

Inhaltsverzeichnis

<i>Teil I: Sicherheit im Netz</i>	<i>1</i>
<i>1 Wozu braucht man Internet-Firewalls?</i>	<i>3</i>
Was wollen Sie schützen?	4
Wovor müssen Sie sich schützen?	7
Wie können Sie Ihr Firmennetz schützen?	15
Was ist ein Internet-Firewall?	19
<i>2 Internet-Dienste</i>	<i>29</i>
Elektronische Post	30
Übertragung von Dateien	32
Terminal-Zugang und ferne Ausführung von Kommandos	35
Usenet-News	36
World Wide Web	37
Andere Informationsdienste	40
Informationen über Netzbenutzer	41
Dienste für Echtzeitkonferenzen	43
Name-Service	44
Dienste zur Netzverwaltung	46
Zeitdienst	47
Netzweit verteilte Dateisysteme	48
Fenstersysteme	49
Druckdienste	50
<i>3 Sicherheitsstrategien</i>	<i>51</i>
Minimale Zugriffsrechte	51
Mehrschichtige Verteidigung	53
Die Passierstelle	54
Das schwächste Glied	55
Fehlersicherheit	56
Allumfassende Beteiligung	59

Vielfalt der Verteidigung	60
Einfachheit	61
<i>Teil II: Einrichten von Firewalls</i>	<i>63</i>
<i>4 Entwurf von Firewall-Systemen</i>	<i>65</i>
Einige Definitionen zu Firewalls	65
Proxy-Dienste	69
Architekturen für Firewalls	72
Varianten von Firewall-Architekturen	81
Interne Firewalls	93
<i>5 Bastion-Hosts</i>	<i>105</i>
Grundlagen	106
Besondere Arten von Bastion-Hosts	107
Auswahl des Rechners	108
Wahl eines geeigneten Standplatzes	114
Plazieren des Bastion-Hosts im Netz	114
Auswahl der Dienste auf dem Bastion-Host	115
Keine Benutzerkennungen auf dem Bastion-Host!	118
Einrichten eines Bastion-Hosts	119
Betrieb des Bastion-Hosts	145
Schutz der Maschine und Sicherungskopien	147
<i>6 Paketfilterung</i>	<i>151</i>
Wozu braucht man Paketfilterung?	152
Konfigurieren eines Routers zur Paketfilterung	157
Aufbau eines Pakets	159
Was macht der Router mit Paketen?	176
Aufstellen von Paketfilterregeln	180
Filterung nach Adressen	184
Filterung nach Diensten	187
Wahl eines Routers zur Paketfilterung	191
Wo plazierte man Paketfilter?	205
Beispiele für Paketfilterung	207

7	<i>Proxy-Systeme</i>	215
	Wozu braucht man Proxy-Dienste?	216
	Wie funktionieren Proxies?	220
	Verschiedene Arten von Proxy-Servern	223
	Proxies für Internet-Dienste	225
	Proxy-Dienste ohne Proxy-Server	227
	Proxy-Dienste mit SOCKS	228
	Proxy-Dienste mit dem Internet Firewall Toolkit von TIS	231
	Wenn Sie keinen Proxy einsetzen können	233
8	<i>Konfiguration von Internet-Diensten</i>	235
	Elektronische Post	238
	Übertragung von Dateien	252
	Terminal-Zugang (Telnet)	270
	Ferne Ausführung von Kommandos	273
	Network News Transfer Protocol (NNTP)	279
	World Wide Web (WWW) und HTTP	285
	Andere Informationsdienste	296
	Suchdienste	303
	Echtzeit-Konferenzsysteme	307
	Domain Name System (DNS)	316
	syslog	337
	Netzverwaltungsdienste	338
	Network Time Protocol (NTP)	348
	Network File System (NFS)	352
	Network Information Service/ Yellow Pages (NIS/YP)	355
	X Window System (X11)	357
	Druckprotokolle (lpr und lp)	361
	Analyse anderer Protokolle	364
9	<i>Zwei Beispiele für Firewalls</i>	365
	Architektur mit überwachtem Teilnetz	365
	Architektur mit überwachtem Host	387
10	<i>Authentifizierung und eingehende Dienste</i>	397
	Risiken beim Einsatz eingehender Dienste	399

Was versteht man unter Authentifizierung?	402
Verfahren zur Authentifizierung	407
Systeme zur Authentifizierung	413
Verschlüsselung auf Netzebene	419
Schlüsselverwaltung	423
Terminal-Server und Modem-Pools	424

Teil III:

Kontinuierlicher Schutz Ihres Standorts 427

11 Sicherheitspolitik 429

Ihre eigene Sicherheitspolitik	430
Aufstellen einer Sicherheitspolitik	437
Strategische und politische Entscheidungen	440

12 Betreuung von Firewalls 447

Allgemeine Wartungsarbeiten	447
Überwachung Ihres Systems	451
Wie Sie sich auf dem laufenden halten	460
Wie lange Sie für Weiterbildung brauchen	464
Wann sollten Sie Ihren Firewall austauschen?	464

13 Reagieren auf Zwischenfälle 467

Vorgehen bei einem Einbruchsversuch	467
Was nach einem Einbruch zu tun ist	476
Verfolgen und Festsetzen des Eindringlings	476
Planung der Vorgehensweise	479
Geeignete Vorkehrungen	489

Teil IV: Anhänge 497

A Ressourcen 499

World Wide Web	499
FTP-Server	500
Mailing-Listen	500

News-Gruppen	503
Organisationen	503
Konferenzen	506
Dokumente	508
Bücher	511
<i>B Werkzeuge</i>	<i>515</i>
Authentifizierungs-Werkzeuge	516
Analyse-Werkzeuge	517
Paketfilter	519
Proxy-Werkzeuge	520
Dämonen	521
Hilfsprogramme	522
<i>C Grundlagen von TCP/IP</i>	<i>525</i>
Einführung in TCP/IP	525
Ein Modell zur Datenkommunikation	527
Protokollarchitektur von TCP/IP	530
Netzzugangsschicht	532
Internet-Schicht	533
Transportschicht	539
Anwendungsschicht	545
Adressierung, Routing und Multiplexing	547
IP-Adressen	547
Routing im Internet	555
Routing-Tabellen	556
Protokolle, Ports und Sockets	560
<i>Stichwortverzeichnis</i>	<i>569</i>