

Inhaltsverzeichnis

1	Einleitung	11
2	Der Microsoft Internet Information Server 4.0	12
2.1	Installation des MS IIS 4.0	13
2.1.1	Lieferumfang und Installationsvoraussetzungen.....	13
2.1.2	Komponenten des Microsoft Windows NT Server 4.0 Option Pack ..	13
2.1.3	Installationsschritte	17
2.2	Administration des MS IIS 4.0	18
2.2.1	Windows NT-Administration	19
2.2.2	Internetdienst-Manager.....	19
3	Der Microsoft Internet Information Server 5.0	22
3.1	Installation des MS IIS 5.0	22
3.1.1	Lieferumfang und Installationsvoraussetzungen.....	22
3.1.2	Installationsschritte und Komponenten	23
3.2	Administration des IIS 5.0.....	25
4	Der Microsoft Site Server 3.0.....	26
4.1	Komponenten des Site Servers	26
4.2	Installation des Microsoft Site Servers 3.0.....	29
4.2.1	Installationsvoraussetzungen.....	30
4.2.2	Installationsschritte	31
4.3	Administration des Site Servers	34
4.3.1	Microsoft Management Console (MMC).....	34
4.3.2	HTML-Interface.....	36
4.3.3	Kommandozeile	36
4.4	Einsatzumgebungen des Site Servers	37
5	Einsatzumgebungen des MS IIS	44
5.1	Angriffsmethoden	44
5.1.1	ARP-Spoofing.....	44
5.1.2	IP-Spoofing	45
5.1.3	Route-Spoofing.....	45
5.1.4	DNS-Spoofing.....	45
5.1.5	Hijacking.....	46

5.1.6	Denial-of-Service-Attacken.....	46
5.1.7	Portscanning.....	47
5.2	Einsatz des IIS als WWW-Server im Internet	48
5.3	Einsatz des IIS als WWW-Server im Intranet	49
5.4	Verfügbarkeit und Performance	50
5.4.1	Cold-Standby-Lösung	51
5.4.2	Server-Farm	51
5.4.3	Round Robin	51
5.4.4	Lastverteilung durch Load-Balancer	51
5.4.5	Cluster	53
6	Gefährdungen und Schwachstellen des MS IIS	54
6.1	Gefährdungen.....	54
6.2	Angriffszenarien gegen Web- bzw. FTP-Server	56
6.3	Code Red.....	60
6.4	Aktuelle Schwachstellen und Bugs	62
7	Sicherheit	63
7.1	Erstellen einer Sicherheitsrichtlinie.....	63
7.2	Organisatorische und personelle Sicherheitsmaßnahmen.....	64
7.3	Integrierte Sicherheitsfunktionen des Betriebssystems.....	67
7.4	Absichern des Betriebssystems Windows NT/2000	67
7.4.1	Installation/Auswahl eines Servertyps	68
7.4.2	Deaktivieren nichtbenötigter Dienste.....	68
7.4.3	Konfigurieren der Netzwerkeinstellungen	70
7.4.4	Schützen der Registrierung.....	73
7.4.5	Benutzer und Gruppen.....	74
7.4.6	Sichern der Kennwörter	75
7.4.7	Verschlüsseln der SAM-Datei mit dem SYSKEY-Verfahren	76
7.4.8	Festlegen der Sicherheitsüberwachung (Logging).....	77
7.4.9	Abwehren von Denial-of-Service-Angriffen.....	79
7.5	Absichern von IIS 4.0 und IIS 5.0	82
7.5.1	Verzeichnissicherheit und Benutzerauthentisierung	82
7.5.2	Kontrolle des Zugriffs auf Dateien und Verzeichnisse	91

7.5.2.1 Zugriff über IP-Adressen oder Domännennamen einschränken	93
7.5.2.2 Zugriffsrechte auf virtuelle Web-Verzeichnisse	93
7.5.2.3 Datei und Verzeichnissicherheit (NTFS)	96
7.5.3 Prüfen von Verzeichnissen und Dateien	99
7.5.4 Absichern der HTML-Verwaltung	100
7.5.5 Anwendungszuordnung	100
7.5.6 Socket-Pooling	102
7.5.7 Sicherheitsassistenten des MS IIS 5.0	102
7.5.8 Protokollierung unter IIS	104
7.5.9 Weitere Konfigurationsempfehlungen	108
7.6 Absichern des Microsoft Site Servers	108
7.6.1 Benutzer und Gruppen	109
7.6.2 Absichern der HTML-Verwaltung (WebAdmin)	110
7.6.3 Prüfen von Verzeichnissen und Dateien	111
7.6.4 Benutzerauthentisierung	111
7.6.5 Datei und Verzeichnissicherheit (NTFS)	112
7.6.6 Datensicherung	113
7.6.7 Absicherung spezieller Site Server Komponenten	114
7.7 Überprüfung der Konfiguration mit Hilfe verfügbarer Tools	117
8 Weiterführende Links	119
9 Referenzliste	120

Tabellenverzeichnis

Tabelle 2.1: Features des IIS 4.0	13
Tabelle 4.1: Komponenten des Site Servers	33
Tabelle 4.2: Kommunikation der Site Server Komponenten	42
Tabelle 4.3: Zuordnung von Protokollen und Ports	42
Tabelle 4.4: Unverschlüsselte Kommunikation	43
Tabelle 5.1: Load-Balancer	53
Tabelle 7.1: Standardbenutzer Windows NT mit IIS 4.0	75
Tabelle 7.2: Einstellungen des Tcpip.sys	80
Tabelle 7.3: Zusammenfassung der Authentifizierungsmethoden	91

Tabelle 7.4: Zugriffsberechtigungen auf virtuelle Verzeichnisse	97
Tabelle 7.5: Zugriffsrechte auf Dateien	98
Tabelle 7.6: Zugriffsberechtigungen auf Systemdateien	98
Tabelle 7.7: Zugriffsberechtigungen auf Protokolldateien	98
Tabelle 7.8: Beispieldateien in IIS.....	99
Tabelle 7.9: Das W3C-erweiterte Protokollformat.....	107
Tabelle 7.10: Administratorengruppen des Site Servers	110
Tabelle 7.12: Site Server Daten	113
Tabelle 7.13: Zugriffsrechte für SiteAuthors und SiteEditors	114
Tabelle 7.14: TCP-Ports.....	117
Tabelle 7.15: Portscanner und Security-Tools	118

Abbildungsverzeichnis

Abbildung 2.1: Deaktivierung von Active Desktop.....	18
Abbildung 2.2: Microsoft Management Konsole	20
Abbildung 2.3: Internetdienst-Manager	21
Abbildung 3.1: IIS-Komponenten	24
Abbildung 3.2: Microsoft Management Console	25
Abbildung 4.1: Komponenten des Site Servers.....	32
Abbildung 4.2: Konfiguration der Komponenten	34
Abbildung 4.3: Snap In Auswahl.....	35
Abbildung 4.4: Webbasiertes Administrations-Interface	36
Abbildung 4.5: Netzwerkarchitektur	38
Abbildung 4.6: Entwicklungsumgebung Site Server	40
Abbildung 5.1: MS IIS im Internet	48
Abbildung 5.2: MS IIS im Intranet	49
Abbildung 5.3: MS IIS im Intranet mit VLANs	50
Abbildung 6.1: Buffer-Overflow für DoS-Angriff.....	54
Abbildung 6.2: Kontrollierter Buffer-Overflow	55
Abbildung 6.3: Manipulierter Stack	55
Abbildung 6.4: Beispiel zum Ändern des Passwortes.....	57
Abbildung 6.5: Benutzerkonto existiert nicht	57

Abbildung 6.6: Benutzerkonto existiert, Kennwort falsch.....	58
Abbildung 6.7: Anzeigen einer Datei mit showcode.asp	59
Abbildung 7.1: Sicherheitsrichtlinie	63
Abbildung 7.2: Angebotene Netzwerkdienste nach einer Windows NT- Installation	71
Abbildung 7.3: Setzen der TCP/IP-Filter	72
Abbildung 7.4: Deaktivieren des IP-Forwarding	73
Abbildung 7.5: SYSKEY	77
Abbildung 7.6: Festlegen der Protokollierung in den Überwachungsrichtlinien	78
Abbildung 7.7: Authentisierungsmethoden IIS 4.0	83
Abbildung 7.8: Authentisierungsmethoden	84
Abbildung 7.9: Anonymes Benutzerkonto	84
Abbildung 7.10: Erstellen und Verteilen von Schlüsseln	86
Abbildung 7.11: Schlüsselmanager	88
Abbildung 7.12: Sichere Kommunikation	89
Abbildung 7.13: Zugriffskontrolle IIS.....	92
Abbildung 7.14: Beschränken der IP-Adressen und Domänennamen	93
Abbildung 7.15: Sicherheitseinstellungen für virtuelle Verzeichnisse IIS 4.0..	94
Abbildung 7.16: Sicherheitseinstellungen für virtuelle Verzeichnisse IIS 5.0..	95
Abbildung 7.17: Anwendungsverknüpfungen.....	101
Abbildung 7.18: Eigenschaften der Anwendungsverknüpfungen	102
Abbildung 7.19: Zertifikats-Assistent	103
Abbildung 7.20: Berechtigungs-Assistent.....	104
Abbildung 7.21: Konfigurieren der Optionen für die Standard Web-Seite	105
Abbildung 7.22: Eigenschaften des W3C-erweitert Protokolls	106

Anhangsverzeichnis

Anhang:	Revisionskonzept IIS 5.0
---------	--------------------------