

Inhalt

<i>Vorwort</i>	<i>xiii</i>
----------------------	-------------

<i>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
Wem können Sie vertrauen?	16
Wie können Sie Ihr Firmennetz schützen?	17
Was ist eine Internet-Firewall?	22
Weltanschauliche Fragen	29

<i>2: Internet-Dienste</i>	<i>35</i>
----------------------------------	-----------

Gesicherte Dienste und sichere Dienste	37
Das World Wide Web	37
Elektronische Post und News	42
Datenübertragung, File Sharing und Drucken	46
Fernzugriff	51
Echtzeit-Konferenzdienste	54
Namens- und Verzeichnisdienste	56
Authentifizierungs- und Auditingdienste	58
Administrative Dienste	58
Datenbanken	62
Spiele	62

3: Sicherheitsstrategien	63
Minimale Zugriffsrechte	63
Mehrschichtige Verteidigung	65
Passierstelle	66
Das schwächste Glied	67
Fehlersicherheit	68
Umfassende Beteiligung	71
Vielfalt der Verteidigung	72
Einfachheit	74
Sicherheit durch Verschleierung	75
II: Einrichten von Firewalls	79
4: Pakete und Protokolle	81
Wie sieht ein Paket aus?	81
IP	85
Protokolle oberhalb von IP	92
Protokolle unterhalb von IP	100
Protokolle der Anwendungsschicht	101
IP Version 6	101
Nicht-IP-Protokolle	103
Angriffe auf der Grundlage niederer Protokolle	103
5: Firewall-Techniken	109
Einige Definitionen zu Firewalls	109
Paketfilterung	112
Proxy-Dienste	117
Network Address Translation	122
Virtuelle Private Netzwerke	126
6: Firewall-Architekturen	131
Single-Box-Architekturen	131
Architekturen mit überwachten Hosts	136
Architekturen mit überwachtem Teilnetz	138
Architekturen mit mehreren überwachten Teilnetzen	143
Variationen von Firewall-Architekturen	147
Terminal-Server und Modem-Pools	157
Interne Firewalls	159

7: Der Firewall-Entwurf	167
Definieren Sie Ihre Bedürfnisse	167
Bewerten Sie die verfügbaren Produkte	170
Setzen Sie alles zusammen	172
8: Paketfilterung	175
Wozu braucht man Paketfilterung?	176
Konfigurieren eines Routers zur Paketfilterung	182
Was macht der Router mit Paketen?	185
Tips und Tricks zur Paketfilterung	189
Konventionen für Paketfilterregeln	191
Filterung nach Adressen	194
Filterung nach Diensten	196
Wahl eines Routers zur Paketfilterung	200
Paketfilter als Software-Implementierung für normale Computer	214
Wo platziert man einen Paketfilter?	225
Welche Regeln sollten Sie verwenden?	227
Beispiele für Paketfilterung	228
9: Proxy-Systeme	235
Wozu braucht man Proxy-Dienste?	236
Wie funktionieren Proxies?	237
Verschiedene Arten von Proxy-Servern	242
Proxy-Dienste ohne Proxy-Server	243
Proxy-Dienste mit SOCKS	244
Proxy-Dienste mit dem Internet Firewall Toolkit von TIS	248
Einsatz des Microsoft-Proxy-Servers	250
Wenn Sie keinen Proxy einsetzen können	251
10: Bastion-Hosts	253
Grundlagen	254
Besondere Arten von Bastion-Hosts	255
Auswahl des Rechners	256
Wahl eines geeigneten Standorts	261
Plazieren von Bastion-Hosts im Netz	261
Auswahl der Dienste auf einem Bastion-Host	263
Deaktivieren der Benutzerzugänge auf Bastion-Hosts	266

Einrichten eines Bastion-Hosts	268
Absichern des Rechners	269
Deaktivieren überflüssiger Dienste	272
Betrieb des Bastion-Hosts	282
Schutz der Maschine und Anlegen von Sicherungskopien	284
11: Unix- und Linux-Bastion-Hosts	287
Welche Version von Unix?	287
Unix absichern	289
Nicht benötigte Dienste deaktivieren	292
Installieren und Anpassen von Diensten	303
Neukonfiguration für den Dauerbetrieb	306
Eine Sicherheitsüberprüfung durchführen	310
12: Windows NT und Windows 2000-Bastion-Hosts	313
Ansätze zum Erstellen von Windows NT-Bastion-Hosts	313
Welche Version von Windows NT?	314
Windows NT absichern	315
Nicht benötigte Dienste deaktivieren	317
Installieren und Anpassen von Diensten	330
III: Internet-Dienste	333
13: Internet-Dienste und Firewalls	335
Angriffe auf Internet-Dienste	337
Die Risiken eines Dienstes bewerten	346
Andere Protokolle analysieren	353
Was zeichnet einen guten Dienst in einer Firewall aus?	356
Sicherheitskritische Programme auswählen	359
Unsichere Konfigurationen kontrollieren	367
14: Vermittelnde Protokolle	369
Remote Procedure Call (RPC)	369
Distributed Component Object Model (DCOM)	378
NetBIOS über TCP/IP (NetBT)	379
Common Internet File System (CIFS) und Server Message Block (SMB)	382
Common Object Request Broker Architecture (CORBA) und Internet Inter-Orb Protocol (IIOP)	386

ToolTalk	388
Transport Layer Security (TLS) und Secure Socket Layer (SSL)	389
Das Generic Security Services API (GSSAPI)	393
IPsec	394
Remote Access Service (RAS)	398
Point-to-Point Tunneling Protocol (PPTP)	399
Layer 2 Transport Protocol (L2TP)	402
 15: Das World Wide Web	405
HTTP-Server-Sicherheit	406
HTTP-Client-Sicherheit	411
HTTP	419
Mobiler Code und mit dem Web zusammenhängende Sprachen	427
Cache-Kommunikationsprotokolle	434
Push-Techniken	437
RealAudio und RealVideo	439
Gopher und WAIS	441
 16: Elektronische Post und News	445
Elektronische Post	445
Simple Mail Transfer Protocol (SMTP)	452
Andere Mail-Übertragungsprotokolle	464
Microsoft Exchange	464
Lotus Notes und Domino	466
Post Office Protocol (POP)	468
Internet Message Access Protocol (IMAP)	471
Microsoft Messaging API (MAPI)	473
Network News Transfer Protocol (NNTP)	473
 17: Datetübertragung, Filesharing und Drucken	477
File Transfer Protocol (FTP)	478
Trivial File Transfer Protocol (TFTP)	492
Network File System (NFS)	493
Filesharing für Microsoft-Netzwerke	504
Druckprotokolle	507
Verwandte Protokolle	511

18: Der Fernzugriff auf Hosts	513
Terminal-Zugang (Telnet)	514
Entfernte Ausführung von Befehlen	517
Entfernte Grafikschnittstellen	533
19: Echtzeit-Konferenzdienste	547
Internet Relay Chat (IRC)	547
ICQ	550
talk	552
Multimedia-Protokolle	555
NetMeeting	561
Multicast und das Multicast Backbone (MBONE)	563
20: Namens- und Verzeichnisdienste	567
Das Domain Name System (DNS)	567
Network Information Service (NIS)	592
NetBIOS für TCP/IP-Namensdienste und den Windows Internet Name Service	594
Der Windows-Browser	606
Lightweight Directory Access Protocol (LDAP)	613
Active Directory	615
Suchdienste	616
21: Authentifizierungs- und Auditing-Dienste	621
Was ist Authentifizierung?	622
Paßwörter	627
Verfahren zur Authentifizierung	630
Modulare Authentifizierung für Unix	635
Kerberos	640
NTLM-Domänen	646
Remote Authentication Dial-in User Service (RADIUS)	654
TACACS und Konsorten	656
Auth und identd	658
22: Administrative Dienste	661
Systemverwaltungsprotokolle	661
Routing-Protokolle	668

Protokolle zum Booten und für die Konfiguration beim Booten	675
ICMP und Netzwerk-Diagnose	678
Network Time Protocol (NTP)	685
Dateisynchronisation	689
Überwiegend harmlose Protokolle	692
23: Datenbanken und Spiele	695
Datenbanken	695
Spiele	710
24: Zwei Beispiel-Firewalls	713
Architektur mit überwachtem Teilnetz	713
Zusammengelegte Router und Bastion-Host mit allgemein verwendbarer Hardware	737
IV: Kontinuierlicher Schutz Ihres Standorts	755
25: Sicherheitspolitik	757
Ihre eigene Sicherheitspolitik	758
Aufstellen einer Sicherheitspolitik	765
Strategische und politische Entscheidungen	768
Was passiert, wenn Sie keine Sicherheitspolitik durchsetzen können?	774
26: Betreuung von Firewalls	777
Allgemeine Wartungsarbeiten	777
Überwachung des Systems	782
Wie Sie sich auf dem laufenden halten	794
Wieviel Zeit kostet die Weiterbildung?	797
Wann sollten Sie Ihre Firewall austauschen?	798
27: Reagieren auf Zwischenfälle	799
Vorgehen bei einem Einbruchversuch	799
Was nach einem Einbruch zu tun ist	809
Verfolgen und Festsetzen des Eindringlings	809
Planung Ihrer Vorgehensweise	812
Geeignete Vorkehrungen	822

<i>V: Anhänge</i>	829
<i>A: Ressourcen</i>	831
<i>B: Werkzeuge</i>	847
<i>C: Kryptographie</i>	857
<i>Index</i>	885