

Stefan Strobel

Firewalls für das Netz der Netze

Sicherheit im Internet: Einführung und Praxis



dpunkt.verlag

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlagen	9
2.1	TCP/IP und Adressen	9
2.1.1	Geschichtliches zu TCP/IP und zum Internet	9
2.1.2	Internet Standards und RFCs	10
2.1.3	Überblick	10
2.1.4	ARP	18
2.1.5	Routing	21
2.1.6	Fehlersuche	27
2.1.7	TCP und UDP	28
2.1.8	Sun RPCs	29
2.2	Die wichtigsten Dienste im Internet (technische Sicht)	31
2.2.1	DNS	31
2.2.2	Telnet	34
2.2.3	RSH, RCP und RLogin	36
2.2.4	Mail	37
2.2.5	FTP	41
2.2.6	TFTP	43
2.2.7	WWW	43
2.2.8	NFS und NIS	47
2.3	Verschlüsselungsverfahren	48
2.3.1	Symmetrische Verfahren	48
2.3.2	Asymmetrische Verschlüsselung	50
3	Angriffe auf Netze und Computer	53
3.1	Einbrechen in interne Rechnersysteme	53
3.2	Angriffe auf Verbindungen	54
3.2.1	Mitlesen	54
3.2.2	Manipulieren und Übernehmen	55
3.3	Denial-of-Service-Angriffe	56
3.4	Viren und Java	57
3.5	Angriffe aus dem lokalen Netz	58

4	Firewall-Grundlagen	61
4.1	Ziele, Konzepte, Einschränkungen	61
4.2	Mehrstufige oder einstufige Firewalls	63
4.3	Anwendungsbereiche	66
4.4	Integration, Wartung, Organisation	67
4.5	Firewalls und interne Server	69
4.6	Komponenten von Firewalls	69
4.6.1	IP-Filter	69
4.6.2	Dynamische Filter	72
4.6.3	TCP-/UDP-Relays	73
4.6.4	Application Gateways - Proxies	75
4.6.5	Verschlüsselungssysteme	78
4.6.6	Authentifizierungssysteme	80
4.6.7	Protokoll-Auswertung / Alarmsysteme	84
4.7	Standards und Empfehlungen zu Firewalls	88
5	Firewall-Tools und andere Produkte	91
5.1	Firewall-1	91
5.2	Firewall First	96
5.3	Ascend Secure Access Firewall	98
5.4	Digital AltaVista Firewall für NT	100
5.5	Firewall/Plus	102
5.6	TIS-FWTK und Gauntlet	104
5.7	Raptor Systems Eagle	104
5.8	Borderware	106
5.9	NetRoad Firewall	108
5.10	WWW-Proxies	108
5.11	Virens Scanner	108
5.11.1	MimeSweeper	109
5.11.2	InterScan WebProtect (TrendMicro)	109
5.11.3	McAfee WebShield	110
5.12	Hardware-Router als Filter	110
5.13	Linux-Kernel als Filter	111
5.14	Security-Scanner	113
5.14.1	Satan	113
5.14.2	ISS	115
5.15	Andere Überwachungstools	115
5.15.1	SessionWall	116
5.15.2	RealSecure	118
5.15.3	SSH	121
5.15.4	F-Secure VPN	122

6	Adreßumsetzung	123
6.1	IP-Adressen	123
6.1.1	Adreßumsetzung mit Proxies	124
6.1.2	Einfache NAT	125
6.1.3	ITG	129
6.2	Mailadressen	129
6.2.1	Sendmail	130
6.2.2	Netscape Mailserver und Varianten	132
7	Gesamtkonfigurationen	135
7.1	Mehrstufige Beispiele	135
7.2	Absichern eines Gateways	142
7.3	DNS	143
7.4	Mail	146
7.5	FTP ins Internet	148
7.6	WWW ins Internet	151
7.7	Telnet ins Internet	153
7.8	Eigene externe Server	153
7.8.1	WWW-Server	154
7.8.2	FTP-Server	155
7.9	Externe Logins	156
7.10	Intranet- und Dial-In-Firewalls	158
A	ICMP-Typen und Portnummern	163
A.1	ICMP-Typen	163
A.2	Codes für ICMP-Typ 3	165
A.3	Codes für ICMP-Typ 5	165
A.4	Codes für ICMP-Typ 11	166
A.5	Codes für ICMP-Typ 12	166
A.6	Portnummern	166
A.6.1	Privilegierte Ports	166
A.7	Reservierte Ports	172
B	Interessante Web- und FTP-Adressen	175
C	Bibliographie	179
Index	181