Torwächter für WLANs

Es spielt keine Rolle, ob unternehmenseigener Access-Point oder öffentlicher Wireless-LAN-Hotspot: Der Zugang muss stets kontrolliert werden. Ein starkes Team aus Linux, FreeRADIUS und pfsense erledigt diese Aufgabe flexibel und zuverlässig.

ACHIM WAGENKNECHT

Authentifizierung, Autorisierung, Accounting, kurz Triple-A, das sind die drei Kernfunktionen bei der Zugangskontrolle zu Netzwerken. Das war schon zu Modem-Zeiten so und ist heute bei drahtlosen Hotspots nicht anders. Geht es nur um wenige Benutzer, so kann der Zugang von einer einzelnen Netzwerk-Komponente kontrolliert werden. Wie das mit der Firewall-Distribution pfsense im WLAN funktioniert, können Sie in Linux Professionell 06/2006 ab Seite 79 nachlesen. Wer aber viele Benutzer erwartet oder gar einen öffentlichen Hotspot betreibt, wird schnell an die Grenzen der eingebauten Benutzerverwaltung von pfsense stoßen.

Mehr Leistung

Um diese Grenzen zu sprengen, bietet sich ein RADIUS-Server an. Das Netzwerkprotokoll RADIUS verwaltet zentral alle Netzwerk-Zugänge über Modem, DSL, VPN oder WLAN. Es gibt mehrere freie Implementierungen dieses Protokolls, die führende ist FreeRADIUS *(www.freeradius.org)*.

Wer einen Hotspot auf der Basis von pfsense mit lokaler Benutzerverwaltung betreibt, hat mehrere Dienste auf einem Rechner, die in einer typischen RADIUS-Installation getrennt werden: 1. Log-in, 2. Authentifizierung und 3. Benutzerkonten.

Es mag auf den ersten Blick befremden, warum diese drei Bereiche getrennt werden sollten, da sie doch eng verzahnt sind. Und wie werden sie überhaupt getrennt? Das Warum ist schnell beantwortet: Wenn der Zugangskontrollrechner unter Last in die Knie geht, liegt es nahe, seine Arbeit auf mehrere PCs zu verteilen. Und wenn unterschiedliche Zugangsarten verwaltet werden sollen, ist eine modulare Lösung viel flexibler.

Drei Wächter

In einer typischen RADIUS-Installation teilen sich drei Torwächter die Arbeit. Der erste nimmt die ankommenden Verbindungen entgegen. Er präsentiert den Benutzern Eingabefelder für Benutzername und Passwort. Diese Rolle übernimmt hier pfsense. Die Anmeldedaten des Benutzers reicht pfsense an den zweiten Torwächter weiter, der sie überprüft. Das ist die Aufgabe des RADIUS-Servers. Der wiederum fragt bei einer dritten Instanz die Benutzernamen, Passwörter und Berechtigungen ab. Da es meist darum geht, eine große Zahl von Benutzern performant zu verwalten, erledigt diesen Teil der Arbeit ein Datenbankserver.

RADIUS als zentrale Komponente in diesem Aufbau ist sehr flexibel. Ein RADIUS-Server kann mehrere Zugangs-Server versorgen. Diese werden hier auch NAS genannt, Network Access Server. NAS steht in anderen Zusammenhängen verwirrenderweise auch für Network Attached Storage. Die Zugangs-Server brauchen noch nicht einmal alle von der gleichen Art zu sein. Es bietet sich daher an, einen FreeRADIUS-Server als zentralen Zugangskontrolleur in einem besonders gesicherten Bereich aufzustellen.

RADIUS auf der Firewall

FreeRADIUS ist nach Auskunft seiner Entwickler sogar noch flexibler als andere RADIUS-Implementationen. Das soll hier nicht überprüft werden. Im Folgenden wird vor allem das Zusammenspiel zwischen pfsense und FreeRADIUS beschrieben. Es gibt sogar ein Paket für pfsense, mit dem FreeRADIUS direkt auf der Firewall installiert werden kann: *http://cvstrac.pfsense.com/dirview?d=tools/packages*. Im Normalfall ist das aber keine gute Idee. Der Leistungsvorteil, den die modulare RADIUS-Installation bietet, wird wieder aufgegeben. Und auf einer Firewall-Maschine soll nach der reinen Lehre eigentlich nur die Firewall laufen und sonst nichts. pfsense weicht von diesem Dogma schon recht weit ab, und jedes zusätzliche Paket schwächt die Sicherheit weiter.

Empfohlene Installation

FreeRADIUS wird also auf einem zusätzlichen Linux-Rechner installiert. Viele Distributionen bringen schon fertige Pakete zur Installation mit, unter anderem das im Test verwendete Suse Linux 10. Ansonsten stehen die Quellpakete zum Kompilieren auf der Homepage des Projektes bereit. Für Testzwecke kann FreeRADIUS auf einem beliebigen Linux-Rechner installiert werden, auch der Arbeitsrechner des Admins ist geeignet. Anders sieht es aus, wenn der RADIUS-Server produktiv eingesetzt werden soll. Dann sollte diese sicherheitskritische Komponente in einem verschlossenen Raum auf robuster Hardware und einer gehärteten Linux-Installation eingerichtet werden.

Im Test installierte das FreeRADIUS-Paket seine Programmdatei auf zwei Rechnern in unterschiedliche Ordner: einmal in */usr/local/sbin/* und einmal in */usr/sbin/*. Die Konfiguration landete aber immer in */etc/raddb/*. Auch wenn die Konfiguration eines RADIUS-Servers in vielen Szenarios ziemlich kompliziert werden kann, sollte eine einfache, aber funktionierende Testinstallation in weniger als einer Stunde fertig sein.

Der zentrale Dämon des RADIUS-Servers heißt *radiusd*. Damit der Server startet, muss er Zugriff auf seine Konfigurationsdateien haben. Dazu sollten diese dem gleichen Benutzer gehören, der auch in der Konfigurationsdatei des Dämons unter */etc/raddb/radiusd.conf* angegeben ist. Dort finden sich ungefähr bei Zeile 110 Benutzer und Gruppe des Dämons. Was hier einzutragen ist, hängt auch von der Art der gewünschten Authentifizierung ab. Vorgegeben ist der Wert *radiusd* sowohl als Benutzer als auch als Gruppe. Damit kann RADIUS unter anderem seine eigene *users*-Datei zur Authentifizierung verwenden, aber auch LDAP, SQL und andere Benutzerverzeichnisse. Für einen ersten Test sind diese aber zu kompliziert.

Benutzerdaten

Einfacher ist es, wenn RADIUS auf die systemeigenen Benutzerdaten zugreift. Damit das funktioniert, sollte die Gruppe, unter der der Dämon läuft, auf *shadow* geändert werden. Bisweilen wird auch empfohlen, *radiusd* als *root* laufen zu lassen, aber das kann aus Sicherheitsgründen nur eine vorübergehende Notlösung sein. Im Abschnitt *unix* um Zeile 640 ist verzeichnet, wo die Benutzerkonten zu finden sind:

```
passwd = /etc/passwd
shadow = /etc/shadow
group = /etc/group
```

Überprüfen Sie, ob diese Einträge mit den tatsächlichen Gegebenheiten auf Ihrem Computer übereinstimmen.

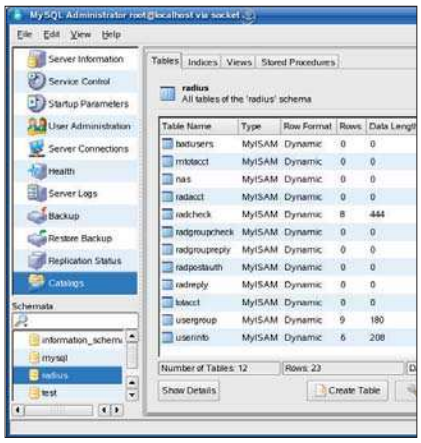
In der aktuellen Version entnimmt FreeRADIUS alle Informationen nur noch einer einzigen Datei namens */etc/raddb/clients.conf*. Für pfsense kann ein Eintrag in dieser Datei wie folgt aussehen. Der Schlüssel oder das »secret« darf bis zu 31 Zeichen lang sein:

```
client 192.168.0.15 {
  secret = testschluessel987
  nastype = other }
```

Damit ist die Konfiguration von FreeRADIUS für einen ersten einfachen Test schon abgeschlossen. Damit daraus eine Zugangslösung wird, muss jetzt noch der Zugangs-Server präpariert werden, also in diesem Fall pfsense. Auf einem PC mit Wireless-Karte können Sie pfsense als Access-Point mit Captive Portal konfigurieren. Wie das im Einzelnen geht, steht in Linux Professionell Ausgabe 06/2006 ab Seite 79. Hier eine kurze Zusammenfassung: Zunächst muss die WLAN-Karte einem Interface zugewiesen und aktiviert werden. Die Firewall-Regeln müssen den Zugang vom WLAN ins Internet erlauben. Dann kann das Captive Portal unter *Services* aktiviert werden. Wer jetzt versucht, über diesen Rechner drahtlos ins Internet zu kommen, bekommt eine Log-in-Seite zu sehen. Übrigens kann das Captive Portal auch für herkömmliche Ethernet-Schnittstellen aktiviert werden.

Captive Portal

Für einen ersten Test brauchen Sie auf der umfangreichen Einstellungsseite des Captive Portals nur drei Dinge zu konfigurieren: Kreuzen Sie unter *Authentication* die Option *RADIUS* an. Tragen Sie die IP Ihres RADIUS-Servers ein. Schreiben Sie den Schlüssel in das Feld *shared secret*. Noch ein Klick



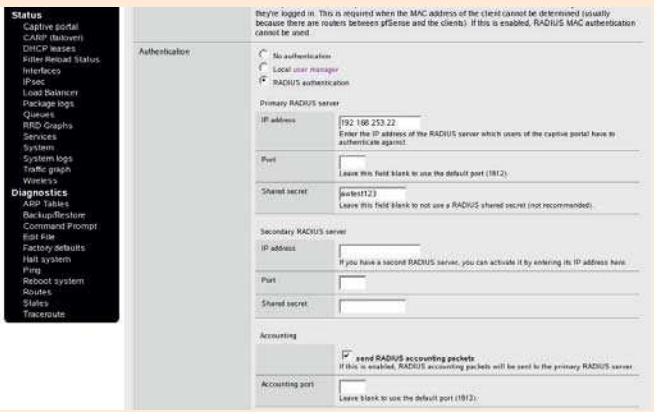
Die Benutzerverwaltung für den Hotspot liegt in dieser MySQL-Datenbank

ganz unten auf der Seite auf die Schaltfläche *Save* und wenige Sekunden später sollte das Captive Portal funktionieren. Starten Sie jetzt FreeRADIUS mit dem Befehl *radiusd -xyz*. Diese Optionen sorgen dafür, dass Systemmeldungen des Dämons ausgegeben und alle Log-in-Versuche protokolliert werden. Stellen Sie dann mit einem drahtlosen Gerät eine Verbindung zu pfsense her und versuchen Sie, irgendeine Internetseite aufzurufen. Es erscheint stattdessen die Log-in-Seite von pfsense. Hier geben Sie einen Benutzernamen und ein Passwort an, mit denen Sie sich auch auf der Linux-Installation Ihres RADIUS-Servers anmelden können. Sie sollten zur gewünschten Seite weitergeleitet werden. Geben Sie falsche Zugangsdaten an, erscheint nur eine Fehlermeldung.

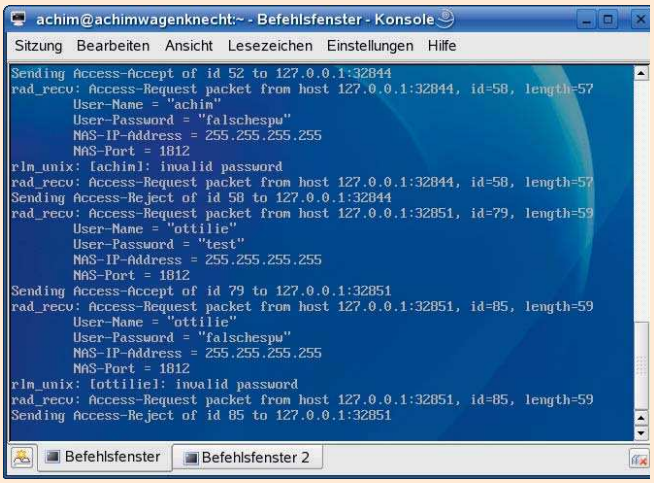
Erster Funktionstest

Leider ist die Fehlermeldung von pfsense sehr knapp. Egal welcher Fehler vorliegt, das Captive Portal meldet immer nur lakonisch: *Authentication error*. Das ist verständlich, denn wäre das Portal an dieser Stelle geschwätzig, böte es potenziellen Angreifern

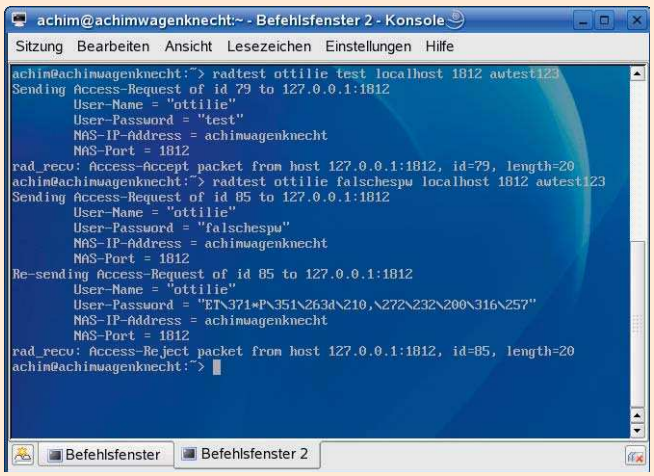
Mit pfsense wird aus einem PC eine Firewall mit WLAN-Access-Point. Den Zugang regelt das Captive Portal



Drei einfache Einstellungen reichen, damit pfsense mit dem FreeRADIUS-Authentifizierungsserver zusammenarbeitet



Torwächter in Aktion: In den Meldungen von radiusd ist zu sehen, wie FreeRADIUS Benutzer einlässt oder abweist



Wächterprüfung: Mit dem Befehl »radtest« können Sie ausprobieren, ob FreeRADIUS funktioniert

möglicherweise Munition. Falls der Log-in nicht auf Anhieb funktioniert, können Sie mögliche Fehlerursachen in den Ausgaben des radiusd finden. Bleiben die Gründe immer noch im Dunkeln, können Sie die Auskunftsfreude des Dämons noch erhöhen, indem Sie in den Optionen ein großes X statt eines kleinen angeben.

Eine weitere Quelle von Debug-Informationen ist das Windows-Programm NTRadPing *(www.dialways.com)*. Um Ihren RADIUS-Server damit zu testen, tragen Sie einen Windows-Rechner in der Datei *clients.conf* als Zugangsrechner ein. Der nastype ist wie bei pfsense *other*. Den Schlüssel können Sie wieder frei wählen, und die IP ist natürlich die des Client. Den gleichen Test können Sie auch unter Linux durchführen, aber hier nur von der Kommandozeile mit dem Befehl:

```
radtest username password
   servername port secret
```

Troubleshooting

Wenn die Authentifizierung misslingt, kommen verschiedene Ursachen infrage. FreeRADIUS benutzt standardmäßig den Port *1812*, pfsense ebenfalls. Sie können diese Einstellungen auch ändern, solange sie übereinstimmen. Wenn Sie einen anderen Zugangs-Server benutzen, ist der vielleicht auf den alten Port *1645* eingestellt. Der Port muss auf allen beteiligten Firewalls freigegeben sein. In der Konsole gibt *radiusd* die Passwörter von Log-in-Versuchen im Klartext aus. Kommt hier nur Kauderwelsch an, ist das ein Zeichen dafür, dass die Schlüssel auf pfsense und RADIUS nicht übereinstimmen.

Benutzerseiten

Typischerweise bekommt der Benutzer bei der Zugangskontrolle drei Seiten zu sehen: 1. Die Log-in-Seite, 2. eine Fehlerseite, wenn der Log-in scheitert, und 3. eine Begrüßungsseite nach erfolgreichem Log-in.

Diese Seiten lassen sich trefflich für Benutzerinformationen einsetzen. Insbesondere sollte hier stehen, dass der Hotspot nicht für illegale Downloads benutzt werden darf. Denn wer einen WLAN-Zugang ohne irgendwelche Einschränkungen freigibt, kann unter Umständen für Urheberrechtsverletzungen, die seine Nutzer begehen, haftbar gemacht werden. Alle drei Seiten lassen sich in pfsense anlegen. Log-in- und Fehlerseite werden auf der pfsense-Maschine selbst gespeichert, für die Begrüßungsseite wird auf der Einstellungsseite des Captive Portals unter *Redirection URL* eine Umleitung hinterlegt.

Die Log-in- und die Fehler-Seite können Sie unten im Captive Portal auf die Firewall hochladen. Falls diese Seiten Grafiken enthalten, müssen die Namen der Grafikdateien mit *captiveportal-* anfangen. Oben rechts auf der Seite gibt es den *File Manager*, dort können Sie Grafiken hochladen. Hier lassen sich auch PHP-Scripts hinterlegen.

Aber seien Sie sparsam, denn es stehen für diese Dateien insgesamt nicht mehr als 256 KByte zur Verfügung. In die HTML-Seite werden die Grafiken mit relativen Links eingebunden, sie befinden sich im gleichen Ordner wie die HTML-Datei.

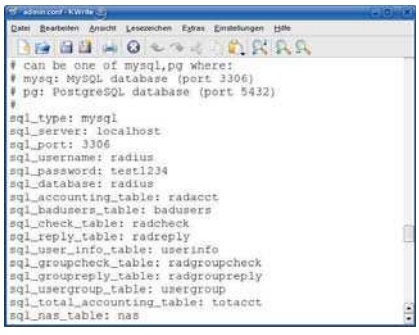
Benutzerverwaltung

Um einen öffentlichen Hotspot sinnvoll betreiben zu können, brauchen Sie eine flexible und leicht zu bedienende Benutzerverwaltung. Es bietet sich an, die Benutzerdaten in einer MySQL-Datenbank abzulegen und das Ganze mit einer Web-Oberfläche mit PHP zu verwalten. Genau diese Lösung ist im FreeRADIUS-Paket auch enthalten. Die Web-Oberfläche heißt *Dialup Admin*. Doch damit die funktioniert, müssen zunächst die Datenbanktabellen in MySQL angelegt werden.

Im Ordner */usr/share/doc/packages/freeradius/* findet sich ein SQL-Script namens *db_mysql.sql*. Dieses Script können Sie von der Kommandozeile in MySQL ausführen oder seinen Inhalt per Cut and paste in phpMyAdmin einfügen und dort ausführen lassen. Es erzeugt die nötige Datenbankstruktur für FreeRADIUS und Dialup Admin.

Dialup-Admin

Kopieren Sie den Inhalt des Ordners *dialup_admin* aus dem TAR-Paket von FreeRADIUS nach */usr/local/dialupadmin/*. Das Paket enthält ein Unterverzeichnis *htdocs*, das die eigentliche Web-Oberfläche enthält. Verknüpfen Sie dieses mit dem Wurzelverzeichnis Ihres Webservers und setzen Sie die pas-



Bis der Hotspot läuft, müssen einige Konfigurationsdateien editiert werden

senden Rechte, damit Ihr Webserver darauf zugreifen kann. Dialup Admin speichert seine Konfigurationsdateien in dem Verzeichnis, in dem auch das Programm selbst installiert ist, im Unterordner *conf*. Die wichtigste Datei dort heißt *admin.conf*. Wenn Sie Dialup Admin in einem anderen Verzeichnis installiert haben, ändern Sie die entsprechende Variable *general_base_dir* vom voreingestellten Wert */usr/local/dialup_admin* auf den richtigen Ordner. Etwa ab Zeile 220 werden in der Datei *admin.conf* die Zugangsdaten zur MySQL-Datenbank eingetragen:

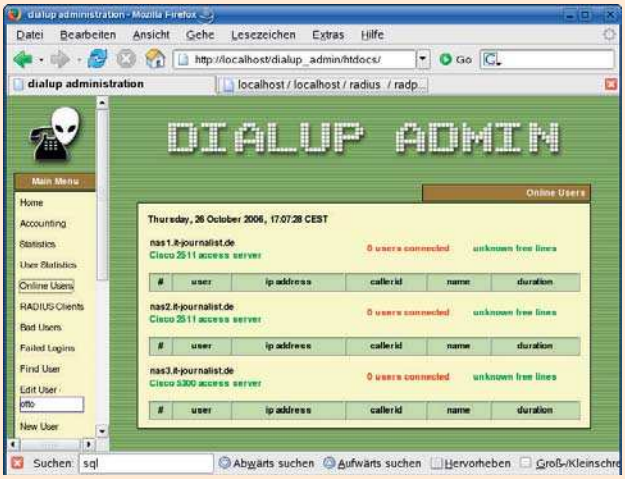
```
sql_type: mysql
sql_server: localhost
sql_port: 3306
sql_username: radius
sql_password: test123
sql_database: radius
```

Das Passwort sollten Sie ändern, die Serveradresse und den Benutzernamen je nach Gegebenheiten. Port, Datenbankname und Tabellenbezeichnungen sollten bleiben.

Um den Aufbau testen zu können, müssen jetzt Benutzer in die SQL-Datenbank. Rufen Sie Dialup Admin im Browser auf. Die Web-Oberfläche sollte unter *http:///localhost/dialupadmin/* erreichbar sein. Klicken Sie links unten auf *New Group* und legen Sie eine Gruppe an. Dabei brauchen Sie nur den Namen der Gruppe einzutragen, alle anderen Felder können frei bleiben. Als Nächstes legen Sie einen Benutzer an. Auch hier können die meisten Felder frei bleiben, nur *Username* und *Password* sind Pflicht.

In der Web-Oberfläche Dialup Admin genügt es, zunächst nur eine Gruppe und einen Benutzer anzulegen. Dabei können die meisten Felder frei bleiben

Mit Dialup Admin haben Sie die Online-Aktivitäten Ihrer Benutzer immer im Blick



SQL-Anmeldung

Damit FreeRADIUS die Benutzerinformationen in der MySQL-Datenbank auch nutzt, muss zunächst die Verbindung zur Datenbank in der Konfigurationsdatei */etc/raddb/sql.conf* eingestellt werden. Als Nächstes suchen Sie in der Datei */etc/raddb/radiusd.conf* den Abschnitt *authorize{}* gegen Ende der Datei. Tragen Sie dort eine Zeile ein, die nur die Zeichenfolge *sql* enthält, und zwar am besten genau vor dem Eintrag *files*. Schließlich brauchen Sie noch einen Standardbenutzer, für den als Anmeldemethode die SQL-Datenbank benutzt wird. Das erreichen Sie, indem Sie in die Datei */etc/raddb/users* folgende Zeile einfügen:

```
DEFAULT Auth-Type = SQL
```

Bereit zur Inbetriebnahme

Damit sollte Ihr Hotspot fertig sein. Beim Log-in mit einem drahtlosen Gerät werden nur noch die Benutzer akzeptiert, die in der SQL-Datenbank eingetragen sind. Das System besteht jetzt aus insgesamt vier Komponenten: pfsense mit dem Captive Portal, FreeRADIUS, MySQL und Dialup Admin. Dadurch dass die Benutzerdatenbank in MySQL vorliegt und mit PHP-Scripts per Web administriert wird, sind auch individuelle und komfortable Sonderlösungen möglich.

In jeder dieser Komponenten finden sich noch eine Vielzahl von Einstellungen, die in diesem Schnelldurchgang zu kurz gekommen sind. Vor allem die *Accounting*-Lösung für die Abrechnung ist bei öffentlichen Hotspots interessant. In pfsense wird das Accounting einfach per Mausklick eingeschaltet: Sie brauchen nur im Captive Portal die Option *send RADIUS accounting packets* anzukreuzen. Im Datenbankschema und in Dialup Admin sind die Accounting-Tabellen für die Abrechnung ebenfalls schon vorgesehen.

Ein anderer Aspekt ist die Sicherheit. Die hier beschriebene Lösung arbeitet völlig unabhängig von der eingesetzten WLAN-Verschlüsselung. Der Hotspot kann sogar ohne Verschlüsselung benutzt werden. Um ihr WLAN besser abzusichern, können Sie WPA-Verschlüsselung mit Zertifikaten verwenden. Wie das funktioniert, können Sie in Linux Professionell 01/2006 ab Seite 66 nachlesen. Zudem können die Clients gezwungen werden, die Authentifizierung jede Minute zu wiederholen, indem Sie im Captive Portal die Option *Reauthentication* ankreuzen. ■

Weitere nützliche Anleitungen im Netz

- Scott Bartlett beschreibt unter *www.frontios.com/freeradius.html*, wie Sie FreeRADIUS mit MySQL verbinden.
- Wie auf der anderen Seite die Verbindung von MySQL zu Dialup Admin funktioniert, hat Karel Stadler dokumentiert: *http://kstadler.ch/index.php?page=dialup*
- Wie Sie einen Wireless-Hotspot mit Chillispot und OpenWRT einrichten, können Sie unter *www.howtoforge.com/wireless_hotspot_howto* nachlesen.
- Von Jonathan Hassell kommt das Standardwerk zu Radius: *www.onlamp.com/pub/a/onlamp/excerpt/radius_5/index1.html*