienste identifizieren .....	340
Kritische Dienste mit MBSA prüfen .....	340
Dienste mit der MMC kontrollieren .....	341
Dienste mit NET-Befehl verwalten .....	342
Eindeutige Dienstnamen bestimmen .....	343
Abhängigkeiten von Diensten bestimmen .....	344
Entbehrliche Dienste finden .....	345
Dienste für Clients .....	345
Basisdienste für alle Server .....	351
Anwendungsserver .....	353
Datei- und Druckserver .....	353
Infrastruktur-Server .....	353
Webserver .....	354
Domänencontroller .....	354
Dienste deaktivieren .....	354
Dienste manuell deaktivieren .....	355
Dienste unternehmensweit konfigurieren .....	356
Dienste per Skript deaktivieren .....	358
Dienste deinstallieren .....	361
Dienste skriptgesteuert deinstallieren .....	361
<b>21 Registry-Absicherung .....</b>	<b>363</b>
Registry-Zugriff schützen .....	363
Zugriffsberechtigungen setzen .....	363
Überprüfen der Basis-Berechtigungen .....	367
Basis-Sicherheit wiederherstellen .....	369
Netzwerkzugriff kontrollieren .....	369
Netzwerkzugriff testen .....	370
Netzwerkzugriff unterbinden .....	370
Ausnahmen für den Netzwerkzugriff erlauben .....	372
Lücken in der Netzwerksicherheit .....	372
Abwärtskompatibilität herstellen .....	374
Sicherheitsberechtigungen lockern .....	375
Maßgeschneiderte Abwärtskompatibilität .....	375
<b>22 Systemüberwachung .....</b>	<b>377</b>
Systemüberwachung verstehen .....	378
Die Ereignisprotokolle .....	378
Physischer Aufbewahrungsort .....	378
Informationen filtern .....	380
Sicherheitsprotokoll verwenden .....	381
Ereignisprotokolle verwalten .....	381

Größe der Ereignisprotokolle festlegen . . . . .	382
Ereignisprotokolle sichern und löschen . . . . .	385
Automatische Protokollverwaltung . . . . .	386
Sicherheitsüberwachung aktivieren . . . . .	389
Überwachungskategorien auswählen . . . . .	391
Übernahme der Einstellungen kontrollieren . . . . .	391
Überwachungsaufträge erteilen . . . . .	391
Andere Objektzugriffe überwachen . . . . .	393
Ereignisprotokolle analysieren . . . . .	393
Nach Ereignis-IDs suchen . . . . .	393
Eingebaute Filterfunktion . . . . .	394
Skriptgesteuert Ereignisprotokolle analysieren . . . . .	394
Ereignis-IDs und ihre Bedeutung . . . . .	402
Anmeldeereignisse . . . . .	402
Benutzerkonten und Gruppen . . . . .	403
Rechteverwendung kontrollieren . . . . .	404
Richtlinienänderungen . . . . .	405
Objektzugriffe überwachen . . . . .	405
Sicherheitsereignisse des Systems . . . . .	405
<b>23 Patch-Management . . . . .</b>	<b>407</b>
Hotfixes, Service Packs & Co. . . . .	407
Hotfixes oder QFEs . . . . .	409
Service Packs . . . . .	409
Kumulative Updates und Rollup Packages . . . . .	409
Patch-Management . . . . .	409
Aktuelle Informationen, Service Packs und Hotfixes erhalten . . . . .	410
Patchstatus eigener Systeme prüfen . . . . .	413
Überprüfung der Rechner mit HFNetChk . . . . .	415
HFNetChk-Zusatzoptionen . . . . .	416
Auswertung von HFNetChk-Ergebnissen . . . . .	419
Patchverteilung . . . . .	421
Direktes Client-Update über das Internet . . . . .	421
Manuelle Updates mit dem Windows Update Center . . . . .	423
Automatische Office-Updates . . . . .	423
Hotfix-Installation über Batch-Dateien . . . . .	425
Microsoft Software Update Service (SUS) . . . . .	426
SUS-Server administrieren . . . . .	427
SUS-Server synchronisieren . . . . .	428
Updates freigeben . . . . .	429
Logbücher einsehen . . . . .	430
Verfügbare Updates verwalten . . . . .	430
SUS-Server Optionen . . . . .	431
Clientkonfiguration . . . . .	432
Updates deinstallieren . . . . .	436
Hotfix-Verwaltung über Systemsteuerung . . . . .	436

24	Physische Sicherheit .....	439
	Physische Absicherung .....	439
	Serverraum .....	439
	Arbeitsstationen und Laptops .....	440
	Backups .....	442
	Angriffsmethoden .....	443
	SAM-Datenbank löschen .....	443
	Hash-Injektion in die SAM-Datenbank .....	444
	Zugriff auf EFS-verschlüsselte Daten .....	444
<b>Teil F</b>		
<b>Praxis Datenverteidigung</b>		<b>447</b>
25	Dateisystemsicherheit .....	449
	Das NTFS-Dateisystem einsetzen .....	449
	FAT-Laufwerke nach NTFS konvertieren .....	450
	Schwächen des NTFS-Dateisystems .....	450
	Basis-Sicherheit herstellen .....	451
	Die NTFS-Sicherheitsvorlagen verstehen .....	451
	Welche Berechtigungen werden gesetzt? .....	452
	Basisberechtigungen überprüfen .....	454
	Basis-Dateizugriffssicherheit implementieren .....	460
	NTFS-Basissicherung auf Windows XP .....	462
	Einfache Dateifreigabe .....	462
	Automatik-Schutz lokaler Benutzerprofile .....	463
	Neue Zugriffsberechtigungen festlegen .....	464
	Aktuelle Zugriffsberechtigungen untersuchen .....	464
	Eigene Berechtigungen definieren .....	468
	Neue Berechtigung einfügen .....	468
	Berechtigungen verstehen .....	469
	Vererbung verstehen .....	471
	Sicherheitsvorlagen definieren .....	475
	Sicherheitsvorlagen nachträglich bearbeiten .....	480
26	Netzwerkfreigaben .....	485
	Freigaben verwalten .....	485
	Überflüssige Freigaben entfernen .....	487
	Freigaben schützen .....	490
	Wie im Netzwerk freigegebene Daten geschützt sind .....	492
27	Verschlüsselndes Dateisystem (EFS) .....	495
	Verschlüsselndes Dateisystem .....	496
	Die Rolle von EFS .....	496
	Wie EFS funktioniert .....	496
	Wo kommen die EFS-Zertifikate her? .....	497
	EFS aus Anwendersicht .....	498
	Empfehlungen .....	501

EFS aus Administratorsicht .....	501
EFS aktivieren und abschalten .....	502
Empfehlungen .....	504
Gefahren von EFS .....	504
Sicherheitslimitationen .....	504
Datenwiederherstellungsagenten implementieren .....	505
Wie Datenwiederherstellungsagenten funktionieren .....	506
Datenwiederherstellungsagent rettet fremde Daten .....	512
Persönliche EFS-Zertifikate sichern .....	513
Backup von EFS-verschlüsselten Daten .....	514
EFS-Steuerung über Konsole oder Batch .....	514
EFS im Netzwerk .....	515
Delegationsvertrauen .....	516
Empfehlungen .....	516
Fragen und Antworten .....	517
<b>28 Temporäre Dateien .....</b>	<b>519</b>
Papierkorb-Einstellungen konfigurieren .....	519
Papierkorb über Gruppenrichtlinien konfigurieren .....	520
Gelöschte Daten permanent entfernen .....	520
Gelöschte Daten überschreiben .....	520
Auslagerungsdatei konfigurieren .....	521
Auslagerungsdatei automatisch löschen .....	521
Alte Systemordner entfernen .....	522
<b>TeilG</b>	
<b>Praxis Anwendungsverteidigung .....</b>	<b>523</b>
<b>29 Anwendungssicherheit .....</b>	<b>525</b>
Malware: Viren, Würmer & Co. ....	526
Programmcode in mehreren Facetten .....	526
Wie Malware ins System gelangt .....	526
Was sind die Ziele der Malware? .....	526
Virens Scanner .....	527
Software-Mißbrauch verhindern .....	527
Klassische Anwendungssoftware .....	527
Software auf Skriptbasis .....	528
Unfreiwillige Fernwartung .....	528
E-Mail-Vertraulichkeit .....	528
Allgemeine Empfehlungen .....	528
<b>30 Webbrowser-Sicherheit .....</b>	<b>531</b>
Webbrowser-Sicherheit .....	532
Sicherheitslücken in Webbrowsern .....	532
Vernünftige Sicherheitsstrategien .....	532
Sicherheitszonen im Internet Explorer .....	533
Lokales Internet .....	535

Vertrauenswürdige und eingeschränkte Sites	535
ActiveX und Java-Applets	536
ActiveX-Schutzmechanismen	536
Java-Schutzmechanismen	538
Scripting-Einschränkungen	539
Gefahren, die von Skripten ausgehen	540
Sicherheitskritische Operationen	541
Download-Beschränkungen	541
Benutzerauthentifizierung	541
Darstellung der Webseiten kontrollieren	542
Gruppenrichtlinien verwenden	545
Einstellungen über Gruppenrichtlinien verwalten	545
Voreinstellungsmodus verwenden	546
Browsen im sicheren Benutzerkontext	547
Internet Explorer unter anderem Kontext ausführen	547
Eingeschränkte Internet Explorer-Sitzung	548
Internetanwendungen deaktivieren	548
Praxis: Internet-Standardsoftware sperren	549
<b>31 E-Mail-Sicherheit</b>	<b>551</b>
E-Mail-Anhänge sichern	552
Virenschutzprogramme	552
E-Mail-Anhänge mit Outlook sichern	553
Outlook Express	562
E-Mail-Anhänge schützen	562
E-Mails signieren und verschlüsseln	566
Signierte E-Mails mit Outlook Express empfangen	571
Signierte E-Mails mit Outlook empfangen	573
E-Mails verschlüsseln	574
Sichere Mailserver-Anmeldung	576
Unverschlüsselte Protokolle	576
Sichere Mailserveranmeldung: SPA und SSL	576
<b>32 Skript- und Makro-Sicherheit</b>	<b>579</b>
Office-Makros sichern	580
Gefahren, die von Makros ausgehen	580
Makrosignaturen verwenden	581
Makroausführung einschränken	582
Vertrauenswürdige Signaturen definieren	584
MakroSignierungen im Unternehmen	585
Skript-Sicherheit	586
Der Versuch, Skripte zu deaktivieren	587
... und der zweifelhafte Erfolg	588
Welche Gefahren von Skripten ausgehen	590
Zwischen guten und bösen Skripten unterscheiden	590
TrustPolicy für Skripte festlegen	591
Codesigning-Zertifikat veröffentlichen	591
Skripte signieren	591

<b>33 Software-Einschränkungen</b>	<b>593</b>
Software-Einschränkung verstehen	593
Wie Softwareeinschränkungen funktionieren	594
Softwareeinschränkungen konfigurieren	596
Softwareeinschränkungen verwenden	597
Wichtige Grundeinstellungen	598
Pfadregeln einsetzen	600
Dateitypen verbieten	602
Mit Umgebungsvariablen arbeiten	602
Hash-Regel: Programme sicher identifizieren	603
Sicherheitsrisiken	603
Hash-Regel einsetzen	603
Zertifikatregeln verwenden	606
Skripte signieren	610
Softwareeinschränkungen kontrollieren	612
Gruppenrichtlinie anwenden	612
Ausführende Software aktualisieren	612
Ausnahmen von der Regel	612
Reihenfolge der Anwendung	613
Diagnosemöglichkeiten	613
<b>34 Windows</b>	<b>615</b>
Windows Update	615
Übertragene Informationen	616
Windows Update abschalten	616
Problembereichterstattung	617
Betriebssystemfehler	617
Anwendungssoftware	619
Problembereichterstattung abschalten	620
Remoteunterstützung und Remotedesktop	621
Remoteunterstützung und Remotedesktop abschalten	621
Windows Installer	622
Gefahren des Windows Installers	623
Media Player	623
Übertragene Daten ins Internet	624
Internetfunktionalität einschränken	624
Media Player deaktivieren	625
Systemwerkzeuge schützen	625
Systemprogramme sperren	627
Grafische Oberfläche einschränken	627
Elemente einschränken	627
Windows File Protection	628
Windows File Protection verstehen	629
Der DLLCACHE-Ordner	629
Windows File Protection konfigurieren	630

<b>TeilH</b>	
<b>Praxis Netzwerkverteidigung</b>	<b>633</b>
<b>35 Netzwerkaufbau</b>	<b>635</b>
Einführung Netzwerksicherheit	635
Die Firma	636
Die Umsetzung	636
Die Perimeterabsicherung	636
Die Webpräsenz	636
Die E-Mail-Lösung	638
Internetzugang	638
Die Absicherung der Forschungsabteilung	638
Remotebenutzer-Lösungen	639
Heimarbeitsplatz-Lösungen	639
Wireless LAN Anbindung	639
<b>36 IP-Hardening</b>	<b>641</b>
Microsoft Netzwerkdienste	642
Microsoft Netzwerk-Dienste abschalten	642
NetBIOS	643
WINS-Server	644
Weitere NetBIOS-Aufgaben	644
NetBIOS ersetzen	644
NetBIOS-Sicherheitsrisiken	645
NetBIOS deaktivieren	647
Null-Sessions	649
Null-Sessions einschränken	649
DNS Server-Absicherung	651
DNS Poisoning	651
Zone Transfers	651
DHCP-Server	653
Schutzmechanismen und Sicherheitslücken	653
Denial-of-Service Abwehr	654
SynAttackProtect	654
EnableDeadGWDetect	655
EnablePMTUDiscovery	655
KeepAliveTime	656
NoNameReleaseOnDemand	656
PerformRouterDiscovery	656
EnablelCMPRedirect	657
<b>37 Firewalls</b>	<b>659</b>
Wie eine Firewall funktioniert	660
Statische Paketfilter	660
Stateful Paketfilter (SPF)	662
Application Level Filterung	663
Übertragung von Datenpaketen	664

Host-basierte Firewalls	664
Routing-basierte Firewalls	665
Network Address Translation	665
NAT-Router als Firewall	667
Proxy Server	667
Positionierung einer Firewall	668
Bastion Host	668
Three-Homed Firewall	669
Back-to-Back Firewall	670
Regelkonfiguration	670
Elemente einer Firewall-Regel kennenlernen	671
Unternehmensrichtlinien umsetzen	672
Intrusion Detection Systeme (IDS)	674
Bestandteile eines Intrusion Detection Systems (IDS)	674
Die Datenanalyse	674
IDS-Reaktionen	675
Honeypots	675
Auswahl einer Firewall-Lösung	675
Microsoft Technologien	676
<b>38 VPN - Virtual Private Network</b>	<b>679</b>
Wozu virtuell und privat?	679
Point-to-Point VPN-Verbindung	680
Point-to-Multipoint VPN-Verbindung	680
Multipoint-to-Multipoint VPN-Verbindung	681
Die VPN-Protokolle	681
Point To Point Tunneling Protokoll (PPTP)	682
Layer 2 Tunneling Protokoll (L2TP)	682
Konfiguration des RAS Servers	682
Authentifizierungsprotokolle von RRAS	683
RAS Richtlinien	686
Probleme beim Betrieb von VPNs	688
Firewallkonfiguration für PPTP	688
Firewallkonfiguration für L2TP mit IPSec	688
<b>39 IPSec</b>	<b>691</b>
Angriffe auf TCP/IP-Protokollschwächen	691
Lauschangriff	692
Datenveränderungen (Man-in-the-Middle)	692
Spoofing	692
IPSec Grundlagen	692
Technische Voraussetzungen	692
Schutzmechanismen	693
Tunnel-Modus und Transport-Modus	693
Authentifizierungsmethoden	694
Kryptografische Algorithmen	694
Verbindungsaufnahme	695



IPSec Konfiguration .....	695
Wie IPSec-Regeln aufgebaut sind .....	695
Planungsphase .....	695
Praxislösungen .....	696
Einschränkungen .....	706
Performance-Bewertung .....	706
<b>40 Wireless LAN Security .....</b>	<b>707</b>
Angriffe aus der Luft .....	707
Wardriving und Warchalking .....	708
Authentifizierung .....	709
Open System Authentication .....	709
Shared Key Authentication .....	710
802.1x Authentifizierung .....	712
Verschlüsselung .....	715
Grundlagen zu WEP .....	715
Schwachstellen von WEP .....	716
Wie groß ist die Gefahr? .....	716
Hoffnung ist in Sicht .....	717
Deployment-Szenarien .....	718
Szenario 1 - Offenes WLAN mit VPN .....	718
Szenario 2 - Geschlossenes WLAN mit dynamic WEP, EAP und RADIUS .....	719
Werkzeuge .....	720
NetStumbler .....	720
MacStumbler .....	722
Airsnot .....	722
Airopeek .....	722
Sniffer Wireless .....	723
ISS Tool .....	724
Die Zukunft ist Wireless .....	725
Sichere Umgebungen .....	725
<b>41 Webserver-Sicherheit .....</b>	<b>727</b>
Installation .....	728
Betriebssystem-Installation .....	728
Webserver-Installation .....	728
Webserver-Konfiguration .....	729
Das IIS Lockdown Tool .....	729
Der URLScan-ISAPI-Filter .....	735
Benutzerauthentifizierung .....	737
Wie die Authentifizierung funktioniert .....	737
Verwaltungsmodelle .....	739
SSL-Verbindungen und Webserver-Zertifikate .....	740
<b>Stichwortverzeichnis .....</b>	<b>751</b>