

2. AUFLAGE

Linux Server-Sicherheit

Michael D. Bauer

*Deutsche Übersetzung von
Andreas Heck, Peter Klicman & Torsten Wilhelm*

O'REILLY®

Beijing · Cambridge · Farnham · Köln · Paris · Sebastopol · Taipei · Tokyo

Vorwort	XI
1 Gefahrenanalyse und Risiko-Management	1
Risikokomponenten	2
Einfache Risikoanalyse: Die jährliche Verlusterwartung	13
Eine Alternative: Angriffsbaum-Modelle	18
Verteidigungsmöglichkeiten	21
Fazit	23
Quellen	23
2 Planung von Perimeter-Netzwerken	24
Etwas Terminologie	25
Verschiedene Arten von Firewall- und DMZ-Architekturen	28
Entscheiden, was in die DMZ gehört	33
Zuteilung von Ressourcen in der DMZ	34
Die Firewall	36
3 Linux härten und iptables verwenden	49
Prinzipien der Betriebssystem-Härtung	50
Automatische Härtung mit Bastille Linux	126
4 Sichere Remote-Administration	132
Warum es an der Zeit ist, Klartext-Administrations-Tools in den Ruhestand zu schicken	132
Hintergrund und Grundlagen von Secure Shell	133
SSH für Fortgeschrittene	145

5	Tunnel graben	162
	Stunnel und OpenSSL: Konzepte	162
6	Domain Name Services (DNS) absichern	191
	DNS-Grundlagen	192
	DNS-Sicherheitsrichtlinien	194
	Auswahl einer DNS-Software	195
	Absicherung von BIND	197
	djbdns	221
	Ressourcen	242
7	Authentifizierung mit LDAP	245
	LDAP-Grundlagen	246
	Aufsetzen des Servers	251
	Verwaltung der LDAP-Datenbank	261
	Schlussfolgerungen	269
	Ressourcen	269
8	Datenbank-Sicherheit	270
	Arten von Sicherheitsproblemen	271
	Server-Platzierung	271
	Installation der MySQL-Software	275
	Datenbank-Betrieb	281
	Ressourcen	286
9	Absichern von E-Mail-Diensten	287
	Hintergrund: MTA- und SMTP-Sicherheit	288
	Die Verwendung von SMTP-Kommandos, um Mängel an SMTP-Servern aufzudecken	292
	Absichern Ihres MTAs	293
	Sendmail	294
	Postfix	323
	Mail Delivery Agents	332
	Eine kurze Einführung in die E-Mail-Verschlüsselung	346
	Ressourcen	351
10	Absichern von Webservern	353
	Websicherheit	353
	Der Webserver	355

Web-Content	368
Web-Anwendungen	379
Verteidigungslinien	403
Ressourcen	403
11 Absichern von Dateidiensten	404
Sicherheit von FTP	404
Andere Methoden des File-Sharing	438
Ressourcen	451
12 Systemprotokolle und -überwachung	452
syslog	452
Syslog-ng	463
Testen der Protokollmechanismen mit logger	482
System-Logdateien mit logrotate verwalten	483
Der Einsatz von Swatch für automatisches Log-Monitoring	487
Einige einfache Tools für Log-Reports	496
Ressourcen	496
13 Techniken zur Intrusion Detection	497
Prinzipien von Intrusion Detection-Systemen	498
Der Einsatz von Tripwire	501
Andere Integritätsprüfer	518
Snort	520
Ressourcen	535
A Zwei vollständige Iptables-Startskripte	537
Index	549