BRAIN-MEDIA.DE

PROFESSIONELLES INTERNET- UND OPEN-SOURCE-KNOW-HOW

Holger Reibold

XAMPP 1.8 kompakt

Web.Edition

Alles, was Sie für den Einsatz der Apache-MySQL-PHP-Perl-Umgebung wissen müssen

Holger Reibold

XAMPP 1.8 kompakt

© 2013 Brain-Media.de

Umschlaggestaltung: Brain-Media.de

Satz: Brain-Media.de

Coverbild: Photocase/hannesleitlein

Druck: COD

ISBN: 978-3-95444-042-9

Inhaltsverzeichnis

Vorwort

Wollten Sie nicht auch schon immer einmal Ihr eigener Web-Administrator sein, der für die Verwaltung einer Apache-Umgebung zuständig ist? Ober haben Sie nicht schon immer eine Umgebung gesucht, in der Sie in aller Ruhe Ihre Web-Seiten in einer realen Umgebung auf Herz und Nieren testen können? Wollten Sie nicht immer schon einmal eine neue Groupware-Umgebung, ein Web-Forum oder eine CRM-Lösung ohne Bauchschmerzen testen, ohne dabei Stunden für die Einrichtung einer entsprechenden Umgebung zu vergeuden? Oder wollten Sie nicht schon immer einmal PHP-Skripts programmieren und diese harten Praxistests unterziehen? Oder wollten Sie nicht schon immer Ihre MySQL-Kenntnisse auf Vordermann bringen?

Wenn Sie eine dieser Fragen (vielleicht auch mehrere) mit Ja beantworten, dann sind Sie hier richtig. XAMPP ist eine Lösung, mit der Sie mit minimalem Aufwand eine typische Apache-MySQL-PHP-Umgebung aufsetzen, wie sie im Internet zu Tausenden anzutreffen ist. Sie bildet den Grundstein für typische Webportale, Online-Shops, Communities und vieles mehr. Sie ist als Entwicklungsplattform konzipiert, taugt aber längst auch als unternehmensinterne Umgebung und kann auch im Internet eingesetzt werden.

Das Apachefriends-Team hat mit der Entwicklung von XAMPP eine wunderbare Lösung geschaffen, die nahezu jedermann den Einstieg in die Welt der Webserver und Apache-PHP-MySQL-basierten Lösungen erlaubt. So ist es auch nicht weiter verwunderlich, dass XAMPP längst ein fester Bestandteil der Open Source-Bewegung ist – und auch nicht mehr wegzudenken ist.

Seit der Veröffentlichung meines ersten XAMPP-Buchs sind inzwischen einige Jahre vergangen. Es folgten im Abstand von ca. 2 Jahren zwei weitere XAMPP-Titel – eine Ewigkeit im Internet-Zeitalter. Nun ist es endlich an der Zeit, der aktuellen XAMPP-Version 1.8 ein neues Buch zu widmen, das auf dem neuesten Stand ist. In dem vorliegenden Buch werden alle Anwendungen und Modul beschrieben, die in dem XAMPP-Paket enthalten sind.

Alles, was Sie für die praktische Verwendung wissen müssen, vermittelt das vorliegende Handbuch. Es führt Sie in die Arbeit mit XAMPP ein. Sie lernen die wichtigsten Komponenten und deren Handling kennen. Dem Buch liegt XAMPP 1.8.3 zugrunde.

Nach der Lektüre sind Sie in der Lage, die verschiedenen Module des XAMPP-Pakets effektiv einsetzen zu können.

Ich wünsche Ihnen dabei viel Erfolg!

Holger Reibold

(Oktober 2013)

1 Quickstart

Wer heute ein Content-Managementsystem, eine Groupware oder einen Online-Shop aufsetzen will, der kommt kaum noch an dem XAMPP-Paket vorbei. Es verknüpft all jene Komponenten, die für die Nutzung von Lösungen erforderlich sind, die auf dem Apache-MySQL-PHP-Gespann basieren. Da derlei Lösungen gerade im deutschsprachigen Raum so beliebt sind, ist auch die Nachfrage nach einem einfach zu installierenden und konfigurierenden Paket in der Vergangenheit rasant gestiegen.

Federführend haben Kai Oswald und Kai Seidler vom Apachefriends-Projekt (*http://www.apachefriends.org/de/xampp.html*) sich dieser Problematik angenommen und mit XAMPP ein Paket geschnürt, das kaum noch Wünsche offen lässt. Das XAMPP-Paket löst Probleme, die bei der Installation eines Apache-Webservers auftreten. Gerade auch, wenn dieser um weitere Komponenten, wie die bereits erwähnte Datenbank & Co., erweitert werden soll.

Ursprünglich war das XAMPP-Paket lediglich zu Testzwecken von Eigenentwicklungen konzipiert. Das hat sich inzwischen gewandelt, denn XAMPP kommt immer häufiger auch in lokalen Netzwerken zum Einsatz. Ihre Beliebtheit hat die Komplettlösung sicherlich auch dem Umstand zu verdanken, dass sie neben Linux auch für Windows, den Mac und Solaris verfügbar ist.

Das vorliegende Buch basiert auf XAMPP 1.8.3.

Die Linux-Variante trägt die Bezeichnung „XAMPP für Linux“. Sie wurde auf unterschiedlichen Linux-Distributionen getestet (SuSE, RedHat, Mandrake und Debian) und enthält folgende Tools: Apache 2.4.4, MySQL 5.5.32, PHP 5.4.19 & PEAR + SQLite 2.8.17/3.7.17 + multibyte (mbstring) support, Perl 5.16.3, ProFTPD 1.3.4c, phpMyAdmin 4.0.4, OpenSSL 1.0.1e, GD 2.0.35, Freetype2 2.4.8, libjpeg 8d, libpng 1.5.9, gdbm 1.8.3, zlib 1.2.3, expat 2.0.1, Sablotron 1.0.3, libxml 2.8.0, Ming 0.4.5, Webalizer 2.23-05, pdf class 0.11.7, ncurses 5.9, mod_perl 2.0.8, FreeTDS 0.91, gettext 0.18.1.1, IMAP C-Client 2007e, OpenLDAP (client) 2.4.21, mcrypt 2.5.8, mhash 0.9.9.9, eAccelerator 0.9.6.1, cURL 7.30.0, libxslt 1.1.28, libapreq 2.12, FPDF 1.7, bzip 1.0.6, ICU4C Library 4.8.1, APR (1.4.6), APR-utils (1.5.1).

Die Windows-Variante trägt entsprechend die Bezeichnung „XAMPP für Windows“. Das Basispaket kommt mit folgenden Programmen und Modulen daher: Apache 2.4.4, MySQL 5.6.11, PHP 5.5.3, phpMyAdmin 4.0.4, OpenSSL 0.9.8, XAMPP Control Panel 3.2.1, Webalizer 2.23-04, Mercury Mail Transport System

v4.62, FileZilla FTP Server 0.9.41, Tomcat 7.0.42 (with mod_proxy_ajp as connector), Strawberry Perl 5.16.3.1 Portable.

In der Mac OS X-Variante sind folgende Komponenten zusammengefasst: Apache 2.4.4, MySQL 5.5.32, PHP 5.4.19 & PEAR + SQLite 2.8.17/3.7.17 + multibyte (mbstring) support, Perl 5.16.3, ProFTPD 1.3.4c, phpMyAdmin 4.0.4, OpenSSL 1.0.1e, GD 2.0.35, Freetype2 2.4.8, libjpeg 8d, libpng 1.5.9, gdbm 1.8.3, zlib 1.2.3, expat 2.0.1, Sablotron 1.0.3, libxml 2.8.0, Ming 0.4.5, Webalizer 2.23-05, pdf class 0.11.7, ncurses 5.9, mod_perl 2.0.8, FreeTDS 0.91, gettext 0.18.1.1, IMAP C-Client 2007e, OpenLDAP (client) 2.4.21, mcrypt 2.5.8, mhash 0.9.9.9, eAccelerator 0.9.6.1, cURL 7.30.0, libxslt 1.1.28, libapreq 2.12, FPDF 1.7, bzip 1.0.6, ICU4C Library 4.8.1, APR (1.4.6), APR-utils (1.5.1).

Ein erster Blick auf XAMPP für Windows.

1.1 Der Begriff XAMPP

Sicherlich haben Sie es schon vermutet: XAMPP ist eine Abkürzung. Aber wofür? Es handelt sich um eine Abwandlung der bekannten Abkürzung LAMP bzw. LAMPP. Dabei steht das A für Apache, das M für MySQL, das erste P für Perl und das zweite P für PHP, das L steht für Linux. In den Anfangstagen von XAMPP gab

es zwei Namen: LAMPP und WAMPP. LAMPP stand dabei für die Linux-, WAMPP für die Windows-Variante.

Da das Paket aber längst nicht mehr nur unter Linux und Windows ausgeführt wird, ersetzten die Entwickler das L und W kurzerhand durch das X, das als Platzhalter für die verschiedenen Plattformen dient.

Viele routinierte Linux-Anwender stellen sich die Frage, warum man überhaupt ein Paket wie XAMPP benötigt, wenn doch die verschiedenen Komponenten einfach über den jeweiligen Paketmanager installiert werden können. Da es einen derartigen Komfort unter Windows nicht gibt, ist verständlich, dass unter dem proprietären System der Einsatz Sinn macht. Aber unter Linux?

Für den Einsatz gibt es verschiedene gute Gründe:

- Mithilfe von XAMPP ist es auch für Einsteiger möglich, eine funktionstüchtige Apache-Umgebung mit allem, was dazugehört, aufzusetzen. Er kann sich das mühsame Installieren und Lösen von Abhängigkeiten sparen, denn nicht überall ist die nachträgliche Installation von Komponenten so einfach wie unter OpenSuSE oder Kubuntu. Er spart sich auch das manuelle Bearbeiten und Anpassen von verschiedenen relevanten Konfigurationsdateien. Dank XAMPP ist die Umgebung in wenigen Minuten aufgesetzt und einsatzbereit.

- Für den Einsatz von XAMPP spricht auch, dass Sie immer die aktuellste Version der jeweiligen Komponenten zur Verfügung haben – und zwar in einer aufeinander abgestimmten Form. Das ist gerade für Entwickler von Web-Anwendungen wichtig, denn sie programmieren für die Zukunft und sind die Ersten, die Neuerungen gebrauchen können. Ein Entwickler kann programmieren, aber sich eine aktuelle Version zu installieren, kann sowohl unter Linux als auch unter Windows schon sehr knifflig sein. Dabei wird auch nicht jeder Zeit und Lust haben, auf eine neue Linux-Distribution zu warten.

- Für XAMPP spricht außerdem, dass das Paket auch dann aktualisiert wird, wenn die Version der Linux-Distribution schon von dem Distributor aufgegeben wurde. Es gibt erfahrungsgemäß eine Vielzahl an XAMPP-Anwendern, die das Paket auf älteren Linux-Systemen einsetzen.

- Ein weiterer Pluspunkt: Mit XAMPP vereinfacht sich der Deployment-Prozess. Wenn Sie Web-Applikationen entwickeln, können Sie diese auf einem Entwicklungssystem ausgiebig testen und verbessern. All das unter realen Bedingungen.

In der Summe spricht eine Vielzahl von Punkten für XAMPP. Sowohl Einsteiger als auch Profis profitieren von der Umgebung.

1.2 Installation von XAMPP für Windows

Genug der Vorrede. Schauen wir uns an, wie wir zu unserer XAMPP-Installation kommen. Laden Sie sich zunächst die aktuellste Version des XAMPP-Pakets herunter. Die nachfolgenden Abschnitte beschreiben die Installation von XAMPP für Linux und XAMPP für Windows, jeweils in der Version 1.8.3, die Ende August 2013 released wurde.

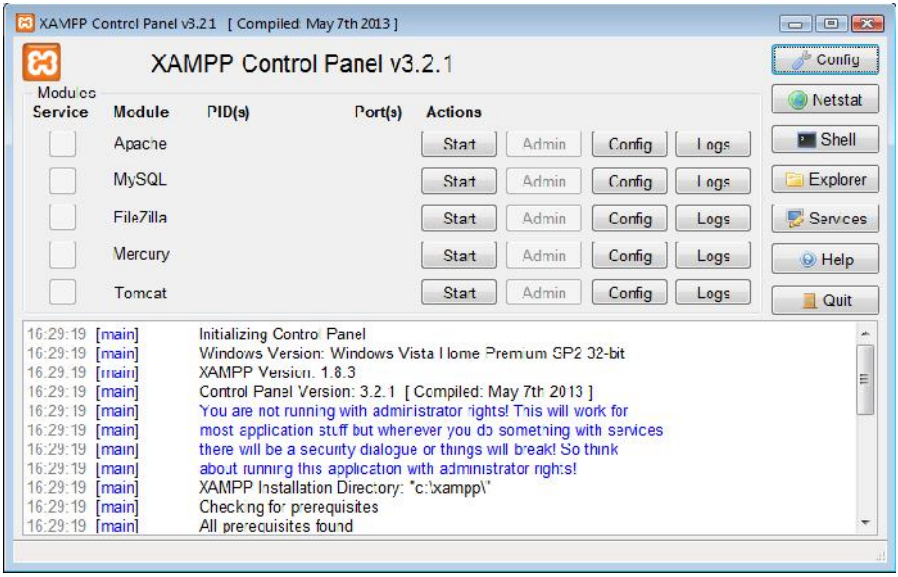
Das Basispaket von XAMPP für Windows steht über die Apachefriends-Website in drei Paketen zur Verfügung:

- Installer-Variante (116 MB)
- Gepackte ZIP-Variante (213 MB)
- EXE-Variante (101 MB)

In der Regel ist es am einfachsten, wenn Sie die Installer-Variante verwenden, denn hier führt Sie ein typischer Installationsdialog durch die notwendigen Schritte. Starten Sie nach dem Download der aktuellen XAMPP-für-Windows-Variante das Installationsprogramm mit einem Doppelklick auf *xampp-win32-1.8.3-installer.exe* (bzw. die entsprechende Bezeichnung Ihrer XAMPP-Version).

Es meldet sich der Installationsassistent, der Sie willkommen heißt. Bestimmen Sie in diesem Dialog das Zielverzeichnis, in das die Komponenten installiert werden sollen, beispielsweise *C:\xampp*, und klicken Sie auf die Install-Schaltfläche.

Der Assistent erlaubt Ihnen die Auswahl der verschiedenen Komponenten und kopiert anschließend die Datei in das gewünschte Verzeichnis. Der letzte Schritt erlaubt das Starten des XAMPP Control Panels. Es erlaubt insbesondere das Starten der verschiedenen Komponenten des XAMPP-Pakets. Damit ist XAMPP unter Windows vollständig installiert und Sie können die ersten Gehversuche unternehmen.



Das XAMPP Control Panel erlaubt Ihnen die Durchführung verschiedenster Steuerungsaktionen.

Mithilfe des XAMPP Control Panels können Sie eine Vielzahl von Aktionen durchführen (es ist übrigens auch über das Tray-Icon verfügbar), so beispielsweise das Starten und Stoppen von Servern, das Einrichten von Diensten, das Aufrufen von administrativen Schnittstellen und vieles mehr.

Wie bereits erwähnt, haben Sie eine weitere Installationsvariante zur Auswahl: Die Installation mit dem ZIP-Paket. Die Installation ohne den Installer ist für all jene geeignet, die ihre Registry frei von XAMPP-Einträgen halten wollen.

Die Vorgehensweise ist einfach: Laden Sie sich das ZIP-Archiv herunter. Entpacken Sie es. Dabei wird das Verzeichnis XAMPP erzeugt. Um eine dieser Varianten zu starten, führen Sie folgenden Befehl aus:

```
setup_xampp.bat
```

Wenn Sie mit dem XAMPP Control Panel arbeiten wollen, können Sie dies auch in der gepackten Variante starten:

```
xampp-control.exe
```

Auf der Konsolenebene sind weitere Kommandos ausführbar (immer im XAMPP-Verzeichnis):

- Apache und MySQL starten: *xampp_start.exe*
- Apache und MySQL anhalten: *xampp_stop.exe*
- nur den Apache starten: *apache_start.bat*
- nur den Apache anhalten: *apache_stop.bat*
- nur MySQL starten: *mysql_start.bat*
- nur MySQL anhalten: *mysql_stop.bat*
- den Mercury Mailserver starten: *mercury_start.bat* (das Stoppen ist nur über Mercury GUI möglich)
- den FileZilla-Server einrichten: *filezilla_setup.bat*
- den FileZilla-Server starten: *filezilla_start.bat*
- den FileZilla-Server anhalten: *filezilla_stop.bat*

Außerdem können Sie über die Konsole die verschiedenen Server als Dienste einrichten. Dazu verwenden Sie folgende Kommandos:

- Apache-Dienst installieren: *\xampp\apache\apache_installservice.bat*
- Apache-Dienst deinstallieren: *\xampp\apache\apache_uninstallservice.bat*
- MySQL-Dienst installieren: *\xampp\mysql\mysql_installservice.bat*
- MySQL-Dienst deinstallieren: *\xampp\mysql\mysql_uninstallservice.bat*
- FileZilla-Dienst einrichten: *\xampp\filezilla_setup.bat*
- FileZilla-Dienst deinstallieren: *\xampp\FileZillaFTP\filezilla_uninstallservice.bat*
- Mercury-Dienst installieren: *\xampp\MercuryMail\mercury_installservice.bat*
- Mercury Dienst deinstallieren: *\xampp\MercuryMail\mercury_uninstallservice.bat*

Die Basis-Variante von XAMPP ist in der Regel die richtige Variante. Sie deckt alle wichtigen Einsatzbereiche mit ihren Modulen ab. Neben der Standardvariante

gibt es auch abgespeckte Versionen, aber auch Add-ons, mit denen Sie die Funktionalität des XAMPP-Pakets aufbohren können.

Wenn Sie XAMPP wieder loswerden wollen, ist auch das kein Problem: Führen Sie einfach das Uninstall-Programm aus dem XAMPP-Programmeintrag der Startleiste aus.

1.3 Installation von XAMPP für Linux

Über die XAMPP-für-Linux-Seite des Apachefriends-Projekts steht auch die Linux-Variante zum Download bereit. Nach dem Download können Sie XAMPP installieren. Dazu starten Sie eine Linux-Shell und verschaffen sich zunächst Admin-Rechte:

```
su
```

Dann führen Sie den Installer für Linux aus:

```
chmod 755 xampp-linux-1.8.3-1-installer.run
./xampp-linux-1.8.3-1-installer.run
```

Wichtig: Verwenden Sie nur diesen Befehl. Entpacken Sie das Paket auf keinen Fall auf einem Windows-Rechner und kopieren Sie es dann auf das Linux-System. Das wird fehlschlagen.

Mit der Ausführung des obigen Befehls ist XAMPP im Verzeichnis */opt/lampp* installiert. Beachten Sie außerdem, dass eine bereits installierte Version von XAMPP dadurch überschrieben wird.

Nach der Ausführung des Einrichtungsassistenten meldet sich ein Skript, das von Ihnen einige Angaben erwartet, beispielsweise, ob Sie das vorgeschlagene Installationsverzeichnis übernehmen wollen. Die Skriptausführung sieht wie folgt aus:

```
./xampp-linux-1.8.3-1-installer.run
-------------------------------------------------------------
Welcome to the XAMPP Setup Wizard.

-------------------------------------------------------------
Select the components you want to install; clear the compo-
nents you do not want
```

```
to install. Click Next when you are ready to continue.

XAMPP Core Files : Y (Cannot be edited)

XAMPP Developer Files [Y/n] :y

Is the selection above correct? [Y/n]: y

-----------------------------------------------------------
Installation Directory

XAMPP will be installed to /opt/lampp
Press [Enter] to continue :

-----------------------------------------------------------
Setup is now ready to begin installing XAMPP on your comput-
er.

Do you want to continue? [Y/n]: y

-----------------------------------------------------------
Please wait while Setup installs XAMPP on your computer.

 Installing
 0% _______________ 50% _______________ 100%
 ########################################

-----------------------------------------------------------
Setup has finished installing XAMPP on your computer.

Launch XAMPP [Y/n]: y
```

Wenn Sei die letzte Frage mit *Y* beantwortet haben, können Sie XAMPP starten. Prinzipiell wird XAMPP mit folgendem Befehl gestartet:

```
/opt/lampp/lampp start
```

Im Terminaldialog sollten anschließend folgende Ausgaben zu sehen sein:

```
Starte XAMPP für Linux 1.8.3-1 ...
XAMPP: Starte Apache mit SSL (mit PHP5)...
XAMPP: Starte MySQL...
XAMPP: Starte ProFTPD...
XAMPP gestartet.
```

Für das Starten benötigen Sie ebenfalls Root-Berechtigungen. Also nicht vergessen, sich diese über *su* zu holen.

Damit ist XAMPP vollständig installiert und Sie können Ihre ersten Gehversuche unternehmen.

1.4 Installation von XAMPP für Mac OS X

Die Installation von XAMPP unter Mac OS X ist ebenfalls einfach. Laden Sie sich das DMG-Image auf Ihren Mac herunter und öffnen Sie das Image. Ziehen Sie den Inhalts des XAMPP-Ordners in den Programme-Ordner Ihres Mac-Systems. Beachten Sie, dass eine bereits installierte Version von XAMPP dadurch überschrieben wird. Das war's auch schon. XAMPP ist nun im Verzeichnis */Anwendungen/XAMPP* installiert.

Zum Starten von XAMPP genügt es, dass XAMPP Control Panel aus dem XAMPP-Ordner heraus zu öffnen. Über das Panel können Sie den Apache, MySQL und ProFTPD starten.

Als Nächstes testen Sie die Umgebung. Dazu folgen Sie im Fenster *Erste Schritte* dem *localhost*-Link. Über den Verweis *http://localhost/~benutzername/* greifen Sie auf die eingerichtete Home-Site zu.

Wenn Sie auch den FTP-Server gestartet haben, können Sie mit einem FTP-Client Ihrer Wahl auf das *htdocs*-Verzeichnis des XAMPP-Servers zugreifen. Standardmäßig eingerichtet ist hierfür der Benutzer *nobody* mit dem Passwort *xampp*.

XAMPP unter Mac OS X.

Auch die XAMPP für Mac-Installation ist standardmäßig unsicher. Doch dank eines einfachen Skripts können Sie die Sicherheitseinstellung einfach auf Vordermann bringen. Führen Sie dazu folgenden Befehl aus:

```
sudo /Programme/XAMPP/xamppfiles/xampp security
```

Auch hier meldet sich ein interaktiver Dialog, in dem Sie den unterschiedlichen Kennungen Passwörter zuweisen können.

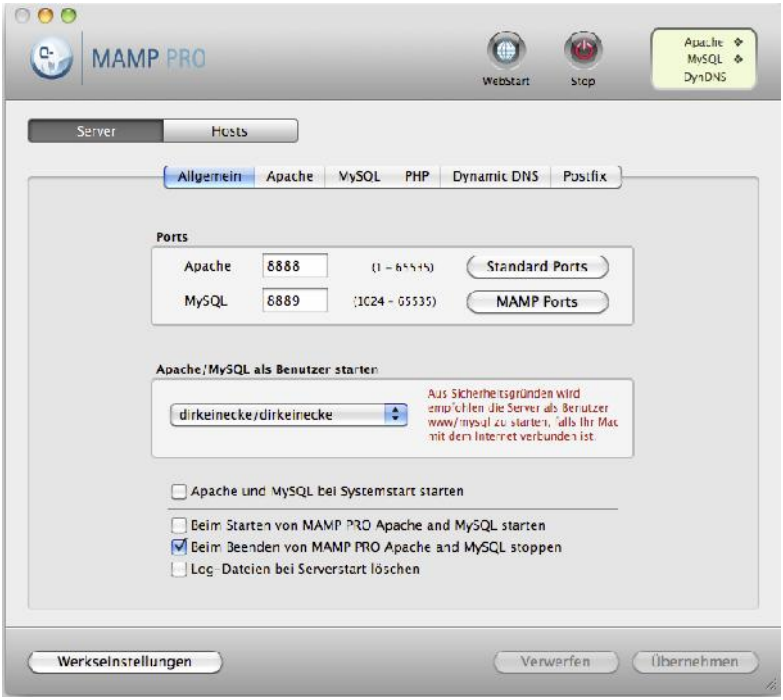
Mit dem Kommando */Programme/XAMPP/xamppfiles/xampp* können Sie auch die oben beschriebenen Start- und Stop-Parameter verwenden. Um beispielsweise die SSL-Unterstützung zu aktivieren, verwenden Sie folgenden Befehl:

```
sudo /Applications/XAMPP/xamppfiles/xampp startssl
```

Auch wenn es in diesem Buch um XAMPP geht, sei in diesem Zusammenhang doch auch auf MAMP (*http://www.mamp.info/de/mamp/index.html*) hingewiesen. MAMP – Sie ahnen es schon – steht für Macintosh, Apache, MySQL und PHP.

Die Mac-Umgebung bietet eine vergleichbare Funktionalität wie XAMPP, ist aber auf Mac OS X bestens abgestimmt.

Einen genauen Überblick, welche Programme und Bibliotheken in dem Paket enthalten sind, finden Sie auf der MAMP-Homepage. Die Ausstattung entspricht im Wesentlichen dem, was Sie bei XAMPP finden.



Ein Blick auf MAMP Pro.

MAMP ist in einer freien und einer kommerziellen Variante verfügbar. Die Pro-Variante bietet eine Mac-typische Konfiguration der wichtigsten Server-Anwendungen. Für die Detailkonfiguration müssen Sie sich allerdings an die Konfigurationsdateien der jeweiligen Server wagen. MAMP Pro kostet 39 EUR.

1.5 XAMPP kennenlernen

Wenn Ihre XAMPP-Installation ordnungsgemäß startet, sollten Sie mit dem Browser auf die XAMPP-Startseite zugreifen, über die die verschiedenen Komponenten verfügbar sind. Geben Sie bei einer lokalen Installation folgende URL an:

```
http://localhost
```

Wenn Sie von einem Zweitsystem auf die XAMPP-Installation zugreifen, verwenden Sie folgende URL:

```
http://ip_adresse
```

XAMPP präsentiert Ihnen seine Startseite. Wenn Sie diese Startseite später durch eine eigene Seite austauschen, ist die XAMPP-Installation immer noch über folgende URL verfügbar:

```
http://localhost/xampp/
```

Beachten Sie, dass es zwischen den beiden XAMPP-Varianten für Linux und Windows geringfügige Unterschiede gibt.

Die XAMPP-Startseite ist übersichtlich strukturiert. Über die Kopfzeile haben Sie Zugriff auf die verschiedenen Sprachvarianten. Links finden Sie das Navigationssystem, daneben die eigentlichen Inhalte bzw. Funktionen.

In der Navigationsleiste finden Sie die Rubrik *Php*. Anhand der verfügbaren Beispielprogramme (es handelt sich überwiegend um einfache PHP-Applikationen) können Sie sicherstellen, ob die XAMPP-Installation auch korrekt arbeitet. Folgen Sie beispielsweise einfach dem Verweis *CD-Verwaltung* und füttern Sie diese mit ein oder zwei Einträgen. Funktioniert die Anwendung, dürfen Sie davon ausgehen, dass XAMPP korrekt arbeitet.

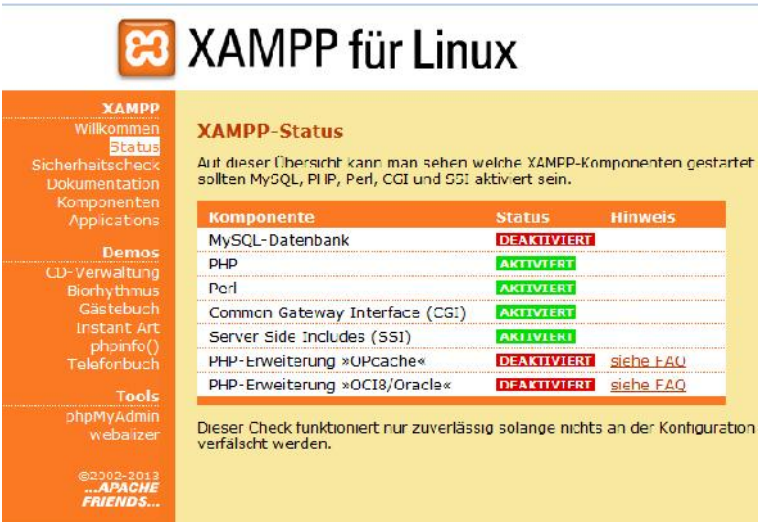
Für Ihre spätere Arbeit mit XAMPP sind insbesondere die Funktionen der Bereiche XAMPP und Tools wichtig. Im Bereich XAMPP finden Sie unter Windows folgende Funktionen: Status, Sicherheitscheck, Dokumentation, Komponenten und *phpinfo()*. Bei XAMPP für Linux stehen Ihnen bis auf *phpinfo()* die gleichen Funktionen zur Verfügung. Die Windows-Version zeigt außerdem die Version der aktuellen PHP-Version an.

Im Bereich *Tools* stehen Ihnen in der Windows-Version folgende Funktionen zur Verfügung: phpMyAdmin, Webalizer, PHP Umschalter, Mercury Mail und FileZilla FTP. Bei der Linux-Variante sind es lediglich zwei Tools: phpMyAdmin und

Webalizer. Auf die einzelnen Tools kommen wir im weiteren Verlauf dieses Buchs – meist in eigenen Kapiteln – noch zu sprechen.

1.6 Funktionen des Bereichs XAMPP

Über die Navigationsleiste der XAMPP-Webschnittstelle greifen Sie auf eine Vielzahl wichtiger Funktionen und Module zu. Einige wurden bereits oben erwähnt, auf Andere kommen wir im weiteren Verlauf dieses Buchs noch detailliert zu sprechen. Der Bereich *XAMPP* der XAMPP-Navigationsleiste stellt Ihnen zwei wichtige Funktionen zur Verfügung: *Status* und *Sicherheitscheck.*

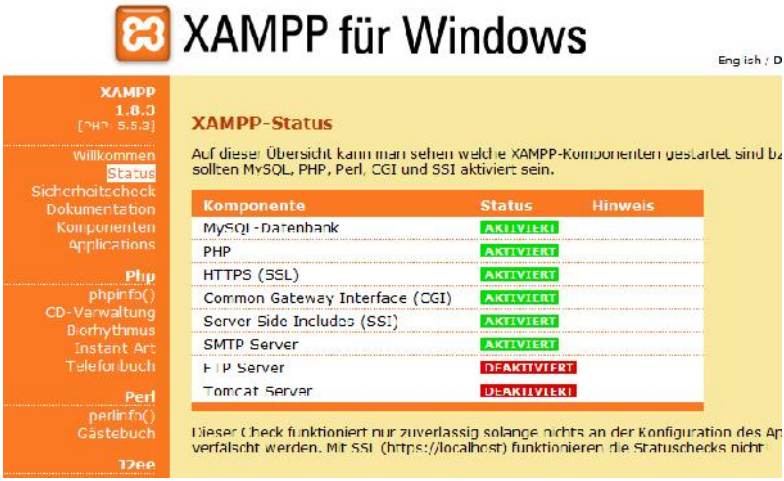


Der Status einer XAMPP-für-Linux-Installation.

Bei einer Linux-basierten Standardinstallation sind folgende Komponenten aktiv:

- PHP
- Perl
- CGI
- SSI

Es versteht sich von selbst, dass der Apache aktiv ist, denn sonst können Sie nicht auf die Web-Schnittstelle zugreifen. Nicht aktiv sind die PHP-Erweiterungen eAccelerator und OCI8/Oracle.



Der Status einer XAMPP-für-Windows-Installation.

Bei einer Windows-basierten Installation sind folgende Dienste aktiviert:

- MySQL-Datenbank
- PHP
- HTTPS (SSL)
- Common Gateway Interface (CGI)
- Server Side Includes (SSI)

Deaktiviert sind der SMTP- und der FTP-Server. Beide können allerdings, wie Sie noch sehen werden, recht einfach in Betrieb genommen werden.

Beachten Sie, dass der Status-Check nur dann zuverlässig funktioniert, solange Sie keine Änderungen an der Apache-Konfiguration vorgenommen haben. Der Check funktioniert auch nicht, wenn Sie SSL verwenden.

1.7 XAMPP Control Panel für Windows

Wenn Sie mit einer XAMPP für Windows-Installation arbeiten, so ist das XAMPP Control Panel ein wichtiges Hilfsmittel, das Ihnen bei verschiedenen Aktionen gute Dienste leistet. Es erlaubt besonders einfach, folgende Server zu starten bzw. zu stoppen:

- Apache
- MySQL
- FileZilla
- Mercury
- Tomcat

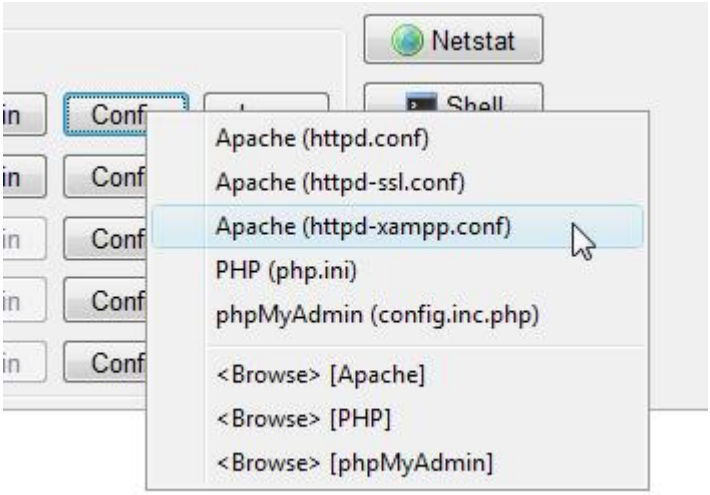
Wenn Sie die Server gestartet haben, können Sie über die jeweilige Admin-Schaltfläche auf die zugehörigen Administrationsfunktionen zugreifen. Im Falle des Apache landen Sie auf der XAMPP-Web-Schnittstelle und bei MySQL auf der Windows-MySQL-Administration. Auch für den Mercury-Mail- und den FileZilla-FTP-Server stehen Windows-basierte Administrationszentralen zur Verfügung.

Das Control Panel erlaubt Ihnen über die Schaltfläche *Service* auch das Starten der Windows-Diensteinstellungen. Mit einem Doppelklick können Sie dann beispielsweise den MySQL-Service öffnen und den Starttyp verändern.

Das XAMPP Control Panel hat weitere nützliche Funktionen zu bieten. Sie können über den *Admin*-Button auf das Administrationswerkzeug des jeweiligen XAMPP-Moduls zugreifen. Im Falle von Apache ist das die webbasierte XAMPP-Schnittstelle, bei MySQL starten Sie mit einem Klick auf *Admin* den Datenbankmanager phpMyAdmin, auf den wir in Kapiel 4 detailliert zu sprechen kommen.

Über die Spalte mit den Config-Schaltflächen greifen Sie auf die Konfigurationsdateien der verschiedenen Applikationen und Serverkomponenten zu. So können Sie beispielsweise die Apache-Konfiguration ändern, die PHP-Installation oder auch den Datenbankmanager phpMyAdmin anpassen.

Entsprechend können Sie auf Protokolldateien der verschiedenen Module zugreifen. Klicken Sie dazu auf die Schaltfläche *Logs* und wählen Sie die gewünschte Log-Datei aus, sofern mehrere angeboten werden.



Der Zugriff auf die Konfigurationsdateien.

Im linken oberen Bereich zeigt Ihnen das Control Panel den Status der verschiedenen Server an. Aktive Server werden grün hinterlegt und samt PID und Port-Angabe aufgeführt

In der Statusausgabe unterhalb der Schaltfläche zeigt Ihnen das Tool neben der verwendeten Windows-Version das XAMPP-Verzeichnis sowie den Status an. Eine typische Ausgabe sieht wie folgt aus:

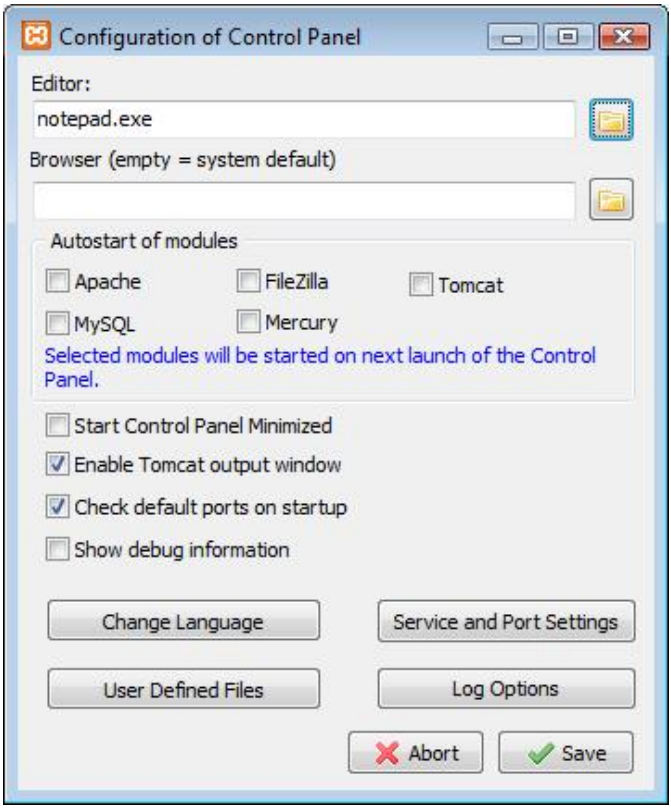
```
08:59:04  [main]    Initializing Control Panel

08:59:04  [main]    Windows Version: Windows Vista Home Pre-
mium SP2 32-bit

08:59:04  [main]    XAMPP Version: 1.8.3

08:59:04  [main]    Control Panel Version: 3.2.1  [ Compiled:
May 7th 2013 ]

08:59:04  [main]    You are not running with administrator
rights! This will work for

08:59:04  [main]    most application stuff but whenever you do
something with services

08:59:04  [main]    there will be a security dialogue or
things will break! So think
```

```
08:59:04  [main]    about running this application with admin-
istrator rights!
08:59:04  [main]    XAMPP Installation Directory: "c:\xampp\"
08:59:04  [main]    Checking for prerequisites
08:59:04  [main]    All prerequisites found
08:59:04  [main]    Initializing Modules
08:59:04  [main]    Starting Check-Timer
08:59:04  [main]    Control Panel Ready
09:00:18  [Apache]  Attempting to start Apache app...
09:00:19  [mysql]   Attempting to start MySQL app...
09:00:19  [mysql]   Status change detected: running
09:00:20  [Apache]  Status change detected: running
09:00:23  [main]    Executing "c:\xampp\"
09:01:36  [main]    Executing "services.msc"
```

Im Statusfeld werden Statusinformationen zu den Servern ausgegeben. Sie erfahren dort, ob ein Server ausgeführt wird und vieles mehr.

Im rechten oberen Bereich des Control Panels finden Sie weitere Schaltflächen, hinter denen sich weitere nützliche Funktionen verbergen. Über die *Config*-Schaltfläche greifen Sie auf die Konfigurationsmöglichkeiten des Control Panels zu. In dem zugehörigen Dialog können Sie zunächst den Standardeditor und den Standard-Browser bestimmen.

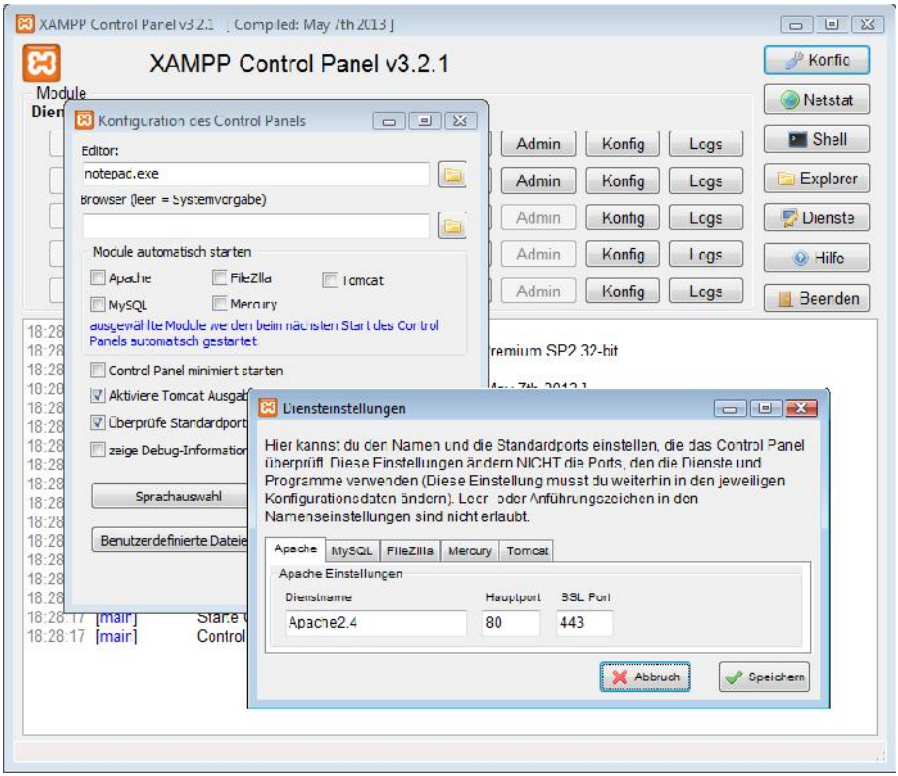
Im Bereich *Autostart of modules* bestimmen Sie, welche der Module in Zukunft automatisch gestartet werden soll. Sie können durch das Aktivieren der Option *Start Control Panel Minimized* dafür sorgen, dass das Panel minimiert gestartet wird. Sollten Probleme bei der Ausführung von XAMPP auftreten, aktivieren Sie die Option *Show debug information*, um anhand der Debug-Ausgabe eventuell weitere relevante Informationen auszulesen.



Die Konfiguration des XAMPP Control Panels 3.2.1.

Mit *Change Language* können Sie die Sprachversion wählen. Neben der englischen Version steht Ihnen auch die deutsche Variante zur Verfügung. Nach dem Neustart des Panels steht Ihnen die deutsche Version zur Verfügung.

Wenn Sie die deutsche Sprachversion aktiviert haben, können Sie in der Panel-Konfiguration über die Schaltfläche *Dienste und Ports einstellen* die Dienstbezeichnungen für die fünf Server Apache, MySQL, FileZilla, Mercury und Tomcat sowie die zughehörigen Port-Einstellungen bearbeiten.



Das eingedeutschte XAMPP Control Panel erlaubt über die Konfiguration das Einstehen und Bearbeiten der Diensteinstellungen.

Im Panel können Sie über *Benutzdefinierte Log- und Konfigurationsdateien* alternative Konfig-Dateien angeben. Damit steht Ihnen eine ausgesprochen praktische Funktion zur Verfügung, mit der Sie schnell mal alternative Server-Einstellungen testen können. Über die Schaltfläche *Log-Optionen* können Sie lediglich die Schriftart und -größe der Protokolldatei anpassen.

Das XAMPP Control Panel verrät Ihnen über das Netstat-Modul, welche Netzwerkverbindungen aktuell bestehen. Über *Shell* öffnen Sie ein Terminal-Fenster, das Ihnen die Eingabe von Kommandos auf der Konsolenebene erlaubt.

Um einen Blick in die XAMPP-Verzeichnisstruktur zu werfen, klicken Sie auf *Explorer*. Mit *Dienste* öffnen Sie die Windows Diensteverwaltung, in der Sie beispielsweise den Starttyp ändern können.

1.8 XAMPP Control Panel für Linux

Inzwischen gibt es sogar eine einfache Version des Control Panels für Linux. Es handelt sich dabei um ein Python-basiertes Tool. Um es nutzen zu können, müssen Sie auf Ihrem Linux-System den Python-Interpreter installieren. Bei einer Standardinstallation finden Sie das Panel in folgendem Verzeichnis:

```
/opt/lampp/share/xampp-control-panel/
```

Sie starten es mit folgendem Kommando:

```
./xampp-control-panel.py
```

Beachten Sie, dass Sie zur Ausführung Root-Rechte benötigen. Da das Panel Python-basiert ist, wird es wohl bis auf Weiteres auch nicht direkt zugänglich sein oder über die Web-Schnittstelle integriert werden.

Das XAMPP Control Panel für Linux in Aktion.

Im Unterschied zur Windows-Variante bietet das Linux-Control-Panel deutlich weniger Funktionalität. Sie können die gesamte XAMPP-Installation oder auch einzelne Server anhalten bzw. neu starten. Über die Schaltfläche *Einstellungen* können Sie außerdem ein alternatives XAMPP-Installationsverzeichnis angeben, falls Sie XAMPP an einem anderen Ziel eingerichtet haben.

1.9 Linux- und Windows-spezifische Eigenheiten

Wenn Sie XAMPP unter Linux verwenden, so steht Ihnen eine Fülle von weiteren Befehlen zur Verfügung, mit denen Sie beispielsweise das Starten und Anhalten steuern oder auch XAMPP deinstallieren können. Die meisten dieser Funktionen sind unter Windows über das Control Panel verfügbar.

Das XAMPP-Paket hat weitere nützliche Befehle zu bieten. Hier alle Kommandos im Überblick:

- **start**: Startet XAMPP.
- **stopp**: Stoppt XAMPP.
- **restart**: Stoppt und startet XAMPP.
- **reload**: Apache, MySQL und − wenn gestartet − ProFTPD lesen ihre Konfigurationsdatei neu ein.
- **security**: Führt einen kleinen Sicherheitscheck des XAMPP durch und schließt eventuelle Lücken.
- **startapache**: Startet nur den Apache.
- **startssl**: Hiermit wird der Apache mit SSL-Unterstützung gestartet und unter *https://localhost* kann man seinen Apache via SSL erreichen. Durch diesen Befehl wird die SSL-Unterstützung permanent aktiviert. Das bedeutet, dass er auch beim nächsten Start des XAMPP-Pakets wieder mit SSL-Unterstützung gestartet wird.
- **startmysql**: Dieser Befehl startet nur die MySQL-Datenbank.
- **startftp**: Dieses Kommando startet nur den ProFTPD-Server. Der FTP-Server ist so vorkonfiguriert, dass man mit dem Benutzer *nobody* und dem Passwort *lampp* nun z. B. die HTML-Dateien auf den XAMPP-Server hochladen kann.

Daneben gibt es einige Stopp-Kommandos:

- **stopapache**: Stoppt den Apache.
- **stopssl**: Stoppt die SSL-Unterstützung des Apache. Auch beim nächsten Start von XAMPP wird die SSL-Unterstützung nicht mehr mit gestartet.
- **stopmysql**: Hält die MySQL-Datenbank an.

- **stopftp**: Stoppt den ProFTPD-Server. Auch beim nächsten Start von XAMPP wird der FTP-Server nicht mehr mit gestartet.

Und es gibt drei Reload-Befehle:

- **reloadapache**: Der Apache liest seine Konfigurationsdatei neu ein.
- **reloadmysql**: MySQL liest seine Konfigurationsdatei neu ein.
- **reloadftp**: ProFTPD liest seine Konfigurationsdatei neu ein.

Schauen wir uns noch ein konkretes Beispiel an. Um den Apache mit SSL-Unterstützung zu starten, verwenden Sie einfach den folgenden Befehl:

```
/opt/lampp/lamp startssl
```

Der SSL-gesicherte Zugriff auf den Webserver erfolgt dann über *https://localhost* bzw. *https://ip_adresse*.

Die meisten Administratoren geben sich ungern mit den Möglichkeiten zufrieden, die ihnen eine webbasierte Schnittstelle bietet. Vielmehr wollen sie wissen, wo welche Dateien liegen, um gegebenenfalls selbst Hand anlegen zu können. Eine Standard-XAMPP-Installation besitzt folgende Verzeichnisse und Dateien:

- **/opt/lampp/bin/**: In diesem Verzeichnis finden Sie die XAMPP-Befehle (siehe oben).
- **/opt/lampp/htdocs/**: Das ist das DocumentRoot-Verzeichnis des Apache-Webservers. Hier liegen die Webseiten Ihres Webservers.
- **/opt/lampp/etc/httpd.conf**: Das ist die zentrale Konfigurationsdatei für den Apache-Webserver.
- **/opt/lampp/etc/my.cnf**: Das ist die Konfigurationsdatei des MySQL-Datenbankservers.
- **/opt/lampp/etc/php.ini**: Das ist die PHP-Konfigurationsdatei.
- **/opt/lampp/etc/proftpd.conf**: Und das ist die Konfigurationsdatei für den ProFTPD.
- **/opt/lampp/phpmyadmin/config.inc.php**: Das ist die Konfigurationsdatei für phpMyAdmin.

Wenn Sie Änderungen an einer Konfigurationsdatei vornehmen, sollten Sie XAMPP stoppen, die Änderungen vornehmen und dann die Umgebung wieder starten. Zum Stoppen von XAMPP verwenden Sie folgenden Befehl:

```
/opt/lampp/lampp stop
```

Die zugehörige Aufgabe im Terminalfenster sollte wie folgt aussehen:

```
Stopping XAMPP für Linux 1.8.3 ...
XAMPP: Stopping Apache...
XAMPP: Stopping MySQL...
XAMPP: Stopping ProFTPD...
XAMPP stopped.
```

Damit ist XAMPP beendet.

Wenn Sie XAMPP deinstallieren wollen, so ist auch das mit einem einfachen Befehl möglich:

```
rm -rf /opt/lampp
```

Aber Vorsicht, denn Sie entfernen damit auch etwaige auf der Umgebung aufsetzende Installationen, wie einen Online-Shop, ein Content-Managementsystem etc.

Damit kennen Sie die wichtigsten Funktionen der XAMPP-Schnittstelle. Auf die Funktion *Sicherheitscheck* kommen wir in Kapitel 11 noch detailliert zu sprechen. Der Vollständigkeit halber soll noch erwähnt werden, dass Sie der Link *Dokumentation* zu einer Übersicht mit relevanten Websites führt, unter *Komponenten* Links zu den einzelnen XAMPP-Komponenten zu finden sind und Ihnen die Funktion *phpinfo()* – allerdings nur unter Windows – die technischen Details Ihrer PHP-Installation liefert.

System	Linux linux-ivwi.site 3.7.10-1.1-desktop #1 SMP PREEMPT Thu Feb 28 15:06:29 UTC 2013 (82d3f21) x86_64
Build Date	Aug 26 2013 13:27:06
Configure Command	'./configure' '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/opt/lampp' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap=/bitnami/xamppunixinstallerstackDev-linux/src/imap-2007e' '--with-imap-ssl' '--with-gettext=/opt/lampp' '--with-mssql=/opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-oci8=shared,instantclient,/opt/lampp/lib/instantclient' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared,/opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared,/opt/lampp/' '--with-iconv=/opt/lampp' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo-sqlite' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar' '--enable-zip' '--enable-intl'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc

Diese Informationen sind überwiegend für PHP-Entwickler von Interesse – gerade dann, wenn etwas nicht funktioniert.

2 Apache im Griff

Der Apache-Webserver (*http://www.apache.org*) ist das Herzstück Ihrer XAMPP-Installation. Er ermöglicht die Veröffentlichung von Dokumenten und erlaubt die Ausführung von Anwendungen (vorausgesetzt, die notwendigen Interpreter sind ebenfalls installiert).

2.1 Apache-Basics

Mit der Einführung von Version 2.0 wurden die Stabilität und Geschwindigkeit des Servers erheblich verbessert; gerade auch auf Nicht-Linux-Plattformen. Der Apache-2.0 brachte eine neue Architektur, deren Ziel es war, den Apache leichter portierbar zu machen. Dieses Ziel wurde dadurch erreicht, dass nun sämtlicher plattformspezifischer Code sauber getrennt vom restlichen Apache-Code in den Sourcen der Apache Portable Runtime (APR) und der Multi Processing Modules (MPM) zu finden ist. Durch diese Kapselung ist es für die Apache-Entwickler leichter geworden, plattformspezifische Änderungen und Optimierungen vorzunehmen.

Ein weiteres sehr wichtiges Merkmal des Apache-Webservers ist sein modularer Aufbau. Durch entsprechende Module kann er beispielsweise die Kommunikation zwischen Browser und Webserver verschlüsseln (*mod_ssl*), als Proxy-Server agieren (*mod_proxy*) oder komplexe Manipulationen von HTTP-Kopfdaten (*mod_headers*) und URLs (*mod_rewrite*) durchführen.

Wie Sie bereits wissen, bietet er die Möglichkeit, mit Hilfe unterschiedlicher Skriptsprachen Webseiten dynamisch zu erstellen. Häufig verwendete Skriptsprachen sind PHP und Perl.

Das Schöne an dem XAMPP-Paket: Der Server ist fix und fertig installiert und voll funktionstüchtig. Aufwendige Installationen und Konfigurationen entfallen. Das genügt zumindest für die gängigsten Aufgaben.

Ursprünglich wurde der Server fast ausschließlich über die Apache-Konfigurationsdatei *httpd.conf* gesteuert. Das hat sich mit der Einführung von Version 2.2 geändert. Nun wird die Konfiguration auf mehrere Konfigurationsdateien verteilt. Die Konfigurationsdateien finden Sie unter Linux im Verzeichnis */opt/lampp/etc/extra* und unter Windows standardmäßig unter *C:\xampp\apache\conf\extra*.

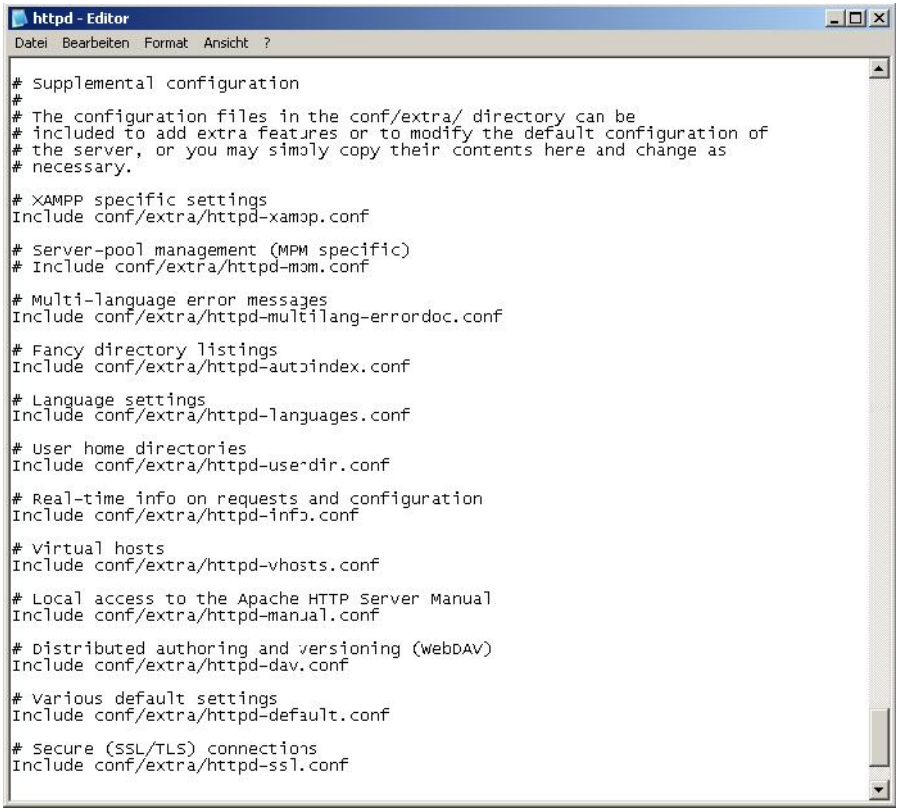
Die Hauptkonfigurationsdatei *httpd.conf* finden Sie im Verzeichnis */opt/lampp/etc* bzw. *C:\xampp\apache\conf*, also eine Verzeichnisebene höher. Im Falle der Linux-Konfiguration finden Sie im */etc*-Verzeichnis auch die Konfigurationsdateien für den FTP-Server ProFTP und Webalizer.

Zu beiden XAMPP-Varianten finden Sie zwölf Unterkonfigurationsdateien:

- **httpd-autoindex.conf**: Dient der Konfiguration des Index und der Icons
- **httpd-dav.conf**: Dient der Konfiguration der WebDAV-Funktionalität
- **httpd-default.conf**: Hier finden Sie die Standardeinstellungen für den Webserver
- **httpd-info**: Hier hinterlegen Sie die Einstellungen zum Serverstatus und zur Server-Info
- **httpd-language**s: Dient der Konfiguration länderspezifischer Einstellungen
- **httpd-manual**: Einstellungen für die Server-Dokumentation
- **httpd-mpm**: Server-Pool-Management
- **httpd-multilang-errordoc**: Mehrsprachige Fehlermeldungen
- **httpd-ssl**: Dient der Konfiguration der SSL-Unterstützung
- **httpd-userdir**: Konfiguration der Benutzerpfade
- **httpd-vhosts**: Hier konfigurieren Sie die virtuellen Server.
- **httpd-xampp**: Hier finden Sie verschiedene XAMPP-spezifische Einstellungen

Diese „Unter-Konfigurationsdateien“ werden in der Hauptkonfigurationsdatei *httpd.conf* über die *include*-Anweisung eingebunden. In der Standard-XAMPP-Konfiguration sind alle zwölf Konfigurationen eingebunden und aktiv.

Bevor Sie sich an die Anpassung erster Konfigurationen machen, sollten Sie wissen, dass Änderungen immer einen Neustart des Apache-Webservers erfordern. Halten Sie ihn am besten über das XAMPP Control Panel oder die im Kapitel 1 beschriebenen Kommandos an und starten Sie ihn erneut.



Ein Blick in die Apache-Hauptkonfigurationsdatei zeigt, dass auch alle Unterkonfigurationen eingebunden sind.

Welche Einstellungen im Einzelfall relevant sind, ist meist von den jeweiligen Anforderungen und Einsatzszenarien abhängig. Ihre XAMPP-Konfiguration ist standardmäßig so gut, dass Sie zumindest an der Hauptkonfiguration selten Hand anlegen müssen.

Dennoch gibt es natürlich immer wieder Situationen, in denen man froh ist, wenn man weiß, was man überhaupt anpassen kann. Die Apache-Hauptkonfigurationsdatei erlaubt Ihnen beispielsweise die Anpassung des Ports, des Dokumenten-Root-Verzeichnisses und auch das Ein- bzw. Ausschließen der oben erwähnten Unterkonfigurationen.

Hier ein Beispiel einer sehr einfachen Apache-Konfiguration. Den Erläuterungen können Sie entnehmen, um welche Einstellungen es sich handelt und ob eventuell eine Anpassung für Sie infrage kommt:

```
#
# Apache-Hauptkonfiguration
#

# ThreadsPerChild: Konstante Anzahl an Worker-Threads
# im Server-Prozess.
# MaxRequestsPerChild: Maximale Anzahl an Requests,
# die ein Server-Prozess bedient
ThreadsPerChild 250
MaxRequestsPerChild  0

# ServerRoot-Verzeichnis
ServerRoot "C:/xampp/apache"

# HTTP-Port, auf den der Webserver "horcht"
Listen 80

# Unterstützung von Dynamic Shared Object (DSO)
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule asis_module modules/mod_asis.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule authn_default_module modules/mod_authn_default.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authz_default_module modules/mod_authz_default.so
LoadModule authz_groupfile_module mod-
ules/mod_authz_groupfile.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_user_module modules/mod_authz_user.so
```

```
LoadModule cgi_module modules/mod_cgi.so
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule dir_module modules/mod_dir.so
LoadModule env_module modules/mod_env.so
LoadModule include_module modules/mod_include.so
LoadModule info_module modules/mod_info.so
LoadModule isapi_module modules/mod_isapi.so
LoadModule ldap_module modules/mod_ldap.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule mime_module modules/mod_mime.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule status_module modules/mod_status.so
LoadModule ssl_module modules/mod_ssl.so
LoadModule autoindex_color_module mod-
ules/mod_autoindex_color.so

## Hauptkonfiguration ##

# E-Mail-Adresse des Server-Admins
ServerAdmin admin@localhost

# Servername
ServerName localhost:80

# DocumentRoot-Verzeichnis
DocumentRoot "C:/xampp/htdocs"

# Zugriffssteuerung
<Directory />
```

```
    Options FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>

# DocumentRoot-spezifische Einstellungen
<Directory "C:/xampp/htdocs">
    Options Indexes FollowSymLinks Includes ExecCGI
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>

# Verzeichnisindex
<IfModule dir_module>
    DirectoryIndex index.php index.php4 index.php3 index.cgi
index.pl index.html index.htm index.shtml index.phtml
</IfModule>

# Schützt Dateien, die durch .htaccess und .htpasswd
# geschützt sind, vor den Blicken von Web-Clients.
<FilesMatch "^\.ht">
    Order allow,deny
    Deny from all
</FilesMatch>

# Pfad zur Fehlerprotokolldatei
ErrorLog logs/error.log
```

```
# Protokoll-Level. Mögliche Werte sind debug, info,
# notice, warn, error, crit, alert, emerg.
LogLevel warn


# Einstellungen für die Protokollierung
<IfModule log_config_module>
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    <IfModule logio_module>


      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\" %I %O" combinedio
    </IfModule>
# Pfad zur Access-Logdatei
CustomLog logs/access.log common
</IfModule>


# Konfiguration des Skript-Verzeichnisses
<IfModule alias_module>
    ScriptAlias /cgi-bin/ "C:/xampp/cgi-bin/"
</IfModule>


<Directory "C:/xampp/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>


# Standarddateitypen
```

```
DefaultType text/plain

<IfModule mime_module>
    TypesConfig conf/mime.types
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
    AddHandler cgi-script .cgi
    AddType text/html .shtml
    AddOutputFilter INCLUDES .shtml
</IfModule>

# Konfiguration der Fehlerausgabe
#ErrorDocument 500 "Der Server ist nicht verfügbar."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402
http://www.server.de/subscription_info.html

# Deaktiviert EnableMMAP und EnableSendfile
EnableMMAP off
EnableSendfile off

# Ergänzende Konfigurationen (die bereits erwähnten
# Konfigurationen für SSL etc.)
Include conf/extra/httpd-xampp.conf
Include conf/extra/httpd-mpm.conf
Include conf/extra/httpd-multilang-errordoc.conf
Include conf/extra/httpd-autoindex.conf
Include conf/extra/httpd-languages.conf
Include conf/extra/httpd-userdir.conf
Include conf/extra/httpd-info.conf
```

```
Include conf/extra/httpd-vhosts.conf
Include conf/extra/httpd-manual.conf
Include conf/extra/httpd-dav.conf
Include conf/extra/httpd-default.conf
Include conf/extra/httpd-ssl.conf

# Erforderlich für SSL
<IfModule ssl_module>
    SSLRandomSeed startup builtin
    SSLRandomSeed connect builtin
</IfModule>
```

Welchen Einstellungen Sie sich als Nächstes widmen wollen, ist natürlich auch von Fall zu Fall sehr unterschiedlich. Die gängigsten Folgeaktionen nach einer Anpassung der Apache-Grundkonfiguration sind meist das Erstellen eines Verzeichnisschutzes, die Sicherung des Zugriffs per SSL, die Aktivierung des WebDAV-Zugriffs auf den Webserver oder das Anlegen von virtuellen Hosts.

2.2 Verzeichnisschutz mithilfe der .htaccess

Eine der häufigsten Anforderungen an einen Apache-Webserver: Den Zugriff auf spezifische Verzeichnisse über ein Log-in zu schützen. Das ist besonders einfach mit der .htaccess-Datei möglich. Aber Sie können mit diesen Dateien noch mehr anstellen.

Die .htaccess-Datei ist eine Apache-Konfigurationsdatei, die es Ihnen erlaubt, über Regeln das Verhalten der zu Ihrem Server-Paket gehörenden Verzeichnisse zu steuern. Mithilfe einer solchen Datei können Sie beispielsweise Weiterleitungen umsetzen, IP-Sperren einfügen, virtuelle Verzeichnisse erstellen und Passwortgeschützte Bereiche realisieren. Der häufigste Einsatzbereich ist sicherlich das Erstellen eines Passwortschutzes.

Mit der .htaccess-Konfigurationsdatei lassen sich mit relativ wenig Aufwand Verzeichnisse und Dateien per Passwort schützen. Der Vorteil dieses Schutzes: Er gilt für die meisten Anwendungen als ausreichend sicher und lässt sich einfach einrichten.

Hier ein Beispiel für eine entsprechende .htaccess-Datei:

```
# Passwortschutz .htaccess
AuthType Basic
AuthName "gemein"
AuthUserFile /usr/.htusers
AuthGroupFile /usr/.htgroups
Require user Holger Reibold
Require group brain-media
```

Dann müssen Sie noch die Gruppendatei *.htgroups* erzeugen. Sie könnte wie folgt aussehen:

```
# Gruppendatei .htgroups
bomots: Holger Reibold
```

Es fehlt noch die Benutzerdatei *.htusers*. Die sieht in unserem Beispiel wie folgt aus:

```
# Benutzerdatei .htusers
Holger:Passwort1
Silke:Passwort2
```

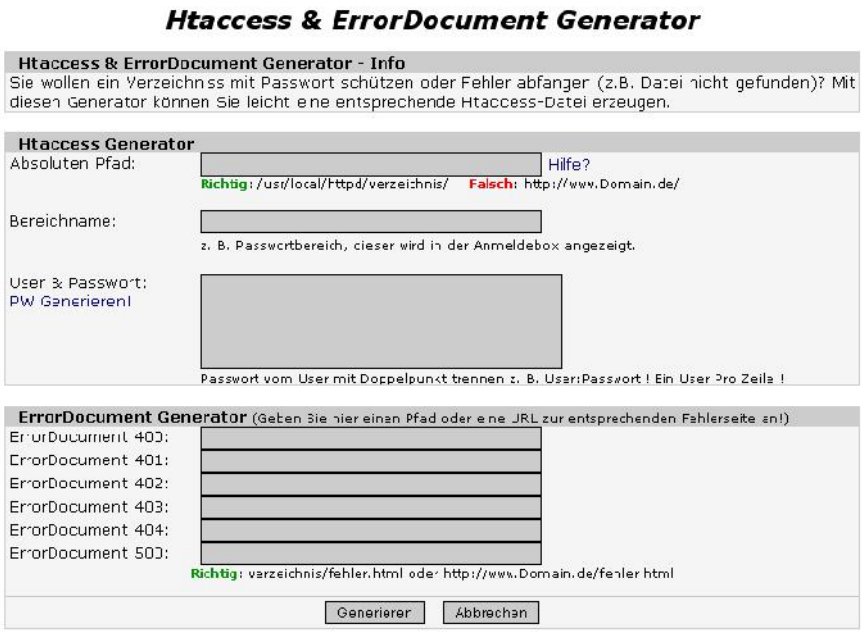
In der Benutzerdatei *.htusers* steht zunächst der Benutzername, gefolgt vom dazugehörigen Passwort. Beachten Sie, dass die Passwörter auf Ihrem Linux-System verschlüsselt gespeichert werden.

Auch wenn der Passwortschutz einfach zu realisieren ist, sollten Sie dennoch einige Dinge beachten. So werden der Benutzername und das Passwort bei der htaccess-Passwortschutz-Methode unverschlüsselt über die Internetleitung übertragen. Achten Sie außerdem darauf, dass die .htaccess-Konfigurationsdatei außerhalb des Lese- und Schreibzugriffes liegen muss.

Für das Erstellen des Passworts steht Ihnen unter Linux und Windows das Tool *htpasswd* zur Verfügung. Sie führen es wie folgt aus:

- **Linux**: */opt/lampp/bin/htpasswd*
- **Windows**: *C:\xampp\apache\bin\htpasswd.exe*

Wenn Ihnen das Hantieren mit der .htaccess-Datei zu fehleranfällig und zu komplex ist, greifen Sie doch einfach zum Htaccess & ErrorDocument Generator (*http://www.ekiwi.de/ tools/htaccess/index.php*). Mit diesem Angebot schließen Sie auch Syntaxfehler aus.



Mit diesem Generator wird das Erzeugen von .htaccess-Dateien zum Kinderspiel.

Eine weitere gängige Anwendung der .htaccess-Datei ist das Weiterleiten. Ein Beispiel verdeutlicht, wie einfach Sie einen Besucher von einer Site A auf eine Site B weiterleiten können:

```
# Weiterleitung htaccess

# Weiterleitung von Site_A.de zur Site_B.de

Redirect / http://www.site_B.de/site_A.de/
```

Wichtig ist dabei, dass sich die .htaccess-Datei im Stammverzeichnis der Site befindet, von der aus die Besucher auf eine andere Internet-Adresse umgeleitet werden sollen.

Zwei letzte Beispiele zeigen, wie flexibel die .htaccess ist. Wie bereits erwähnt, können Sie auch Benutzer von Ihrer Website fernhalten. Die nachfolgende Definition sorgt dafür, dass nur Benutzer mit der hier hinterlegten IP-Adresse auf den Server zugreifen dürfen. Alle anderen werden abgelehnt. Und so sieht eine entsprechende Konfiguration aus:

```
order deny,allow
allow from 192.168.1.200
deny from all
```

Auch das Sperren von Dateien ist möglich. Diese Funktion sorgt dafür, dass bestimmte, den Kriterien entsprechende Dateien nicht vom Server ausgeliefert werden. Die folgende Konfiguration verhindert das Ausliefern von Dateien, die mit einem Punkt beginnen:

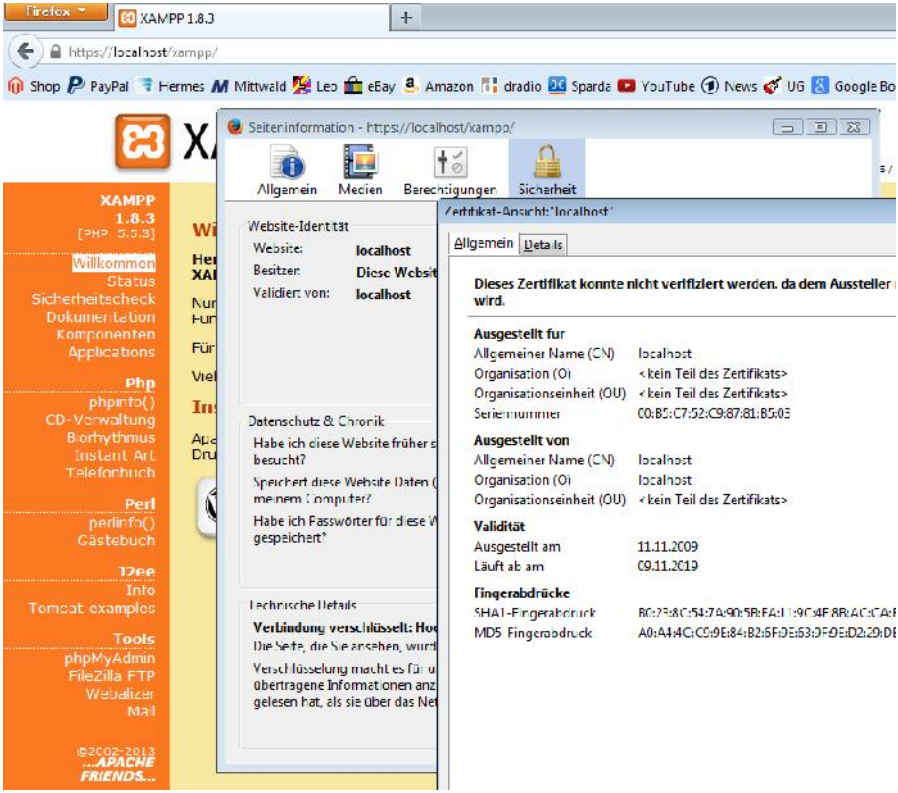
```
<FilesMatch "^\." >
deny from all
</FilesMatch>
```

2.3 Sicherer Zugriff dank SSL

Wenn Sie die Kommunikation zwischen dem Webbrowser und Ihrer XAMPP-Installation gegen Attacken von Dritten absichern wollen, so ist SSL die Standardtechnologie hierfür. Sie sollte beispielsweise beim Betrieb eines Online-Shops, aber auch bei allen anderen kritischen Bereichen verwendet werden.

Standardmäßig kommt Ihre XAMPP-Installation auch mit SSL-Unterstützung daher. Das zeigt sich etwa beim Starten der XAMPP-für-Linux-Installation, wie Sie der Meldung *Starten von SSL* entnehmen können. Auch bei der Windows-Variante ist die SSL-Unterstützung aktiviert.

Einziges Problem: Sie taugt nicht für den Produktionseinsatz. Das zeigt der Zugriff auf den Server mit Ihrem Browser. Öffnen Sie dazu die URL *https://localhost_bzw_ip-adresse*. Ihr Browser weist Sie darauf hin, dass das von Ihrer XAMPP-Installation, genauer dem Apache-Modul *mod_ssl* bereitgestellte Zertifikat abgelaufen ist. Es handelt sich um ein Demo-Zertifikat, das die Entwickler dem XAMPP-Paket beigelegt haben.



XAMPP kommt standardmäßig mit SSL-Unterstützung daher, allerdings mit einem unsicheren Zertifikat.

Was aber tun, wenn Sie nun ein gültiges Zertifikat für Ihren Einsatzbereich benötigen? Das Trustcenter (*http://www.trustcenter.de/products/true_businessid.htm*) ist einer der wenigen deutschen Anbieter, bei dem Sie ein solches bekommen können. Die Preise beginnen übrigens pro Lizenz und Jahr bei ca. 100 EUR.

Bevor Sie sich nun zum nächsten Anbieter aufmachen, sollten Sie zunächst die relevanten Konfigurationsdateien und Funktionen Ihres Systems kennen. Jede SSL-Installation verfügt über sechs Dateien, mit denen Sie alle relevanten Funktionen bzw. Einstellungen abdecken:

- **openssl**: Die OpenSSL-Implementierung, mit der Sie ein selbst signiertes Zertifikat bzw. eine PKCS#10-CSR-Datei für einen Zertifikatanbieter erstellen können. Sie finden das Tool in folgendem Verzeichnis:

  - Linux: /opt/lampp/bin/
  - Windows: C:\xampp\apache\bin\

- **mod_ssl.so**: Das Apache-SSL-Modul, das für die gesicherte Kommunikation mit dem Client sorgt. Sie finden das Modul in folgenden Verzeichnissen:
  - Linux: /opt/lampp/modules/
  - Windows: C:\xampp\apache\modules\

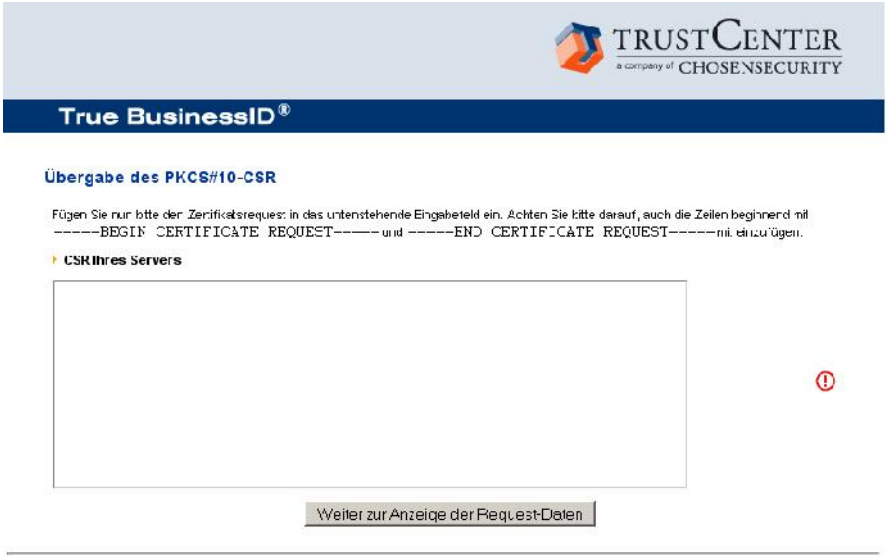
- **openssl.conf**: Dies ist die OpenSSL-Konfigurationsdatei. Sie finden die Datei in folgenden Verzeichnissen:
  - Linux: /opt/lampp/etc/
  - Windows: C:\xampp\apache\bin\

- **httpd-ssl.conf**: Das ist die Konfiguration für das Apache-SSL-Modul. Sie finden die Konfigurationsdatei in folgenden Verzeichnissen:
  - Linux: /opt/lampp/etc/extra/
  - Windows: C:\xampp\apache\conf\extra\

- **ssl.crt**: Das Verzeichnis, in dem alle Zertifikate liegen. Sie finden die Zertifikate in folgenden Verzeichnissen:
  - Linux: /opt/lampp/etc/
  - Windows: C:\xampp\apache\conf\

- **ssl.key**: Hier werden die Server-Schlüssel abgelegt. Sie finden das Tool in folgendem Verzeichnis:
  - Linux: /opt/lampp/bin/
  - Windows: C:\xampp\apache\bin

Ob Sie nun ein selbst signiertes oder ein offizielles Zertifikat erstellen wollen, ist zunächst zweitrangig, denn der Weg dahin ist fast identisch. Sie erzeugen mithilfe von OpenSSL das benötigte Zertifikat. Einziger Unterschied: Bei einem offiziellen Zertifikat übergeben Sie die PKCS#10-CSR-Datei dem Dienstleister. Eine sehr detaillierte Beschreibung finden Sie auf der Website des DFN (Deutsches Forschungsnetz) unter *https://www.pki.dfn.de/fileadmin/PKI/anleitungen/Anleitung_Nutzung_OpenSSL.pdf*).



Wenn Sie ein „echtes“ Server-Zertifikat benötigen, müssen Sie die PKCS#10-CSR-Datei dem jeweiligen Anbieter, hier dem TrustCenter, übergeben.

Nach dem Erhalt des Server-Zertifikats müssen Sie es lediglich im Zertifikat-Ordner ablegen.

2.4 Zugriff per WebDAV

Eine weitere Besonderheit des Apache-Webservers ist seine Unterstützung von WebDAV (Web-based Distributed Authoring and Versioning). Das ist ein offener Standard, der die Bereitstellung und Bearbeitung von Dateien im Internet erlaubt. In der Praxis können Benutzer auf ihre Daten wie auf eine Online-Festplatte zu-

greifen. Daher wird WebDAV gerade auch von professionellen Web-Editoren, wie Dreamweaver & Co., unterstützt, da man Daten online bearbeiten kann. Sie können auch von Windows XP auf einen WebDAV-Ordner zugreifen.

Vom technischen Standpunkt her handelt es sich bei WebDAV um eine Erweiterung des Protokolls HTTP/1.1, die bestimmte Einschränkungen von HTTP aufhebt. So kann man mit WebDAV beispielsweise ganze Verzeichnisse übertragen. Auch die Versionskontrolle ist implementiert – ein nicht ganz unwichtiges Feature, wenn mehrere Personen an einer Website arbeiten.

Eine der zentralen Vorteile von WebDAV ist die Verwendung des standardmäßigen HTTP-Ports. Dadurch kann das Protokoll auch verwendet werden, wenn sich zwischen zwei Rechnern eine Firewall befindet. Bei anderen Übertragungsmethoden, wie FTP oder SSH müssen oft zusätzlich Ports der Firewall freigeschaltet werden. Das wiederum erhöht das Sicherheitsrisiko.

Sicher ahnen Sie es schon: Ja, Ihre XAMPP-Installation ist WebDAV-ready. Sie können sozusagen direkt mit ihr loslegen. Wenn Sie mit Ihrem Browser auf die URL *http://localhost_bzw_ip-adresse/webdav/* zugreifen, landen Sie auf der WebDAV-Testseite.

In der aktuellen XAMPP-Version müssen Sie eigentlich nichts Besonderes beachten, denn die WebDAV-Umgebung ist direkt einsatzbereit. Das war bei früheren XAMPP-Versionen nicht immer so.

Die Konfiguration der WebDAV-Funktionalität erfolgt über die Apache- und über die WebDAV-Konfigurationsdatei. Stellen Sie in der *httpd.conf* sicher, dass die WebDAV-Konfigurationsdatei eingebunden ist. Stellen Sie außerdem sicher, dass die relevanten Module verfügbar sind.

Hier ein Beispiel für eine typische WebDAV-Konfigurationsdatei unter Windows:

```
#
# Beispiel-WebDAV-Konfiguration
#
<IfModule dav_module>
<IfModule dav_fs_module>
<IfModule setenvif_module>
<IfModule authn_file_module>

DavLockDB "C:/xampp/tmp/DavLock"
Alias /webdav "C:/xampp/webdav"
```

```
<Directory "C:/xampp/webdav">
    Dav On
    Order allow,deny
    Allow from all
    AuthName DAV-upload

    # Mit htdigest können Sie ein Datenbankpasswort
    # erstellen:
    # \xampp\apache\bin\htdigest -c
    # "\xampp\security\htpasswd.webdav" "XAMPP mit WebDAV"
    # user
    # AuthType Digest
    # AuthDigestDomain / http://localhost/

    # Hier ein Passwort mit htpasswd und md5
    # \xampp\apache\bin\htpasswd -b
\xampp\security\htpasswd.webdav user
    AuthType Basic
    AuthUserFile "C:/xampp/security/htpasswd.webdav"

       <LimitExcept GET HEAD OPTIONS>
        require valid-user
       </LimitExcept>
</Directory>
BrowserMatch "Microsoft Data Access Internet Publishing Pro-
vider" redirect-carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
BrowserMatch "MSIE" AuthDigestEnableQueryStringHack=On
```

```
</IfModule>
</IfModule>
</IfModule>
</IfModule>
```

Wenn Sie voranstehende Konfigurationsdatei aufmerksam prüfen, werden Sie feststellen, dass die WebDAV-Implementierung zwei Authentifizierungsverfahren unterstützt:

- Digest
- .htaccess

Meist verwendet man die .htaccess-Variante. Die Passwortdatei liegt bei einer Windows-Installation im Verzeichnis *C:\xampp\security\htpasswd.webdav*.

Der Zugriff auf den WebDAV-Ordner.

In der Standardkonfiguration ist bereits ein WebDAV-Benutzer angelegt. Seine Daten:

- **Kennung**: wampp
- **Passwort**: xampp

Sie können mit dieser Kennung also direkt loslegen und auf den WebDAV-Ordner zugreifen. Besonders einfach ist das, wenn Sie mit einem Windows-XP-Client auf den Ordner zugreifen wollen. Öffnen Sie dazu den Windows Explorer, markieren Sie den Arbeitsplatz mit der rechten Maustaste und führen Sie den Befehl *Netzwerklaufwerk verbinden* aus. In dem zugehörigen Dialog weisen Sie dem neuen Laufwerk einen Buchstaben zu und geben die Server- und Verzeichnisadresssen an. Die kann beispielsweise *\\localhost_bzw_ip-adresse\webdav* lauten.

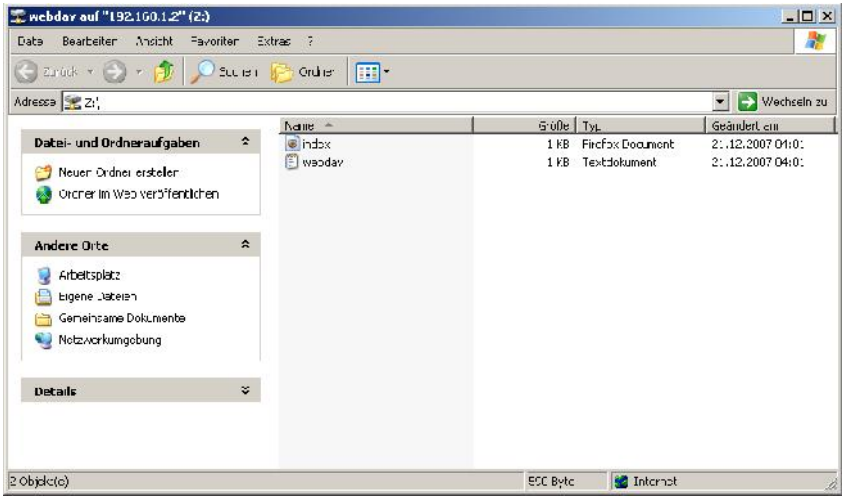
Folgen Sie außerdem dem Link *Anderen Benutzernamen* und geben Sie in den Dialog *Verbinden als …* die Kennung *wampp* und das Passwort *xampp* an. Mit einem Klick auf *Fertigstellen* öffnet sich ein weiterer Dialog, in dem Sie erneut die Kennung angeben müssen. Bestätigen Sie mit *OK*, und die Verbindung wird hergestellt.

Ohne eine netzwerkweite Freigabe funktioniert der WebDAV-Zugriff nicht.

Achtung:

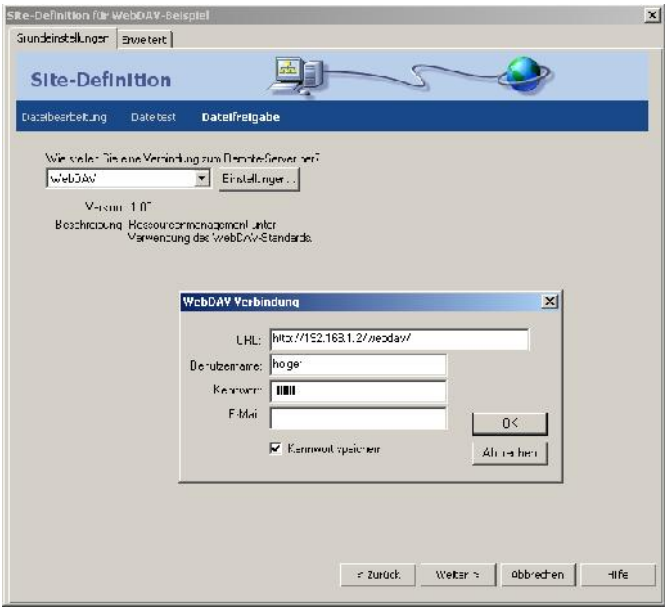
Bei den meisten Anwendern scheitert der Zugriff aus einem einfachen Grund: Sie haben den WebDAV-Ordner nicht freigegeben. Ohne eine Freigabe ist allerdings auch kein Zugriff per WebDAV möglich.

Wenn der Zugriff gelingt, präsentiert Ihnen der Windows Explorer den Inhalt des WebDAV-Verzeichnisses und Sie können sich nun an das Bearbeiten der Dateien machen.

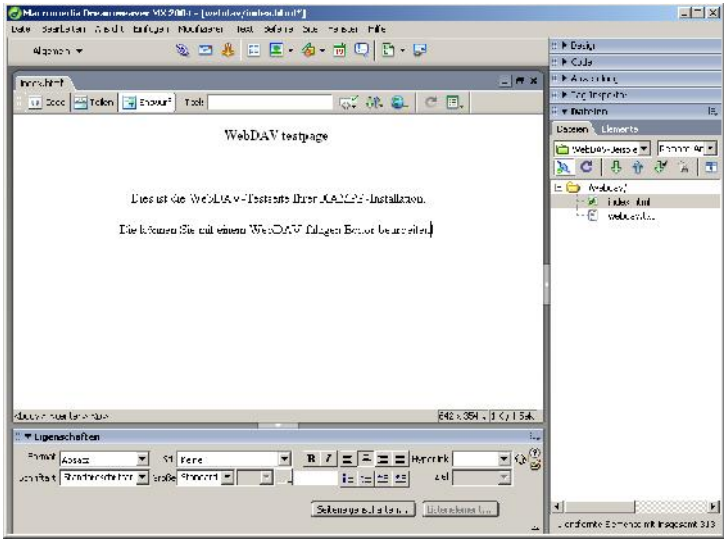


Der geöffnete WebDAV-Ordner im Windows Explorer.

Einer der wichtigsten Einsatzbereiche von WebDAV ist das Bearbeiten von Web-Seiten aus der Ferne. Wie bereits erwähnt, unterstützen gängige Web-Editoren das Remote-Bearbeiten von Web-Seiten. So auch Dreamweaver. Bei der Definition einer neuen Site können Sie den Zugriffstyp WebDAV verwenden und müssen über die WebDAV-Einstellungen nur noch die Adresse des freigegebenen Verzeichnisses, den Benutzernamen und das Passwort angeben. Schon können Sie die entfernten Dokumente mit dem lokalen Editor bearbeiten.



Die Site-Definition von Dreamweaver unterstützt den WebDAV-Zugriff.



Das Bearbeiten der WebDAV-Testseite mit Dreamweaver.

2.5 Virtuelle Hosts

Das Thema Virtual Hosts ist der Themenkomplex, an dem erfahrungsgemäßig das größte Interesse besteht. Als Virtual Hosts oder zu Deutsch virtueller Host bezeichnet man einen Server, auf dem mehrere Web-Auftritte gehostet, also bereitgestellt, werden. Auch ihre lokale XAMPP-Konfiguration kann auf einem Rechner mehrere Web-Anwendungen bereitstellen. Alles, was Sie dafür wissen müssen, verrät Ihnen dieser Abschnitt.

Man unterscheidet bei den virtuellen Hosts zwischen zwei Typen: Der Eine besitzt eine IP, der Andere ist namensbasiert, wobei einer IP-Adresse mehrere Hostnamen zugewiesen werden können. Der Anwender bekommt von all dem im Übrigen nichts mit. Für ihn ist es gleich, ob ein Web-Angebot auf dem einen oder dem anderen Typ basiert. Worin liegen nun genau die Unterschiede und wann ist die Nutzung der einen oder anderen Variante sinnvoll?

Bei den IP-basierten virtuellen Hosts wird die IP-Adresse der Verbindung verwendet, um den korrekten virtuellen Host zu ermitteln, damit dieser die Anfrage verarbeiten kann. Damit ist klar: Sie benötigen eine IP-Adresse für jeden virtuellen Host.

Anders ist das bei namensbasierten virtuellen Hosts. Bei dieser Variante verlässt sich der Server darauf, dass der Client den Hostnamen als Bestandteil des HTTP-Headers angibt. Mithilfe dieser Technik können Sie mehrere verschiedene Hosts auf der gleichen IP-Adresse unterbekommen.

In der Regel ist die Konfiguration von namensbasierten virtuellen Hosts einfacher. Das Einzige, was es zu beachten gilt: Sie müssen Ihren DNS-Server entsprechend konfigurieren, so dass auf jedem Hostnamen die richtige IP-Adresse abgebildet wird. Im nächsten Schritt konfigurieren Sie den Apache-Server so, dass er die verschiedenen Hostnamen erkennt.

Ein weiterer Vorteil namensbasierter Hostnamen ist, dass sich der hohe Bedarf an knappen IP-Adressen ein wenig entschärft. Zwar stößt IPv6 hier in ganz andere Dimensionen vor, doch das Internet ist nach wie vor IPv4-dominiert. Auch aus diesem Grund – und der vergleichsweise einfachen Konfiguration – spricht in der Regel alles für die Verwendung von namensbasierten virtuellen Hosts.

Doch es gibt auch Gründe, die für den Einsatz von IP-basierten virtuellen Hosts sprechen. Einer hierfür ist: Verschiedene antiquierte Clients sind nicht mit namensbasierten virtuellen Hosts kompatibel. Wie Sie im übernächsten Abschnitt noch sehen werden, gibt es hierfür aber auch eine einfache Lösung.

Namensbasierte virtuelle Hosts unterliegen einer Einschränkung: Sie können wegen der SSL-Protokolleigenschaften nicht mit SSL-gesicherten Servern verwendet

werden. Wenn Sie also Ihre Verbindungen per SSL absichern wollen, sind auch hier IP-basierte Hosts die richtige Wahl.

Der Apache verwendet die folgenden Konfigurationsdirektiven für die Konfiguration von virtuellen Hosts:

- <VirtualHost>
- NameVirtualHost
- ServerName
- ServerAlias
- ServerPath

Schauen wir uns als Nächstes an, wie Sie die beiden Host-Typen anlegen.

2.5.1 Namensbasierte virtuelle Hosts

Wenn Sie einen namensbasierten virtuellen Host verwenden wollen, müssen Sie die IP-Adresse (womöglich auch den Port) des Servers spezifizieren, an welche die Client-Anfragen übermittelt werden.

Hierfür verwenden Sie die Direktive *NameVirtualHost*. Sollen alle IP-Adressen des Servers verwendet werden, benutzen Sie hier ein Sternchen als Argument. Sollten Sie mehrere Ports einsetzen wollen, um beispielsweise auch SSL nutzen zu können, sollten Sie das Argument um die Port-Angabe ergänzen.

Beachten Sie, dass die Angabe einer IP-Adresse in einer *NameVirtualHost*-Direktive den Server nicht automatisch an dieser Adresse lauschen lässt. Außerdem ist für jede angegebene IP-Adresse eine Netzwerkkarte des Servers erforderlich.

Als Nächstes erstellen Sie für jeden Host einen <*VirtualHost*>-Block. Beachten Sie, dass das Argument der Direktive <*VirtualHost*> das Gleiche wie das Argument der *NameVirtualHost*-Anweisung sein soll. Konkret heißt das: Sie verwenden eine IP-Adresse oder das Sternchen für alle Adressen.

Sie müssen innerhalb jedes <*VirtualHost*>-Blocks mindestens eine *ServerName*-Anweisung anlegen, mit der Sie festlegen, welcher Host bedient wird. Eine weitere wichtige Angabe: die *DocumentRoot*-Anweisung. Mit ihr legen Sie fest, wo im Dateisystem der Inhalt des Hosts abgelegt wird.

Ganz wichtig ist außerdem Folgendes: Wenn Sie – wie in unserem Fall – einen virtuellen Host zu einem bestehenden Webserver hinzufügen wollen, müssen Sie auch einen <*VirtualHost*>-Block für den bestehenden Host erstellen.

Beachten Sie dabei, dass die *ServerName*- und *DocumentRoot*-Anweisungen zu diesem virtuellen Host die gleichen sein sollten, wie die globalen *ServerName*- und *DocumentRoot*-Anweisungen. Der virtuelle Host sollte außerdem als Erstes in der Konfigurationsdatei aufgeführt werden, damit er als Standard-Host agiert.

Ein konkretes Beispiel: Wenn Sie die Domain *www.domain1.de* verwenden, dieser den virtuellen Host *www.domain2.de* hinzufügen und beide die gleiche IP-Adresse besitzen, so müssen Sie folgende Konfiguration in die Apache-Konfigurationsdatei schreiben:

```
NameVirtualHost *:80

<VirtualHost *:80>
ServerName www.domain1.de
ServerAlias domain1.de *.domain1
DocumentRoot /www/domain1
</VirtualHost>

<VirtualHost *:80>
ServerName www.domain2.de
DocumentRoot /www/domain2
</VirtualHost>
```

Statt der Sternchen können Sie bei den beiden Anweisungen *NameVirtualHost* und <*VirtualHost*> auch eine eindeutige IP-Adresse hinterlegen.

Wenn Sie einen Server anlegen wollen, der unter mehr als einem Hostnamen erreichbar ist, so verwenden Sie hierfür die Direktive *ServerAlias*. Sie wird innerhalb des <*VirtualHost*>-Abschnittes angegeben.

Dann kann beispielsweise die *ServerAlias*-Anweisung in den ersten <*VirtualHost*>-Block verweisen, damit die aufgeführten Namen alternative Namen sind. Konkret sieht die Konfiguration dann wie folgt aus:

```
ServerAlias server1.de *.server.de
```

Das bedeutet, dass die Anfragen für alle Hosts der Domain *server1.de* von dem virtuellen Host *www.server.de* bedient werden. Sie können dabei die beiden Platzhalter * und ? anstelle entsprechender Namen verwenden.

Nachdem Sie diese Grundkonfiguration angelegt haben, können Sie die Konfiguration der virtuellen Hosts mithilfe weiterer Direktiven innerhalb des <*VirtualHost*>-Containers verfeinern.

2.5.2 IP-basierte virtuelle Hosts

Wenn Sie sich für die IP-basierte virtuelle Host-Variante entscheiden, müssen Sie für jeden virtuellen Host eine IP-Adresse besitzen. In der Praxis bedeutet das, dass Sie für jede Adresse einen Netzwerkadapter benötigen. Sollte der Rechner nicht über die benötigte Anzahl an Netzwerkkarten verfügen, können Sie aber auch virtuelle Netzwerkschnittstellen verwenden. Man spricht auch von IP-Aliasing.

Da Sie sich vermutlich eher für die namensbasierte Variante entscheiden, soll nur anhand eines einfachen Beispiels gezeigt werden, wie die Konfiguration der IP-basierten virtuellen Hosts aussehen kann.

Nehmen wir an, Ihr Hostings-System besitzt drei Netzwerkadapter und Sie haben diesen die IP-Adressen *192.168.1.1* bis 1*92.168.1.3* zugewiesen. In diesem Fall könnte Ihre Konfiguration wie folgt aussehen:

```
<VirtualHost 192.168.1.2>
       ServerName www.beispiel.de
       DocumentRoot /xampp/htdocs/beispiel1.de
       ServerAdmin webmaster@beispiel1.de
       ErrorLog /xampp/apache/www.beispiel1.de-error_log
       CustomLog /xampp/apache/www.beispiel1.de-access_log
common
</VirtualHost>


<VirtualHost 192.168.1.3>
       ServerName www.beispiel2.de
       DocumentRoot /xampp/htdocs/beispiel2.de
       ServerAdmin webmaster@beispiel2.de
       ErrorLog /xamp/apache/www.beispiel2.de-error_log
```

```
    CustomLog /xampp/apache/www.beispiel2.de-access_log
common
</VirtualHost>
```

In diesem Beispiel sind nur für die beiden zusätzlichen IP-Adressen (also nicht für 192.168.1.1) die VirtualHost-Direktiven spezifiziert.

Bei der Apache-Konfiguration steckt der Teufel häufig im Detail. Schon kleine Unsauberkeiten können Ihre Konfiguration aushebeln oder dafür sorgen, dass nichts mehr geht. Bei der Suche von Fehlern in Virtual-Host-Konfigurationen ist die Apache-Befehlszeilenoption *-S* oftmals eine große Hilfe. Verwenden Sie dazu den folgenden Befehl:

```
/xampp/apache/bin/httpd -S
```

Der Apache liefert Ihnen eine Beschreibung, wie er die Konfigurationsdatei analysiert hat. Eine sorgfältige Überprüfung der IP-Adressen und Servernamen ist meist hilfreich, um Konfigurationsfehler aufzudecken.

2.5.3 Beispiele für typische Konfigurationen

Anhand einiger Beispiele wird deutlich, wie Sie typische Konfigurationen in der Praxis umsetzen. Eine der gängigsten Konfigurationsvarianten ist die Ausführung von mehreren namensbasierten Websites auf einer einfachen IP-Adresse.

Ihr Server besitzt dabei eine IP-Adresse und mehrere Aliase (CNAMES). Sie betreiben also beispielsweise die Webserver *www.server.de* und *www.firma.de* auf einem System.

Hier ein Beispiel für eine derartige Konfiguration

```
# Stellt sicher, dass der Apache auf Port 80 hört
Listen 80

# Stellt sicher, dass der Server für alle virtuellen Host-
# Requests an allen Ports hört.
NameVirtualHost *:80

<VirtualHost *:80>
```

```
DocumentRoot /htdocs/server
ServerName www.server.de
# Weitere Direktiven hier
</VirtualHost>

<VirtualHost *:80>
DocumentRoot /htdocs/firma
ServerName www.firma.de
# Weitere Direktiven hier
</VirtualHost>
```

Der Platzhalter steht für alle Adressen und der Haupt-Server bedient keine Requests. Beachten Sie auch, dass durch die Reihenfolge der Einträge auch die Priorität bestimmt wird. Sie können den ersten Eintrag auch als primären Webserver verstehen.

Sie können das Sternchen auch durch die tatsächliche IP-Adresse des Hosting-Systems ersetzen. In diesem Fall muss das *VirtualHost*-Argument allerdings auch dem *NameVirtualHost*-Eintrag entsprechen. Ein Beispiel:

```
NameVirtualHost 191.168.1.10

<VirtualHost 191.168.1.10>
# ...
```

Die Verwendung des Platzhalters macht insbesondere dort Sinn, wo dem Hosting-Server keine feste IP-Adresse zugewiesen wird.

Wenn Sie virtuelles Hosting in einer namensbasierten Umgebung verwenden, ist das die richtige Variante. Beachten Sie allerdings, dass diese Konfiguration nicht funktionieren wird, wenn Sie verschiedene Content-basierte Server mit unterschiedlichen IP-Adressen oder Ports verwenden wollen.

Schauen wir uns als Nächstes namensbasierte Hosts auf mehr als einer IP-Adresse an. In nachstehender Beispielkonfiguration besitzt der Server zwei IP-Adressen. Dabei ist die Erste (*192.168.1.1*) die Haupt-Adresse mit *server.domain.de*, die andere IP-Adresse (*192.168.1.2*) hostet zwei oder mehr virtuelle Hosts:

```
Listen 80

# Der “Haupt-Server” ist unter 192.168.1.2 erreichbar
ServerName server.domain.de
DocumentRoot /htdocs/hauptserver

# Die zweite IP-Adresse
NameVirtualHost 192.168.1.2

<VirtualHost 192.168.1.2>
DocumentRoot /htdocs/server1
ServerName www.server.de
# Weitere Direktiven hier
</VirtualHost>

<VirtualHost 191.168.1.2>
DocumentRoot /htdocs/server2
ServerName www.server.de
# Weitere Verzeichnisse hier
</VirtualHost>
```

Alle Anfragen, die nicht an *192.168.1.2* gerichtet werden, werden von dem Haupt-Server bedient. Ein Request an *192.168.1.2* mit unbekanntem Hostnamen oder keinem Host-Header wird, von *www.server.de* verarbeitet.

Dank der virtuellen Host-Funktionen können Sie noch eine Vielzahl weiterer interessanter Einstellungen vornehmen. Sie können die gleichen Inhalte über verschiedene IP-Adressen verfügbar machen und dabei beispielsweise eine interne und eine externe Adresse verwenden.

Nehmen wir an, Ihr Server besitzt die beiden IP-Adressen *192.168.1.1* und *204.20.10.40*. Das System sitzt an der Schnittstelle zwischen lokalem und globalem Netzwerk. Für die Clients, die von außen auf den Server zugreifen, hat der Server die IP-Adresse *204.20.10.40*, für die internen Clients die Adresse *192.168.1.1*.

Um die gleichen Inhalte für interne und externe Requests bereitzustellen, verwenden Sie eine einfache Konfiguration in der VirtualHost-Sektion. Die sieht wie folgt aus:

```
NameVirtualHost 192.168.1.1
NameVirtualHost 204.20.10.40

<VirtualHost 192.168.1.1 204.20.10.40>
DocumentRoot /htdocs/server1
ServerName www.server1.de
ServerAlias server
</VirtualHost>
```

Sie können mithilfe der Virtual-Host-Funktionen auch mehrere Sites auf verschiedenen Ports ausführen. Wenn Sie mehrere Domains anlegen wollen, die auf die gleiche IP-Adresse zeigen, aber auf unterschiedlichen Ports zu finden sind, greifen Sie zur Direktive *NameVirtualHost*. Auch dazu ein einfaches Beispiel:

```
Listen 80
Listen 8080

NameVirtualHost 192.168.1.1:80
NameVirtualHost 192.168.1.1:8080

<VirtualHost 192.168.1.1:80>
ServerName www.server1.de
DocumentRoot /htdocs/server-80
</VirtualHost>

<VirtualHost 192.168.1.1:8080>
ServerName www.server1.de
DocumentRoot /htdocs/server-8080
</VirtualHost>
```

```
<VirtualHost 192.168.1.1:80>
ServerName www.server2.de
DocumentRoot /htdocs/andererserver-80
</VirtualHost>

<VirtualHost 192.168.1.1:8080>
ServerName www.server2.de
DocumentRoot /htdocs/andererserver-8080
</VirtualHost>
```

Schauen wir uns ein Beispiel für IP-basiertes virtuelles Hosting an. Der Server besitzt die beiden IP-Adressen *192.168.1.1* und *192.168.1.2*, die als Server-Namen *www.server1.de* und *www.server2.de* aufgelöst werden. Die entsprechende Konfiguration sieht wie folgt aus:

```
Listen 80

<VirtualHost 192.168.1.1>
DocumentRoot /www/server1
ServerName www.server1.de
</VirtualHost>

<VirtualHost 192.168.1.2>
DocumentRoot /www/server2
ServerName www.server2.de
</VirtualHost>
```

Alle Anfragen an Adressen, die nicht in der *VirtualHost*-Direktive definiert sind, also beispielsweise *localhost*, werden an den Haupt-Server übergeben, sofern ein Solcher angelegt ist.

Sie können auch Port- und IP-basierte virtuelle Hosts miteinander vermischen. Auch dazu ein Beispiel. Der Server besitzt wieder zwei IP-Adressen (*192.168.1.1* und *192.168.1.2*), die über die beiden Hostnamen *www.server1.de* und

www.server2.de aufgelöst werden. In beiden Fällen sollen die Hosts auf Port 80 und 8080 laufen.

Realisieren lässt sich eine solche Konfiguration mit folgenden Einstellungen:

```
Listen 192.168.1.1:80
Listen 192.168.1.1:8080
Listen 192.168.1.2:80
Listen 192.168.1.2:8080

<VirtualHost 192.168.1.1:80>
DocumentRoot /htdocs/server1-80
ServerName www.server.1
</VirtualHost>

<VirtualHost 192.168.1.1:8080>
DocumentRoot /htdocs/server1-8080
ServerName www.server1.de
</VirtualHost>

<VirtualHost 192.168.1.2:80>
DocumentRoot /htdocs/server2-80
ServerName www.server2.de
</VirtualHost>

<VirtualHost 192.168.1.2:8080>
DocumentRoot /htdocs/server2-8080
ServerName www.server2.de
</VirtualHost>
```

Sie können auch namens- und IP-basierte Hosts in einer Konfigurationsdatei mischen. Sollen einige Ihrer Adressen namens-, andere IP-basiert sein, so kann die Konfiguration hierfür wie folgt aussehen:

```
Listen 80

# namensbasierte Konfiguration
NameVirtualHost 192.168.1.1

<VirtualHost 192.168.1.1>
DocumentRoot /htdocs/server1
ServerName www.server1.de
</VirtualHost>

<VirtualHost 192.168.1.1>
DocumentRoot /htdocs/server2
ServerName www.server2.de
</VirtualHost>

<VirtualHost 192.168.1.1>
DocumentRoot /htdocs/server3
ServerName www.server3.de
</VirtualHost>

# IP-basierte Konfiguration
<VirtualHost 192.168.1.2>
DocumentRoot /htdocs/server4
ServerName www.server4.de
</VirtualHost>

<VirtualHost 192.168.1.3>
DocumentRoot /htdocs/server5
ServerName www.server5.de
</VirtualHost>
```

Zwei letzte Beispiele möchte ich Ihnen noch vorstellen. Mit der *VirtualHost*-Direktive können Sie einen namenbasierten virtuellen Host in einen IP-basierten virtuellen Host migrieren.

In diesem Beispiel wird dem namensbasierten Hostnamen *www.server1.de* eine eigene IP-Adresse zugewiesen. Um dabei Probleme mit Name-Server und Proxy-Server zu verhindern, der die alte IP-Adresse des namenbasierten virtuellen Hosts zwischenspeichert, sollten beide Varianten während der Migrationsphase angeboten werden.

Die Lösung ist in der Praxis recht einfach: Wir fügen einfach die neue IP-Adresse (*192.168.1.2*) der *VirtualHost*-Direktive hinzu.

Die Konfiguration sieht dann in der Praxis wie in nachstehendem Beispiel dargestellt aus:

```
Listen 80
ServerName www.server1.de
DocumentRoot /htdocs/server1

NameVirtualHost 192.168.1.1

<VirtualHost 192.168.1.1 192.168.1.2>
DocumentRoot /htdocs/server2
ServerName www.server2.de
# ...
</VirtualHost>

<VirtualHost 192.168.1.1>
DocumentRoot /htdocs/server3
ServerName www.server3.de
ServerAlias *.server3.de
# ...
</VirtualHost>
```

Mit dieser Konfiguration kann der virtuelle Host als IP-basierter Host (über die neue Adresse) und über die alte namensbasierte Adresse angesprochen werden.

Ein letztes Beispiel zeigt die Verwendung der *ServerPath*-Direktive. Bei namenbasierten virtuellen Hosts beruht sie auf der Auswertung des Anfrage-Headers *Host*. Dieser Header-Eintrag ist bei HTTP/1.1 vorgeschrieben und wird sogar von den meisten HTTP/1.0-Browsern gesendet. Allerdings senden einige alte Clients diesen Header nicht.

Um auch diesen Browsern den Zugriff zu erlauben, verwendet man die Direktive *ServerPath* setzen. Sie ermöglicht es, die URLs eines virtuellen Hosts in einem Unterverzeichnis eines anderen virtuellen Hosts abzubilden.

Auch dazu ein Beispiel, wie Sie für die Abbildung sorgen können und so auch sehr alten Browsern den Zugriff auf Ihre Inhalte erlauben:

```
NameVirtualHost 192.168.1.1


<VirtualHost 192.168.1.1>
# primary vhost
DocumentRoot /htdocs/subdomain
RewriteEngine On
RewriteRule ^/.* /htdocs/subdomain/index.html
# ...
</VirtualHost>

<VirtualHost 192.168.1.1>
DocumentRoot /htdocs/subdomain/sub1
ServerName www.sub1.domain.tld
ServerPath /sub1/
RewriteEngine On
RewriteRule ^(/sub1/.*) /htdocs/subdomain$1
# ...
</VirtualHost>

<VirtualHost 192.168.1.1>
```

```
DocumentRoot /htdocs/subdomain/sub2
ServerName www.sub2.domain.tld
ServerPath /sub2/
RewriteEngine On
RewriteRule ^(/sub2/.*) /htdocs/subdomain$1
# ...
</VirtualHost>
```

2.6 Außenanbindung mit DynDNS

Wenn Sie lokal ein Content-Managementsystem, einen Online-Shop oder eine andere Anwendung auf Ihrer XAMPP-Umgebung eingerichtet haben und diese auch über das Internet zugänglich machen wollen, dabei aber nicht über eine permanente Internet-Anbindung verfügen, sondern diese z. B. per DSL realisieren, so ist das über DynDNS möglich.

DynDNS oder auch DDNS (dynamischer Domain-Name-System-Eintrag) ist ein System, das in Echtzeit Domain-Name-Einträge aktualisiert. Dabei sollten Sie beachten, dass mit dem Begriff zwei verschiedene Varianten von Netzwerkdiensten gemeint sind:

- DNS-Dienst, der einen Aktualisierungsmechanismus für Hostnamen per Webinterface anbietet.
- DNS-Dienst, der einen Aktualisierungsmechanismus für DNS-Einträge anbietet.

Wenn Sie mit Ihrem lokalen Rechner eine Internet-Verbindung herstellen, so wechselt häufig die IP-Adresse, die Ihrem Rechner von Ihrem Provider zugeordnet wird. In welchem Adressbereich sich diese Adresse befindet und welche Adresse das ist, ist abhängig von der DNS-Konfiguration aufseiten Ihres Internet-Providers.

2.6.1 DynDNS-Basics

Das Domain Name System, kurz DNS, ist von Haus aus nicht dafür gerüstet, dass es mit ständig wechselnden Einträgen hantieren muss. DNS-Einträge sollten möglichst lange zwischengespeichert werden, am besten mehrere Stunden oder sogar Tage.

Um dennoch dynamische DNS-Einträge zu ermöglichen, verringert man einfach die maximale Speicherzeit (TTL = time to live) der DNS-Einträge erheblich, beispielsweise auf 60 Sekunden. Wichtig dabei ist, dass Sie prüfen, ob der verwendete Name-Server die Speicherzeit (TTL) tatsächlich korrekt wiedergibt. Dazu verwenden Sie das Tool *dig*. Unter Linux ist es standardmäßig verfügbar bzw. kann über einen Paketmanager leicht nachinstalliert werden. Wenn Sie mit einem Windows-System arbeiten, verwenden Sie das Dig-Tool, das Sie unter *http://members.shaw.ca/nicholas.fong/dig/* finden. Dem Answer-Abschnitt können Sie die Speicherzeit entnehmen.

Auch unter Mac OS X ist *dig* standardmäßig verfügbar.

Für das Aktualisieren eines DynDNS-Eintrags in den Nameservern verwendet man in der Regel einen DynDNS-Client. Dieser stellt bei einem IP-Adressen-Wechsel automatisch mit dem DynDNS-Server eine Verbindung her und übermittelt die neue IP-Adresse des lokalen Rechners an das DNS. Ein solcher Client ist über entsprechende Anbieter verfügbar. Allerdings besitzen auch die meisten aktuellen DSL-Router einen derartigen Client.

Ein weiteres Problem: Die meisten dieser Systeme bemerken das Offline-Gehen des Rechners nicht und daher bleibt die letzte IP-Adresse im DNS gespeichert. DynAccess, ein professioneller und kostenpflichtiger Service, löst dieses Problem

mit einem sogenannten Heartbeat. Dabei übermittelt der Client in regelmäßigen Abständen ein Signal zum DynAccess-Server, um diesem zu signalisieren, dass er noch aktiv ist. Bleibt das Signal aus, so setzt der DynAccess-Server die IP-Adresse auf eine Standard-Adresse zurück.

Bei verschiedenen DynDNS-Anbietern ist das temporäre Löschen des DNS-Eintrags möglich. Ein DynDNS-Client kann zum Beispiel beim Herunterfahren des Rechners die IP-Adresse des DynDNS-Eintrags löschen, sodass der DNS-Eintrag während der Offline-Zeit undefiniert ist und damit nicht auf die vorherige (mittlerweile obsolete) IP-Adresse zeigt.

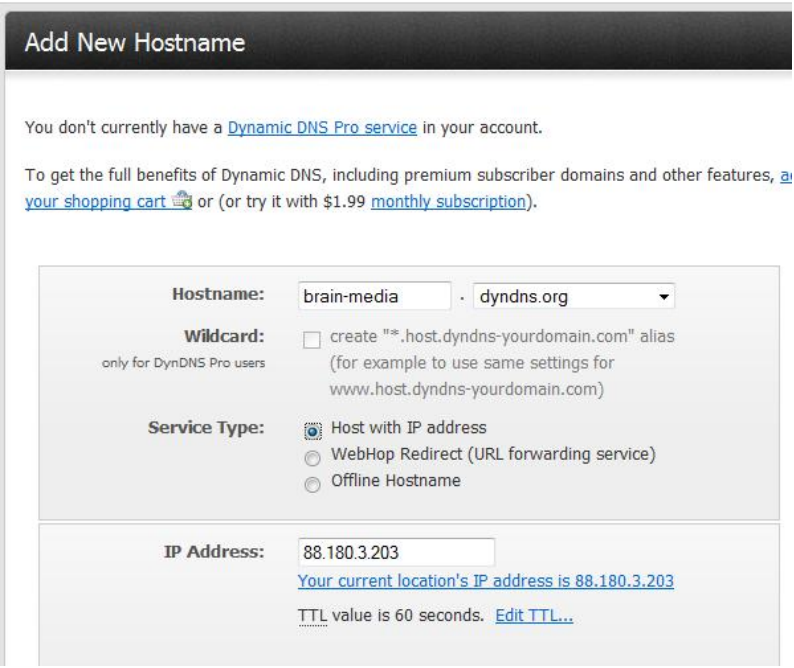
DynDNS ist zweifelsohne ein interessanter Ansatz, um ein lokales System internetweit verfügbar zu machen, aber ersetzen kann das System eine statische IP-Adresse nicht.

In der Praxis haben Sie bei der Nutzung mit DynDNS mit verschiedenen Problemen zu kämpfen. So bleiben offene Netzwerkverbindungen beim Offline-Gehen oder bei einem Wechsel der IP-Adresse hängen und brechen nach dem Timeout zusammen. Ein weiteres Problem: Innerhalb eines Zeitraums von bis zu 60 Sekunden, in dem der alte DynDNS-Hostname zwischengespeichert wird, können keine neuen Verbindungen zu dem Host aufgebaut werden.

2.6.2 DynDNS einrichten

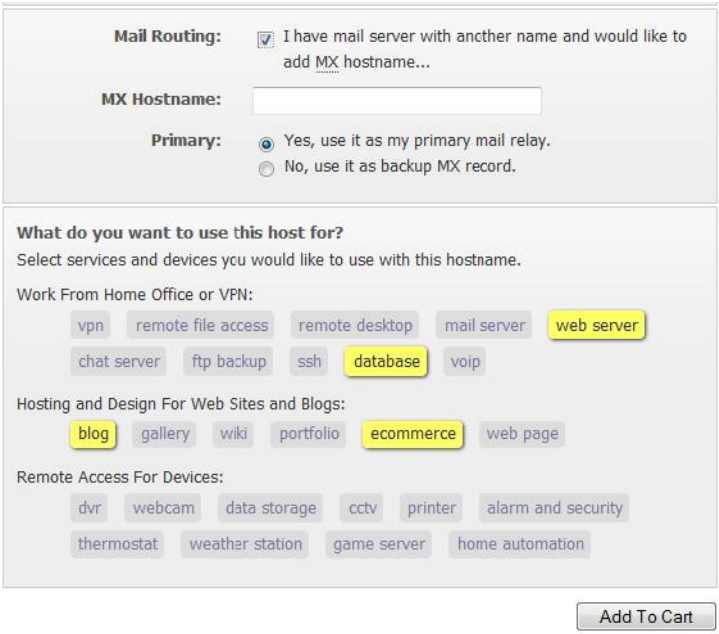
Es gibt verschiedene Anbieter von DynDNS-Services. Der bekannteste ist sicherlich DynDNS.org bzw. DynDNS.com, der unter den gleichnamigen URLs erreichbar ist. Hier stehen Ihnen verschiedene kostenpflichtige und eine kostenlos Variante zur Verfügung. Folgen Sie einfach dem Link *Get a Free Domain Name* und dann *Sign up FREE*.

In dem Formular *Add New Hostname* weisen Sie dem neuen Hostnamen eine Bezeichnung zu und wählen die gewünschte Domainbezeichnung aus. Die kann beispielsweise *IhrName.dyndns.org* oder *IhrName.dyndns-home.com* lauten.



Das Einrichten eines DynDNS-Accounts.

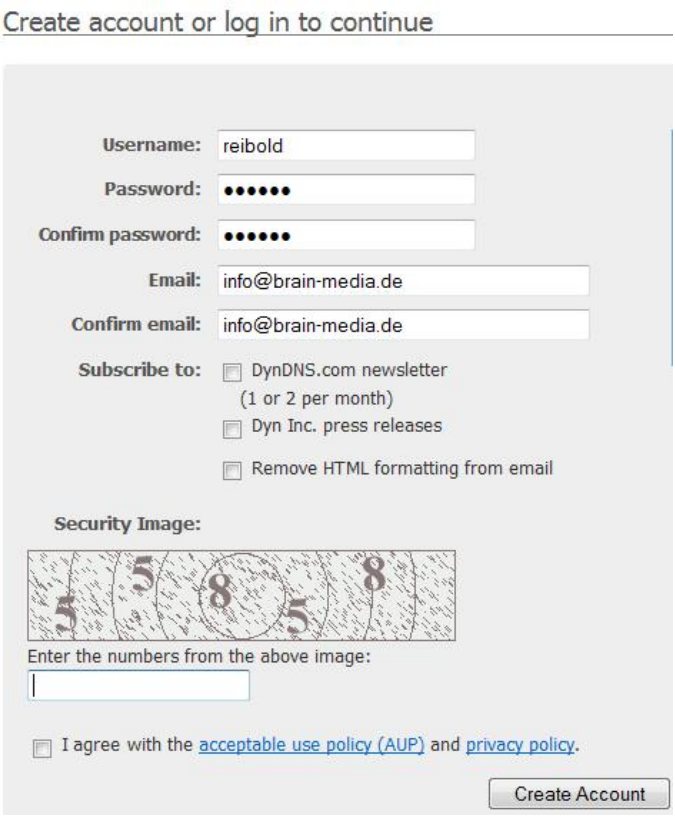
Wenn Sie sich für die Nutzung eines kommerziellen Angebots entscheiden, können Sie mit der Option *Wildcard* mehrere Rechner ansprechen. So werden beispielsweise die Rechner *Host1.IhrName.dyndns.org* und *Host2.IhrName.dyndns.org* von außen ansprechbar. Sinnvoll ist diese Funktion insbesondere dann, wenn Sie mehrere Nicht-IP-basierte virtuelle Hosts nutzen wollen. Unter *Service Type* ist die Option *Host with IP address* in der Regel die richtige Wahl. Sie können dabei auch direkt Ihre aktuelle IP-Adresse übernehmen.



Die Konfiguration der Dienstnutzung.

Als Nächstes können Sie durch Aktivieren der Option *Mail Routing* einen bestehenden Mailserver einbinden. Das ist nur dann erforderlich, wenn Sie einen Mailserver verwenden, der nicht auf dem Zielrechner läuft. Wenn Sie einen Mailserver betreiben, greifen Sie womöglich zu dem im XAMPP-Paket enthaltenen. In diesem Fall müssen Sie unter *Mail Routing* keine Einstellungen vornehmen.

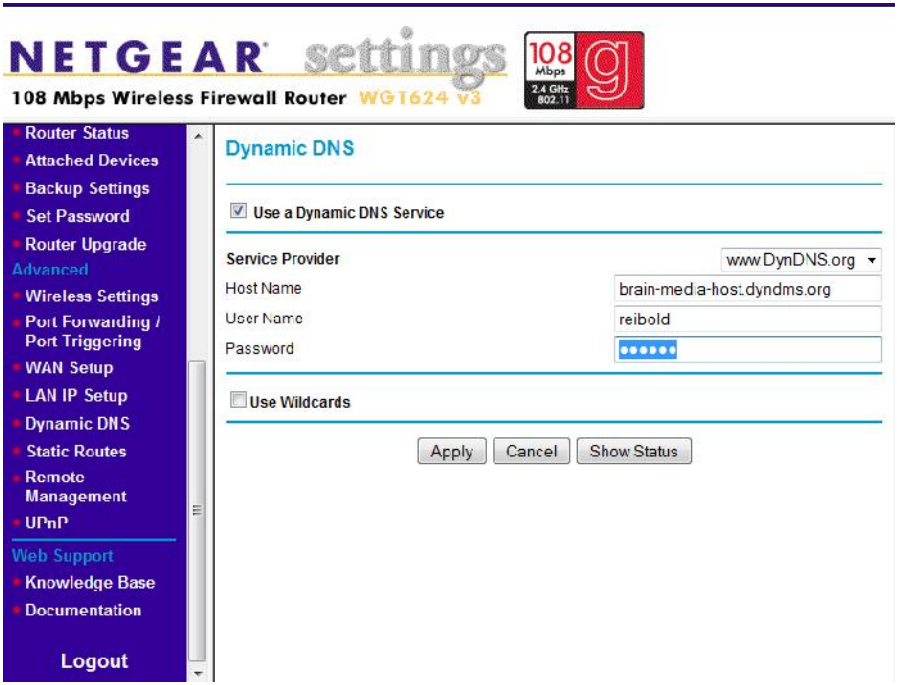
Dann bestimmen Sie, welche Services auf dem Zielsystem ausgeführt werden. Aktivieren Sie die gewünschten Dienste, indem Sie auf die jeweilige Schaltfläche klicken.



Das Anlegen des DynDNS-Accounts.

Der nächste Schritt dient dem Anlegen des DynDNS-Accounts. Geben Sie den gewünschten Benutzernamen, das Passwort und Ihre E-Mail-Adresse an. Sie müssen außerdem den Nutzungsbedingungen und Datenschutzbestimmungen zustimmen.

Mit einem Klick auf *Create Account* wird der Zugang angelegt. Sie erhalten eine E-Mail, in der Sie den Account bestätigen müssen. Wichtig ist außerdem, dass Sie den Check-out-Vorgang abschließen, um Ihren Eintrag zu aktivieren. Anschließend ist der DynDNS-Service verfügbar.



Die Router-Konfiguration

2.6.3 Router für DynDNS konfigurieren

Als Nächstes steht die Router-Konfiguration an. Da sich die IP Adresse ja alle x Stunden ändert, muss Ihr lokales System dem DynDNS-Dienst die neue IP-Adresse mitteilen. Moderne Router verfügen über ein entsprechendes Modul, wie an voranstehender Abbildung zu erkennen ist. Es handelt sich um einen Netgear-WLAN-Router. Bei anderen Geräten ist die Konfiguration ähnlich.

Im Falle des Netgear-Routers greifen Sie über die webbasierte Konfiguration auf die *Dynamic DNS*-Einstellungen zu.

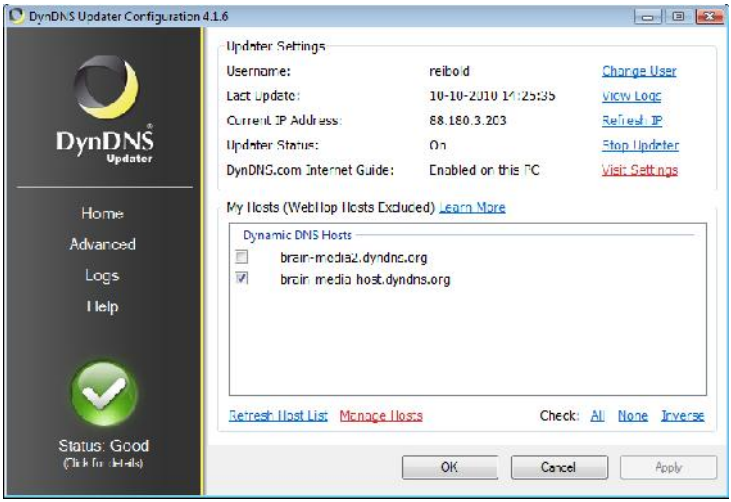
Der Rest ist einfach: Aktivieren Sie die DynDNS-Nutzung und wählen Sie aus dem Auswahlmenü *Provider* Ihren Anbieter aus. Füllen Sie außerdem die folgenden Felder mit den im DynDNS angelegten Einstellungen:

- Host Name
- User Name

- Password
- Use Wildcards

Nach dem Speichern der DynDNS-Einstellungen steht einer Nutzung des Dienstes nichts mehr im Wege.

Was aber tun, wenn der von Ihnen verwendete Router keine DynDNS-Einstellungen bietet? Das kann insbesondere bei älteren Routern vorkommen. In diesem Fall stehen Ihnen zwei Wege offen: Sie passen die Systemkonfiguration manuell an oder aber Sie greifen zu einem speziellen Update-Tool.



Der DynDNS-Updater in Aktion.

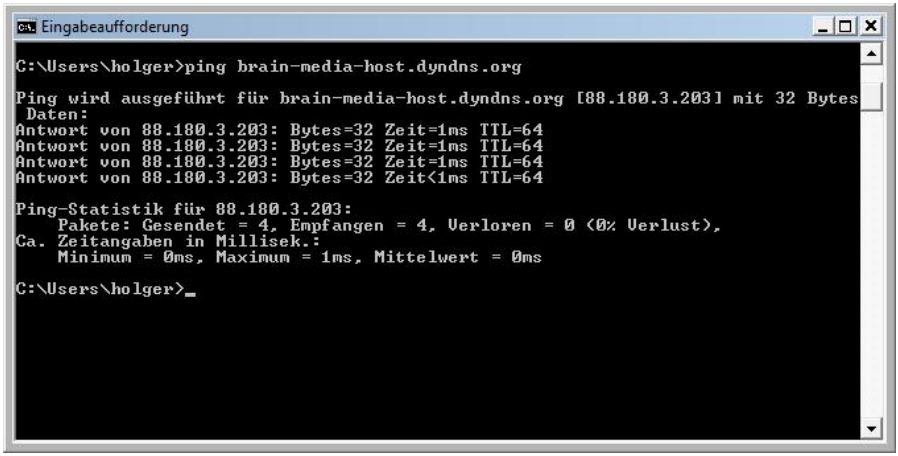
Die zweite Option ist sicherlich die Einfachste. Wenn Sie DynDNS.com nutzen, so finden Sie unter *http://www.dyndns.com/support/clients* verschiedene update-Clients. Nach der Installation des DynDNS-Client ist für die reibungslose Kommunikation zwischen dem lokalen System und dem DynDNS-Dienst gesorgt.

2.6.4 DynDNS testen

Testen wir nun, ob die von Ihnen neu angelegte DynDNS-Adresse auch erreichbar ist. Am Einfachsten greifen Sie dazu zu Ping. Wenn Sie mit Windows arbeiten, öffnen Sie mit *Start> Ausführen> cmd* die Windows-Eingabeaufforderung. Hier geben Sie folgendes Kommando ein:

```
ping ihre_DynDNS-Adresse
```

Im Idealfall gibt Ping die Antwortzeiten zurück, wie Sie in nachstehender Abbildung dargestellt sind. Damit wissen Sie, dass Ihr lokaler Server über diese Adresse ansprechbar ist.



Ihre DynDNS-Site ist erreichbar.

Sie können über einen Browser mit der Eingabe Ihres DynDNS-Namens auf den lokalen Server zugreifen.

Ein letzter Schritt ist noch erforderlich. Beim Zugriff auf Ihre DynDNS-Adresse landen Sie auf der Startseite des Routers. Da Sie – und vor allem die externen Benutzer – dort ja nicht hin sollen, sondern auf Ihren lokalen Webserver, müssen Sie die sogenannten Forwardings nutzen. Man spricht häufig von NAT. Dabei wird eine Anfrage auf eine lokale Adresse umgeleitet.

Die meisten Router besitzen eine entsprechende Konfiguration. Sie müssen Sie nur noch ausfindig machen und dort die IP-Adresse des XAMPP-Servers eintragen. Damit ist Ihr XAMPP-System von außen erreichbar.

3 Mit MySQL arbeiten

Mit MySQL verfügt XAMPP über einen leistungsfähigen Datenbankserver, in dem die unterschiedlichsten Daten gespeichert und verwaltet werden. In der Datenbank landen beispielsweise die Inhalte einer PHP-basierten Website, die Bilder und dergleichen mehr. Neben dem Apache ist MySQL die zweite wichtige Kernkomponente des XAMPP-Pakets.

3.1 MySQL-Basics

Wenn es um das Veröffentlichen von dynamischen Web-Inhalten geht, ist MySQL längst die erste Wahl. Die MySQL-Datenbank ist zweifelsohne das populärste quelloffene SQL-Datenbankmanagementsystem der Welt. Neben einer freien Version gibt es inzwischen auch verschiedene kommerzielle Varianten und unterschiedliche Service-Angebote.

MySQL ist ein Datenbankmanagementsystem, das eigentlich alles verwalten und speichern kann, was man sich so denken kann. Eine Datenbank ist nichts anderes als eine strukturierte Sammlung von Daten. Um Daten einer Datenbank hinzuzufügen, auf sie zuzugreifen oder um sie zu verarbeiten, benötigt man ein Datenbankmanagementsystem.

Als relationales Datenbankmanagementsystem speichert MySQL die Daten in separaten Tabellen, statt alle Daten in einem einzigen großen Speicherraum abzulegen. Das hat verschiedene Vorzüge bezüglich der Geschwindigkeit und Flexibilität zur Folge. Für die Steuerung kommt SQL (Structured Query Language, strukturierte Abfragesprache) zum Einsatz, die gebräuchlichste, standardisierte Sprache für den Zugriff auf Datenbanken.

MySQL hat sich in der Vergangenheit als sehr solides und schnelles System etabliert. Nicht immer so einfach ist seine Handhabung. Aber dafür gibt es spezielle Datenbankmanager, die Ihnen helfen, typische Aktionen beim Datenmanagement durchzuführen.

Ein weiteres wichtiges Merkmal von MySQL ist seine Client-Server-Architektur, die von verschiedenen Back-ends sowie diversen Client-Programmen und -bibliotheken sowie Verwaltungswerkzeugen unterstützt wird. Außerdem lässt sich das System über verschiedene Programmierschnittstellen ansprechen.

Wie Sie den Server starten und anhalten, ist bereits oben beschrieben und soll hier nicht wiederholt werden. Auch die Funktionen, die über das XAMPP Control Panel zur Steuerung des Servers dienen, sind bereits erläutert.

Weitaus interessanter sind die Funktionen, die MySQL selbst mitbringt. Es handelt sich um ein Kommandozeilenprogramm für die Administration des Servers. Schauen wir uns an, wie man in der Praxis mit diesem System arbeitet.

Mit das wichtigste Tool für die Arbeit mit MySQL ist das mysql-Clientprogramm, das Sie sowohl unter Linux als auch unter Windows auf der Konsole starten. Es wird auch als MySQL-Terminalmonitor oder als MySQL-Monitor bezeichnet. Mit diesem interaktiven Programm können Sie Verbindungen mit einem MySQL-Server herstellen, Abfragen ausführen und die Ergebnisse anzeigen. Auch der Stapelbetrieb ist möglich. Um eine Liste aller mysql-Optionen anzuzeigen, rufen Sie es mit der Option *--help* auf:

```
mysql --help
```

Mit dem MySQL-Monitor stellen Sie auch die Verbindung zum Server her. Dazu ist in der Regel die Angabe eines gültigen Benutzernamens und eines Passworts erforderlich. Wenn Sie von einem Drittsystem auf den MySQL-Server zugreifen wollen, so ist auch die Angabe des Hostnamens erforderlich. Wenn Sie den Host und die Anmeldedaten kennen, können Sie eine Verbindung mit folgendem Kommando herstellen:

```
mysql -h host -u user -p
```

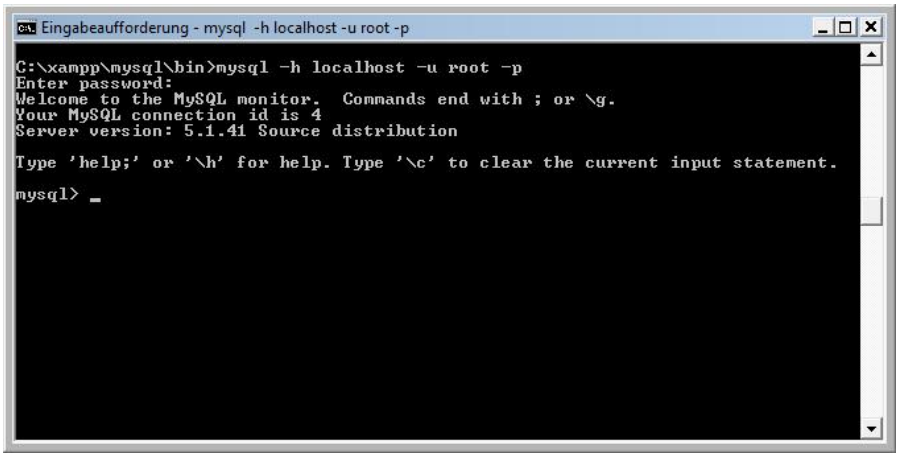
Der MySQL-Monitor fordert Sie dann zur Eingabe des Passworts auf:

```
Enter password:
```

Kann die Verbindung zum Server aufgebaut werden und klappt auch die Authentifizierung, so meldet sich der Server mit der mysql-Eingabeaufforderung. Nun können Sie die ersten MySQL-Befehle ausführen.

Auch das Trennen einer Verbindung ist problemlos: Geben Sie einfach an der mysql-Eingabeaufforderung den Befehl *QUIT* (oder *\q*) > ein:

```
mysql> QUIT;
Bye
```



Die Verbindung mit dem MySQL-Server konnte erfolgreich hergestellt werden.

Ihre MySQL-Installation besitzt bereits verschiedene Beispieldatenbanken. Daher können Sie eigentlich bereits die erste Datenbankabfrage erstellen. Auch das ist einfach mit dem MySQL-Monitor möglich. Eine typische Eingabe zeigt, wie man eine Datenbankabfrage ausführt. Dieses erste Beispiel demonstriert, wie Sie die Version der MySQL-Datenbankversion abfragen:

```
mysql> SELECT VERSION()
```

Die Ausgabe sieht wie folgt aus:

```
+--------------+
| VERSION()    |
+--------------+
| 5.6.11       |
+--------------+
1 row in set (0.01 sec)
mysql>
```

Anhand dieser einfachen Abfrage wird deutlich, dass ein Befehl normalerweise aus einer SQL-Anweisung gefolgt von einem Semikolon besteht.

Der MySQL-Monitor verwendet für die Abfrageausgabe eine Tabellenform, in der die Daten als Zeilen und Spalten ausgegeben werden. Die erste Zeile enthält die Spaltenüberschriften. Alle nachfolgenden Zeilen sind Abfrageergebnisse.

Der Monitor zeigt auch an, wie viele Datensätze (Zeilen) zurückgegeben wurden und wie lange die Ausführung der Abfrage dauerte. In diesem Beispiel war es ein Datensatz und die Bearbeitung hat 0,01 Sekunden gedauert.

Beachten Sie außerdem, dass Schlüsselwörter in beliebiger Groß- und Kleinschreibung angegeben werden können. Die folgenden drei Beispiele sind also gleichwertig:

```
mysql> SELECT VERSION()
mysql> select version()
mysql> SELect verSIOn()
```

Bei der Befehlseingabe müssen Sie nicht unbedingt alles in eine Zeile packen. Sie können vielmehr auch mehrzeilige Anweisungen verwenden. Das erweist sich gerade auch bei komplexen Anweisungen als sinnvoll.

Eine einfache mehrzeilige Anweisung kann wie folgt aussehen:

```
mysql> SELECT
    -> USER()
    -> ,
    -> CURRENT_DATE;
```

Dieses Kommando fragt den aktuellen Benutzer und das Datum ab. Die Ausgabe dazu könnte wie folgt aussehen:

```
+---------------+--------------+
| USER()        | CURRENT_DATE |
+---------------+--------------+
| root@localhost | 2013-09-10  |
+---------------+--------------+
```

Wenn Sie mehrzeilige Anweisungen verwenden, schaltet die Eingabeaufforderung übrigens von *mysql>* auf -> um. Das zeigt Ihnen an, dass der Monitor noch keine

vollständige Anweisung erkannt hat und auf weitere Eingaben wartet. Es gibt weitere Typen von Eingabeaufforderungen:

- **mysql**>: Bereit für ein neues SQL-Kommando
- ->: Der Monitor erwartet die nächste Zeile einer mehrzeiligen Befehlseingabe.
- '>: Erwartet die nächste Zeile und die Vervollständigung eines Strings, der mit einem einfachen Anführungszeichen beginnt.
- ">: Erwartet die nächste Zeile und die Vervollständigung eines Strings, der mit einem doppelten Anführungszeichen (") beginnt.
- `>: Erwartet die nächste Zeile und die Vervollständigung eines Bezeichners, der mit einem Backtick (`) beginnt.
- /*>: Erwartet die nächste Zeile und die Vervollständigung eines Kommentars, der mit /* beginnt.

Mit dem SELECT-Kommando kennen Sie bereits einen der wichtigsten Befehle.

Wenn Sie als Nächstes wissen wollen, welche Datenbanken bereits auf Ihrem Datenbankserver existieren, verwenden Sie den SHOW-Befehl:

```
mysql> SHOW DATABASES;
```

Die Ausgabe sieht dann wie folgt aus:

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| cdcol              |
| mysql              |
| test               |
| webauth            |
+--------------------+
6 rows in set (0.01 sec)
mysql>
```

So oder so ähnlich sollte auch Ihre Ausgabe aussehen.

Das Erstellen von Datenbanken und Tabellen ist ebenfalls recht einfach. Um eine erste Datenbank mit der Bezeichnung *Testdatenbank* zu erstellen, führen Sie folgenden Befehl aus:

```
mysql> CREATE DATABASE Testdatenbank;
```

Das Erstellen einer Datenbank ist ganz einfach. Noch aber ist die Datenbank leer, wie Sie mit *SHOW TABLES* nachprüfen können:

```
mysql> SHOW TABLES;
```

Die Ausgabe in unserem Beispiel zeigt an, dass die Datenbank noch leer ist.

```
Empty set (0.00 sec)
```

Wie erstellt man nun eine Tabelle? Auch das ist einfach: Dazu verwenden Sie den Befehl *CREATE TABLE* gefolgt von den Tabellennamen. Da aber Tabellen auch spezifische Daten aufnehmen sollen (beispielsweise die typischen Kontaktdaten eines Adressbuchs, wie Name, Vorname, Adresse etc.) müssen Sie ein Layout definieren. Dabei können Sie auch festlegen, welche Daten für welchen Informationstyp zulässig sind.

Um eine Tabelle mit verschiedenen Feldern und Eigenschaften zu definieren, könnten Sie etwa folgenden Befehl verwenden:

```
mysql> CREATE TABLE Adressen  (name VARCHAR(20), vorname VAR-
CHAR(20), adresse VARCHAR(20), geburtstag DATE);
```

Nun sollten Sie Ihre Tabelle natürlich auch mit Daten füllen. Hierfür kommen die beiden Kommandos *LOAD DATA* und *INSERT* zum Einsatz. Der eine Befehl kann bestehende Daten, wie beispielsweise eine Textdatei, importieren, der Andere dient der direkten Eingabe von Daten.

Wie Sie anhand dieser wenigen einleitenden Schritte erkennen können, ist das Handling auf Konsolenebene nicht gerade einfach. Hier bietet es sich an, zu grafischen Werkzeugen zu greifen. Dazu im Folgenden mehr.

MySQL kommt mit weiteren Konsolenwerkzeugen daher, mit denen Sie weitere unterschiedliche Aktionen durchführen können:

- **mysql_upgrade**: Führt ein Upgrade aus.
- **mysqladmin**: Dient der Administration des MySQL-Servers.
- **mysqlcheck**: Testet Ihre Tabellen.
- **mysqldump**: Dient dem Übertragen von Tabellen zwischen MySQL-Servern.
- **mysqlimport**: Stellt Importfunktionen bereit.
- **mysqlshow**: Zeigt die Merkmale Ihrer Datenbanken.
- **mysqltest**: Dient dem Testen.

Für weitere Informationen zu den einzelnen Tools (und das waren längst nicht alle) sei auf die offizielle MySQL-Dokumentation verwiesen.

3.2 MySQL Workbench

Administratoren schwören bekanntlich auf Konsolenwerkzeuge. Das mag bei der klassischen Systemadministration praktikabel sein, doch beim Hantieren mit Datenbanken und Tabellen erweisen sich derlei Werkzeuge schnell als unpraktikabel.

Die Zahl der aktuell verfügbaren MySQL-GUIs ist allerdings sehr gegrenzt. Neben phpMyAdmin ist MySQL Workbench das einzige Tool, das kontinuierlich weiterentwickelt wird und professionellen Ansprüchen genügt. MySQL Workbench ist – wie MySQL – in einer freien Community Edition und einer kommerziellen Variante verfügbar und wird von Oracle entwickelt. Das Tool stellt Ihnen drei Funktionsbereiche bereit: Es kann zur SQL-Entwicklung, zur Datenmodellierung und zur MySQL-Datenbankadministration verwendet werden. Workbench kann unter Linux, Mac OS X und Windows ausgeführt werden.

Für die Entwicklung von Datenmodellen steht Ihnen ein grafisches Werkzeug zur Verfügung. Die aktuelle Version 6.0 hat eine runderneuerte Benutzerschnittstelle erhalten, über die Sie Verbindungen zu MySQL-Servern herstellen, Datenmodellierung und -migrationen ausführen und auf die Konsolenwerkzeuge zugreifen können.

Über die Startseite legen Sie mit einem Klick auf das Pluszeichen neben *MySQL Connections* Datenbankverbindungen an. Eine Verbindung stellen Sie her, indem Sie auf einen Verbindungseintrag klicken, den Konfigurationsdialog ausfüllen und mit einem Klick auf *Test connection* die Einstellungen testen. Führen Sie den

Mauszeiger über eine Verbindungskonfiguration, können Sie die wesentlichen Verbindungseigenschaften einsehen und die Managementfunktionen aufrufen.

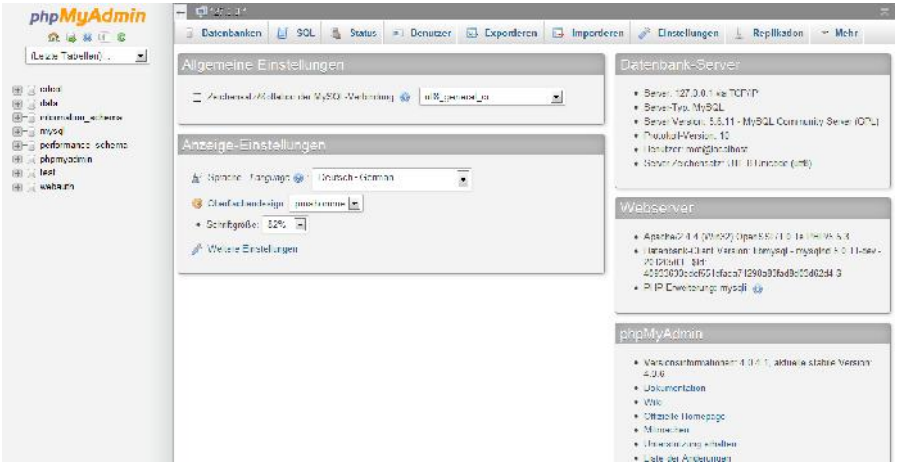
Die Managementfunktionen sind sehr benutzerfreundlich, denn damit können Sie bequem den Serverstatus und die Verbindungsinformationen abrufen, Benutzer und Privilegien einsehen und bearbeiten. Auch die Import- und Exportfunktionen bieten alle wichtigen Einstellungen für die zielgenaue Datenübertragung. Auch MySQL Workbench erlaubt das Einsehen der Protokolldateien und der Options-Datei.

Das Managementwerkzeug stellt Ihnen außerdem verschiedene Assistenten zur Verfügung, mit denen Sie beispielsweise Datenbankschemata von älteren MySQL-Servern auf neuere übertragen können oder die Ihnen bei der Datenbankmigration unter die Arme greifen.

4 XAMPP-Tool phpMyAdmin

Wenn auch Sie zu den Anwendern, Administratoren oder Entwicklern gehören, deren Web-Anwendungen auf dem Apache-MySQL-PHP-Gespann basieren, dann benötigen Sie ein Werkzeug, mit dem Sie Eingriffe in den MySQL-Server vornehmen können. Gleich, ob Sie einen Blog, einen Online-Shop oder ein Content-Managementsystem einrichten wollen: Immer sind Eingriffe in den Datenbankserver erforderlich. Sie müssen beispielsweise vor dem Aufsetzen eines Magento-Shops eine Datenbank anlegen, in der die Shop-Daten gespeichert werden. Wenn Sie sogar Erweiterungen einer PHP-Umgebung planen, benötigen Sie außerdem einen Datenbankmanager.

Nun kommt MySQL zwar mit verschiedenen Tools daher, mit deren Hilfe Sie mit dem Datenbankserver arbeiten könnten, doch die sind alles andere als komfortabel.



Ein erster Blick auf phpMyAdmin 4.0.4.

Das mit Abstand benutzerfreundlichste und leistungsfähigste Werkzeug für die Verwaltung von MySQL-Servern ist phpMyAdmin (*http://www.phpmyadmin.net*). Nicht nur wenn Sie lokal mit MySQL-Datenbanken hantieren, sondern gerade auch

beim Betrieb einer typischen Web-Anwendung macht phpMyAdmin eine hervorragende Figur.

Wie unschwer an seiner Bezeichnung abzulesen ist, ist phpMyAdmin eine PHP-Applikation zur Administration von MySQL-Datenbanken. Mit phpMyAdmin lassen sich MySQL-Datenbanken einfach und schnell per HTTP mit einem Browser ansprechen, ohne auf komplizierte SQL-Befehle zurückgreifen zu müssen.

4.1 Die Highlights von phpMyAdmin

Das Tool wird inzwischen von vielen Providern eingesetzt, damit deren Kunden ihre MySQL-Datenbank verwalten können. phpMyAdmin bietet eine beeindruckende Funktionalität. Mit dem Tool können Sie – Root-Rechte vorausgesetzt – ganze MySQL-Server administrieren. Natürlich lassen sich auch einzelne Datenbanken steuern. Dazu müssen allerdings Benutzerrechte gezielt gesetzt werden. Der Datenbankmanager unterstützt folgende Aktionen:

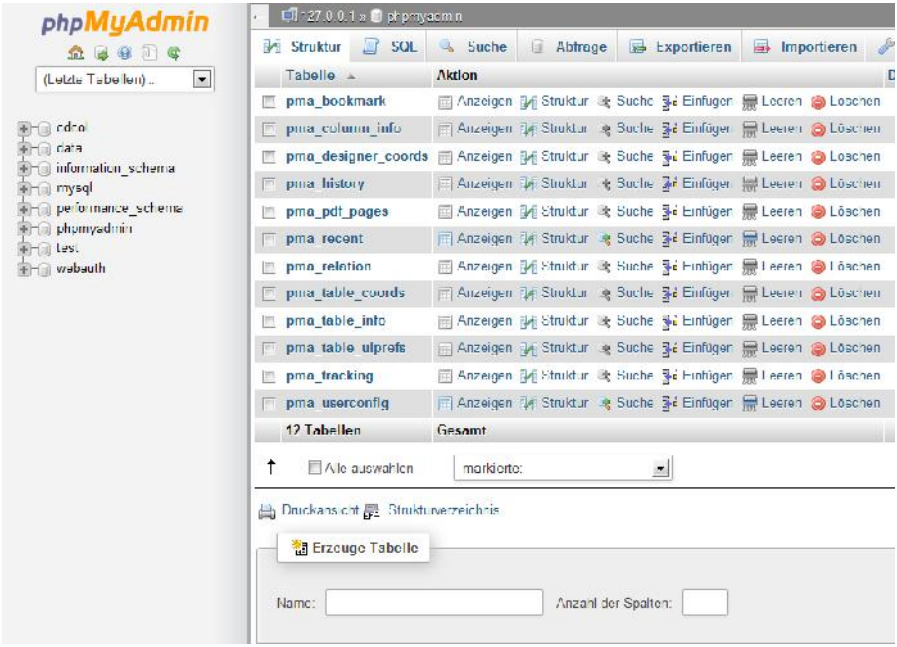
- Erzeugen und Löschen von Datenbanken
- Erzeugen, Kopieren, Löschen, Umbenennen und Bearbeiten von Tabellen
- Tabellen verwalten
- Löschen, Editieren und Hinzufügen von Feldern
- Ausführung von SQL-Statements, auch im Batch-Modus
- Laden von Text in Tabellen
- Export von Daten nach CSV, XML und LaTeX
- Administration von mehreren Datenbankservern
- Verwalten von MySQL-Benutzern und Privilegien
- Erzeugen von PDF-Grafiken des Datenbank-Layouts
- Suche nach Datenbankinhalten – global oder in spezifischen Abschnitten
- und, und, und …

Die Liste der Features ließe sich noch um einige Funktionen erweitern. Doch wenden wir uns der Praxis zu.

4.2 phpMyAdmin kennenlernen

Bislang haben Sie phpMyAdmin installiert und für das Zusammenspiel mit einem oder auch mehreren MySQL-Servern konfiguriert. Sie haben auch eine grobe Vorstellung davon, was Sie alles mit dem Datenbankmanager anstellen können und wie die Benutzerschnittstelle aussieht.

phpMyAdmin besitzt eine übersichtlich strukturierte Schnittstelle, über die man alle typischen Aktionen beim Umgang mit Datenbanken steuert. Schauen wir uns die verschiedenen Bereiche näher an.

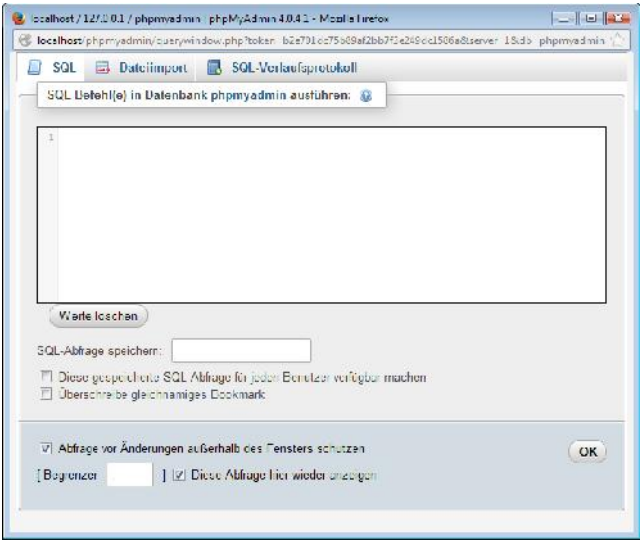


Die geöffnete Datenbank *phpmyadmin*.

Wie Sie voranstehender Abbildung entnehmen können, ist die Web-Schnittstelle zweigeteilt: links die Navigationsleiste, rechts die dazugehörigen Einstellungen und Funktionen. Beim ersten Einloggen können Sie die Sprachversion anpassen. Wir gehen im Folgenden davon aus, dass Sie die deutsche Version verwenden.

Widmen wir uns zunächst der Navigationsleiste. Über den Kopf und das zugehörige phpMyAdmin-Logo gelangen Sie zur phpMyAdmin-Homepage. Unterhalb finden Sie eine kleine Symbolleiste mit vier bzw. fünf Icons. Führen Sie den Mauszeiger über das jeweilige Icon, so präsentiert Ihnen phpMyAdmin eine Kurzinfo. Die Links im Einzelnen:

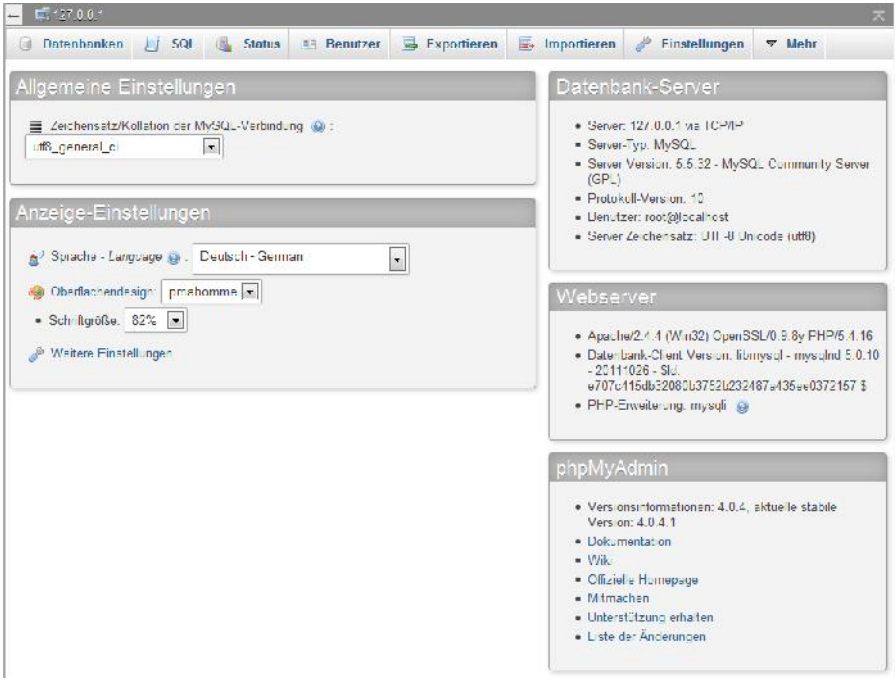
- **Home**: Über dieses Icon gelangen Sie zur Homepage der phpMyAdmin-Installation.
- **SQL-Abfragefenster**: Öffnet das Abfragefenster, über das Sie SQL-Abfragen an die Datenbank übergeben.
- **phpMyAdmin-Dokumentation**: Ein Klick öffnet die lokale Dokumentation. Sie entspricht dem, was Sie auf der phpMyAdmin-Website finden.
- **MySQL-Dokumentation**: Ein Klick auf dieses Icon öffnet die MySQL-Dokumentation der MySQL-Homepage in einem neuen Browser-Fenster.
- **Navigations-Frame aktualisieren**: Bringt das Navigationsfenster auf den neuesten Stand.



Das Abfragefenster erlaubt die manuelle Eingabe und Ausführung von SQL-Kommandos.

Unterhalb dieser kleinen Symbolleiste finden Sie das Auswahlmenü *Tabellen* und darunter die bereits bei einer Erstinstallation vorhandenen verschiedene Datenbanken. Wenn Sie eine Datenbank ausgewählt haben, zeigt phpMyAdmin in der Kopfzeile des Browsers neben dem Server auch die Datenbankbezeichnung an. Diese Ansicht können Sie in der phpMyAdmin-Konfigurationsdatei deaktivieren.

Nach der Auswahl einer Datenbank führt phpMyAdmin unterhalb der Datenbankbezeichnung die Datenbankelemente auf. Standardmäßig werden sie in alphabetischer Reihenfolge aufgeführt. Weitere Details, wie beispielsweise eine Tabelleninfo, sind verfügbar, wenn Sie den Mauszeiger über die jeweilige Tabelle führen. Details zu den einzelnen Tabellen öffnen Sie mit einem Klick auf die jeweilige Tabellenbezeichnung. Bei Multiserver-Umgebungen ist über die linke Navigationsleiste auch die Auswahl der verschiedenen Server möglich.



Die Startseite des Arbeitsbereichs präsentiert Ihnen verschiedene allgemeine Informationen über die Umgebung.

4.3 Der Arbeitsbereich

Der Inhalt des rechten phpMyAdmin-Arbeitsbereichs ist abhängig von der aktivierten Ansicht. Öffnen Sie die Homepage Ihrer phpMyAdmin-Installation, so präsentiert phpMyAdmin rechts die Menüleiste, über die Sie auf die verschiedenen Funktionsbereiche und Einstellungen zugreifen, darunter verschiedene allgemeine Informationen über die Apache-MySQL-PHP-phpMyAdmin-Umgebung. Oberhalb der Menüleiste wird der aktuelle Server angezeigt. Mit einem Klick auf den Pfeil links der Serverbezeichnung blenden Sie die Navigationsleiste ein und wieder aus.

So können Sie sowohl den Navigations-, als auch den Arbeitsbereich, das sogenannten Hauptpanel, an Ihre Vorstellungen und Bedürfnisse anpassen. Mit einem Klick auf die Server-Adresse bzw. auf das Home-Symbol gelangen Sie wieder zurück zur typischen Startseite.

Unterhalb der Menüleiste finden Sie fünf Bereiche mit verschiedenen Informationen und Funktionen. Unter *Allgemeine Einstellungen* können Sie den Zeichensatz für die Verbindung zum MySQL-Datenbankserver anpassen. In der Regel ist hier keine Anpassung erforderlich.

Darunter finden Sie den Bereich *Anzeige-Einstellungen*. Hier werden die aktuell verwendete Sprachvariante, das Oberflächendesign, die Farbe und die Schriftgröße angezeigt. Bei der Wahl des Designs können Sie sich zwischen *Original* und *pmahomme* entscheiden. Mit einem Klick auf Weitere Einstellungen öffnen Sie die phpMyAdmin-Einstellungen.

Der Bereich *Datenbank-Server* zeigt die serverrelevanten Informationen wie die Server-Version, die Verbindung, den Benutzernamen und den verwendeten Zeichensatz an.

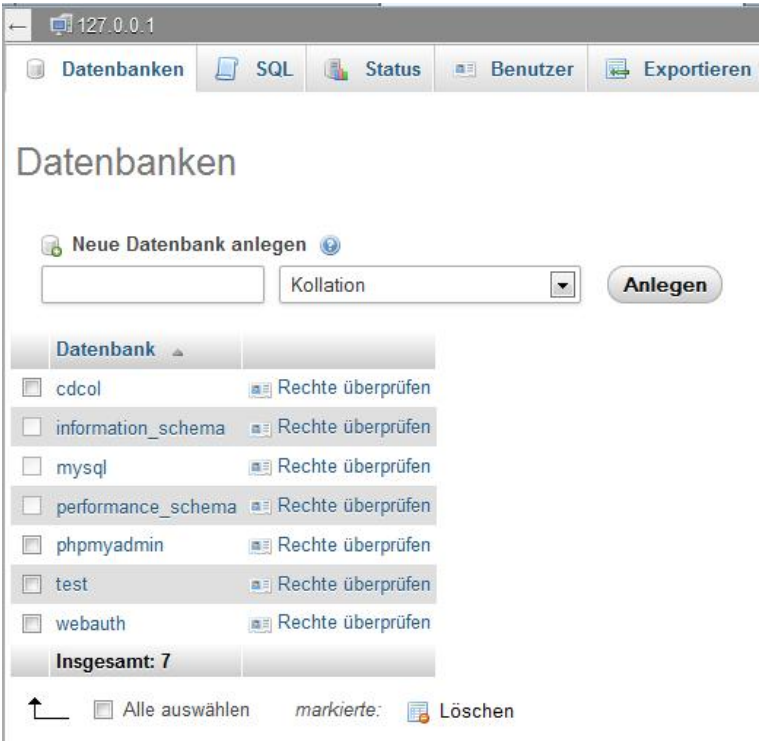
Der Bereich *Webserver* führt folgende Informationen auf:

- Apache-Version einschließlich der relevanten Apache-Module
- MySQL-Client-Version
- PHP-Extension

Im Bereich *phpMyAdmin* wird zunächst die Versionsnummer Ihrer Installation angezeigt. In unserem Fall ist das Version 4.0.4. Über den Link *Dokumentation* rufen Sie die lokale Dokumentation auf. Auch der Zugriff auf das Wiki ist möglich. Schließlich ist der Zugriff auf die phpMyAdmin-Website, den Changelog, CVS-Versionen und die Mailinglisten möglich.

Der rechte Arbeitsbereich weist zwei weitere wichtige Ansichten auf: die Datenbank- und die Tabellenansicht. Die Datenbankansicht öffnet sich immer dann, wenn Sie in der Navigationsleiste eine Datenbank auswählen. Diese Ansicht weist die typischen Details und Funktionen von Datenbanken auf:

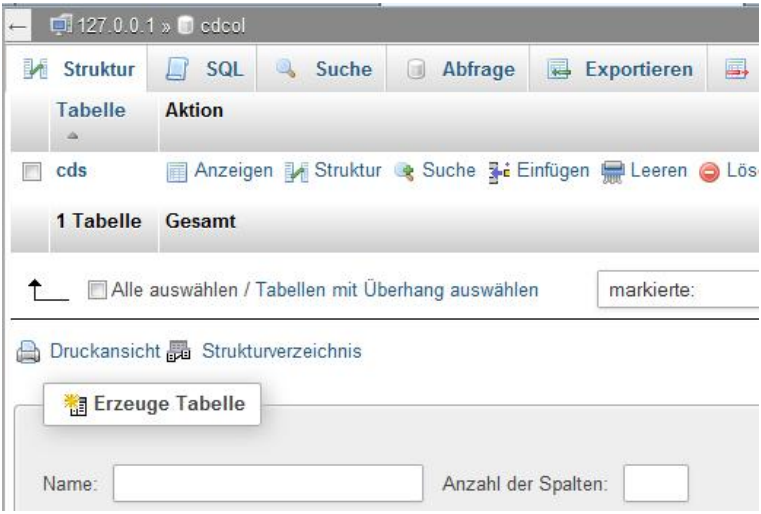
- Ansicht bestehender Tabellen, genauer die Strukturansicht
- Erzeugen neuer Tabellen
- Registerkarten, um SQL-Befehle auf die Datenbank anzuwenden, Inhalte gezielt zu exportieren etc.
- Ergänzende Detailinformationen wie Anzahl der Tabellen, Einträge, Größe etc.



Die typische Datenbanksicht verrät Ihnen, welche Datenbank auf dem MySQL-Server lagern.

In der Kopfzeile der Datenbankansicht werden außerdem der Server sowie die Datenbankbezeichnung aufgeführt. Mit einem Klick auf einen Datenbankeintrag öffnen Sie die Tabellenansicht. Sie führt die Tabellen auf, die in einer Datenbank enthalten sind.

Neben der Tabellenliste finden Sie Checkboxen, über die Sie Tabellen einzeln auswählen können, auf die bestimmte Aktionen angewendet werden.



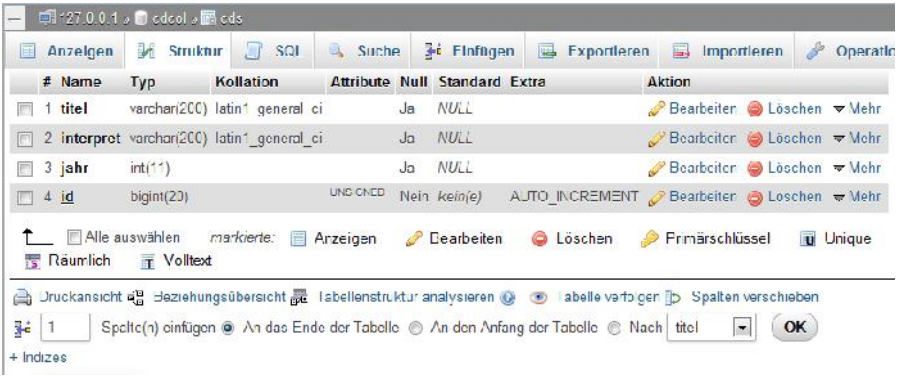
Eine typische Tabellenansicht: In der Datenbank *cdcol* ist lediglich die Tabelles *cds* enthalten.

Unterhalb der Tabellenliste finden Sie eine weitere wichtige Funktion: Das Eingabefeld *Erzeuge Tabelle* erlaubt das Erzeugen einer neuen Ablage. Geben Sie dazu einfach eine Bezeichnung in das zugehörige Textfeld ein, legen Sie unter *Anzahl der Spalten* die Anzahl der Felder fest und bestätigen Sie mit *OK*.

4.4 Ansichten in phpMyAdmin

In der Datenbankansicht ist außerdem das Hinzufügen eines Datenbankkommentars mit ergänzenden Informationen möglich. Die Datenbank kann eine andere Bezeichnung erhalten. Wie nahezu alle Ansichten in phpMyAdmin kann auch die Datenbankansicht über die Konfigurationsdatei angepasst werden.

Die Tabellenansicht öffnen Sie, indem Sie eine Datenbank und eine Tabelle in der Navigationsleiste öffnen. Alternativ wählen Sie in der Datenbankansicht eine Tabelle auf dem Register *Struktur* aus.

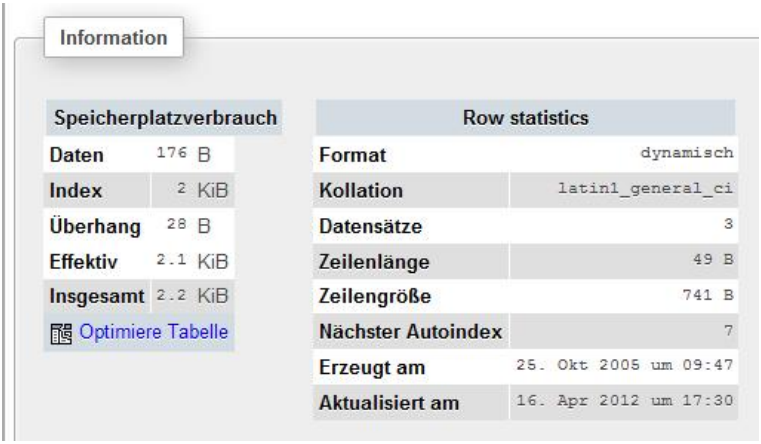


Die typische Strukturansicht.

Zu den einzelnen Tabellen werden folgende Details aufgeführt:

- Feldbezeichnung
- Typ
- Kollation
- Attribute
- Null
- Standort
- Extra

In der Spalte *Aktion* können Sie typische Tabellenaktionen durchführen. Unterhalb der Tabellenliste finden Sie weitere Detailinformationen zu Indizes, Speicherplatzverbrauch sowie eine Zeilenstatistik. Um auf diese Informationen zuzugreifen, klicken Sie auf den Link *Details*.



Die Detailinformationen zu Ihren Tabellen.

Außerdem bietet phpMyAdmin die so genannte Server-Ansicht. Sie ist nur dann verfügbar, wenn Sie mehrere MySQL-Server mit phpMyAdmin verwalten.

4.5 Datenbank erstellen

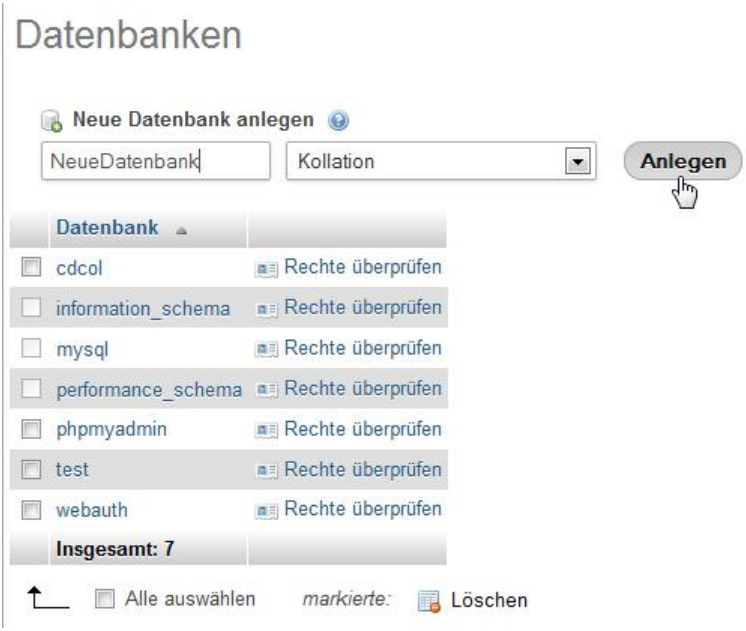
Schauen wir uns also an, wie Sie eine erste Datenbank erzeugen, wie Sie diese mit Daten füllen und wie Sie sich in dem Datenbestand bewegen. Bevor Sie die folgenden Aktionen durchführen können, muss sichergestellt sein, dass Sie über die notwendige *CREATE*-Berechtigung verfügen. Dabei sind prinzipiell verschiedene Szenarien denkbar:

- Im einfachsten Fall ist bereits eine Datenbank eingerichtet, an der Sie erste Erfahrungen sammeln können. Entsprechende Berechtigungen müssen, wie bereits erwähnt, gesetzt sein.
- Das zweite denkbare Szenario erlaubt Ihnen das Erstellen einer neuen Datenbank, an der Sie den Umgang mit phpMyAdmin erlernen können.
- Schließlich ist es denkbar, dass Sie den Datenbankserver mit anderen Anwendern gemeinsam nutzen und für den jeweiligen Account eine Datenbank erzeugen können.

Wir gehen im Folgenden davon aus, dass Sie die erforderlichen Rechte für das Erzeugen einer Datenbank besitzen. Das Erzeugen einer neuen Datenbank ist recht

einfach. Öffnen Sie die Datenbankübersicht Ihrer phpMyAdmin-Installation und geben Sie in das Eingabefeld *Neue Datenbank anlegen* die gewünschte Bezeichnung ein. Dann klicken Sie auf die Schaltfläche *Anlegen*. Ein Fehler tritt auf, wenn die Datenbank bereits existiert.

Für das Verständnis ist es sicherlich interessant, dass Datenbanken in MySQL als Verzeichnisse implementiert sind, die Dateien enthalten, die den Tabellen in der Datenbank entsprechen. Weil es keine Tabellen in einer Datenbank gibt, wenn diese erstmalig erzeugt wird, erzeugt der *CREATE DATABASE*-Befehl nur lediglich ein leeres Verzeichnis unter dem MySQL-Daten-Verzeichnis.



Eine neue Datenbank entsteht.

Nach dem Klick auf *Anlegen* landen Sie in der Datenbankübersicht, über die Sie die Datenbank dann mit Leben füllen. In der Navigationsleiste links wird die aktuell geöffnete Datenbank anzeigt. In der Detailansicht werden wie gewohnt zunächst der Server und die Datenbankbezeichnung aufgeführt. Außerdem gibt phpMyAdmin eine Bestätigung aus, dass eine Datenbank erzeugt wurde und welcher Befehl hierfür verwendet wurde.

Der aufgeführte SQL-Befehl lautet:

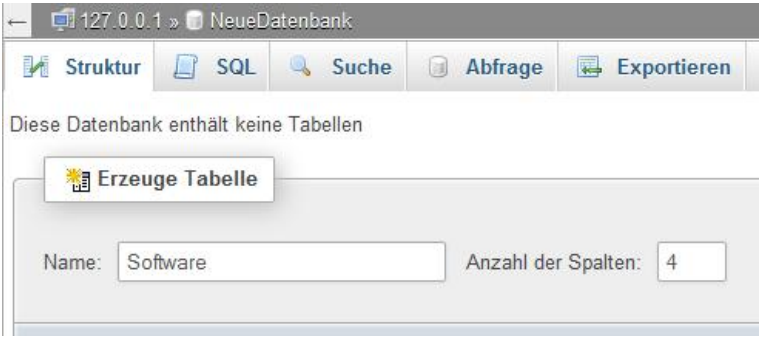
```
CREATE DATABASE `neueDatenbank`
```

Der zugehörige PHP-Befehl entsprechend:

```
$sql = 'CREATE DATABASE `neueDatenbank`';
```

Die Ansicht dieser Informationen wird über den Schalter *$cfg['ShowSQL']* aktiviert. Für SQL-Einsteiger sind diese Informationen ein guter Weg, SQL zu erlernen.

Ihre neue Datenbank besitzt noch keine Tabellen. Um die Datenbank mit Inhalten zu füllen, müssen Sie eine erste Tabelle erzeugen. Öffnen Sie die Datenbank in der Datenbankliste mit einem Klick. Das Anlegen einer Tabelle erfolgt über das Eingabefeld *Erzeuge Tabelle*. In das Feld geben Sie die Bezeichnung sowie die Anzahl der Spalten ein.

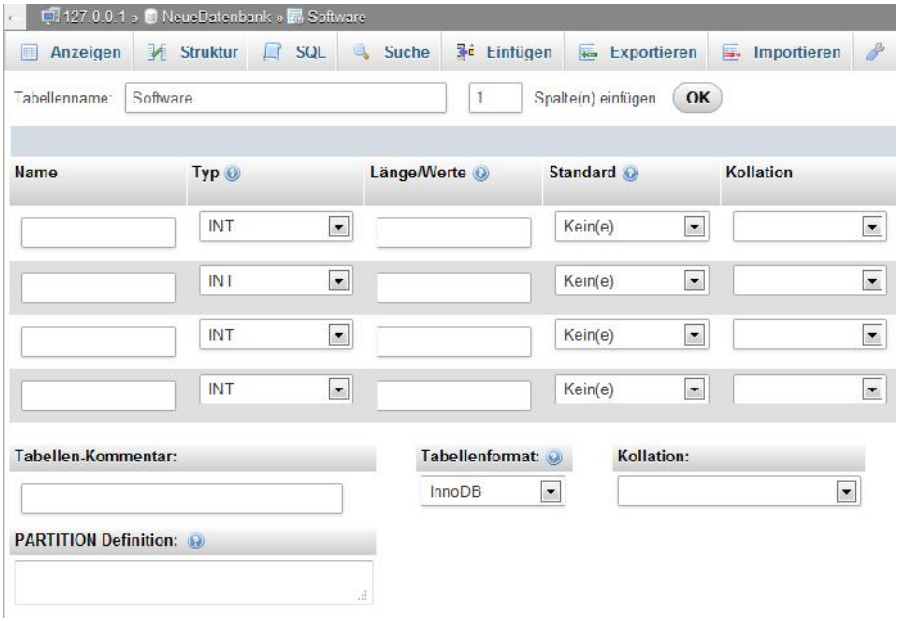


Die erste Tabelle in der neuen Datenbank wird angelegt.

Wir legen im Folgenden eine Datenbank mit Softwareprodukten an, die folgende Informationen verwaltet:

- Produktname
- Hersteller
- Produktkategorie
- Preis

Für die ersten Gehversuche ist es sicherlich nicht erforderlich, dass das Datenbankdesign bis ins letzte Detail ausgetüftelt ist. Wichtiger sind vielmehr die Herangehensweise und die praktische Umsetzung. Erweiterungen sind später immer noch möglich. Entsprechend diesem Beispiel bezeichnen wir die Tabelle mit *Software*, geben vier Felder an und bestätigen den Vorgang mit *OK*.



Eine erste Tabelle mit der Bezeichnung *Software* und vier Feldern ist entstanden.

In der Kopfzeile zeigt phpMyAdmin wieder den Server, die Datenbank und nun auch die Tabellenbezeichnung der gerade angelegten Tabelle ein. Da wir vier Felder gewählt haben, zeigt die Tabellenansicht nun vier Zeilen an, die mit verschiedenen Einstellungen versehen werden können. Es sind über ein Dutzend Einstellungen vorgesehen, über die Sie die Inhalte und weitere Eigenschaften spezifizieren.

Unter *Feld* geben Sie zunächst die Feldbezeichnung an. Wir verwenden hier die Feldbezeichnungen *Produktname*, *Hersteller*, *Kategorie* und *Preis*. Unter *Typ* müssen Sie den Datentyp festlegen, der für das jeweilige Feld zulässig ist.

Es sind über zwanzig Typen zulässig. Man unterscheidet zwischen numerischen Angaben, Zeit- und Datumsangaben sowie Zeichenfolgen. Die wichtigsten fasst nachstehende Tabelle zusammen:

Typ	Beschreibung
VARCHAR	Zeichenkette mit variablen Zeichen.
TEXT	Typischer Text.
DATE	Typische Datumsangabe. Es wird der Datumsbereich von 1000-01-01 bis 9999-12-31 unterstützt. MySQL zeigt DATE-Werte im Format YYYY-MM-DD an.
INT	Ein normaler Integer-Wert, der zwischen -2147483648 und 2147483647 liegen darf.
FLOAT	Fließkommawert
DECIMAL	Dezimalwert
TIME	Zeitangabe, die zwischen 838:59:59 und 838:59:59 liegen kann. MySQL zeigt TIME-Werte im Format HH:MM:SS an.
ENUM	Enumeration, wobei einer der angegebenen Werte aus der Menge {wert1, wert2, wert3, …, wertx} verwendet wird.
BINARY	Speichert binäre Informationen.

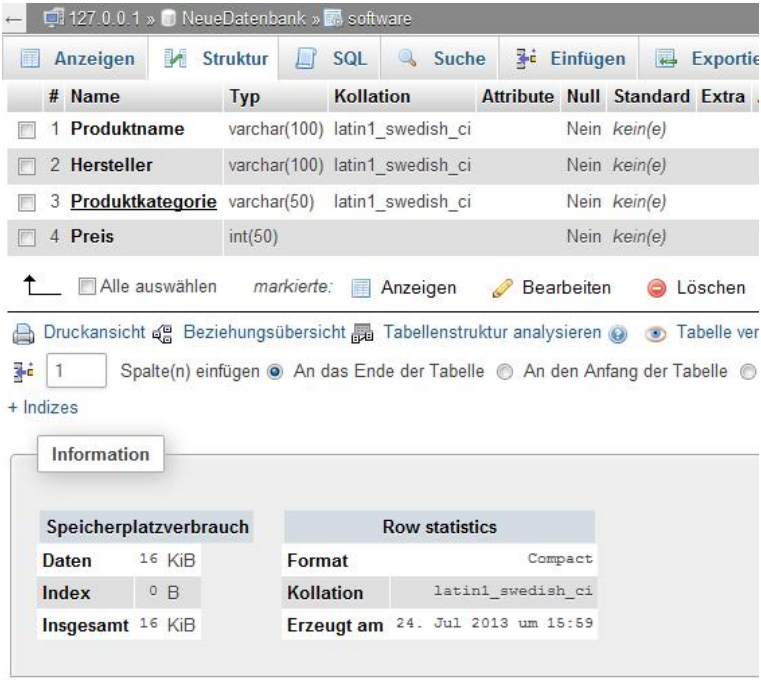
Eine genaue Beschreibung ist über die MySQL-Website verfügbar. Um die zugehörigen Informationen abzurufen, klicken Sie in der Kopfzeile auf das Fragezeichen neben *Typ*. In unserem Beispiel verwenden wir für Produktname, Hersteller und Produktkategorie den Typ *VARCHAR*. Dieser ist sehr flexibel und unterstützt auch die Kombination aus Zeichen und Buchstaben.

Eine weitere wichtige Einstellung nehmen Sie über die Spalte *Länge* vor. Hier legen Sie die maximal zulässige Zeichenlänge fest. In unserem Beispiel verwenden wir die Längen 100, 100, 50 und 10. Es folgen, wie bereits erwähnt, weitere Optionen und Schalter. Wir wollen uns bei diesem Beispiel mit den Ersten begnügen und bestätigen mit *OK*. Die zugehörigen SQL-Befehle lauten wie folgt:

```
CREATE TABLE `Software` ()
`Produktname` VARCHAR( 100 ) NOT NULL ,
`Hersteller` VARCHAR( 100 ) NOT NULL ,
```

```
`Produktkategorie ` VARCHAR( 50 ) NOT NULL ,
`Preis` INT( 10 ) NOT NULL
```

Nachdem die ersten Felder mit den zugehörigen Einstellungen erzeugt sind und Sie diese Tabellenkonfiguration mit *OK* bestätigt haben, präsentiert sich Ihnen etwa das Bild, das folgende Abbildung zeigt.



Eine erste Tabelle mit den erzeugten Feldern.

Dem aufmerksamen Beobachter wird nicht entgangen sein, dass in nachstehender Abbildung die Feldbezeichnung *Produktkategorie* unterstrichen ist, während die anderen Feldbezeichnungen keine vergleichbare Markierung aufweisen. Der Grund: Bei *Produktkategorie* handelt es sich um einen so genannten Primärschlüssel.

4.6 Tabellendetails definieren

Der Primärschlüssel ist ein Index, also eine zusätzliche Spalte, die einem Datensatz einen eindeutigen Wert zuordnet. In einer großen Datenbank kann es stets vorkommen, dass in mindestens einer Spalte eines Datensatzes der Wert identisch ist. An einem Beispiel wird die Problematik deutlich. Bei Adressdatenbanken ist es durchaus nicht ungewöhnlich, dass es mehrere Familien Müller im gleichen Hochhaus gibt. Da in einem solchen Fall Namen und Adressen in der Tabelle gleich wären, läge ein doppelter Eintrag vor.

Um dieses Problem zu lösen, greifen Sie zum sogenannten Primärschlüssel. Der Primärschlüssel bezeichnet Attribute (Spalten) einer Relation (Tabelle), die einen Datensatz dieser Relation eindeutig identifizieren. Meist ist dies nur ein Attribut. Ein Wert dieses Attributes kann nur einmal vorkommen.

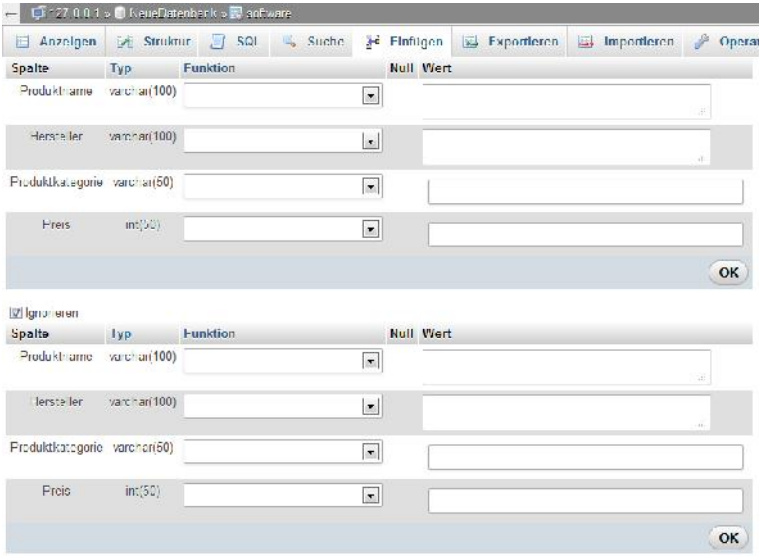
Ein Primärschlüssel kann auch aus der Kombination mehrerer Attribute bestehen, wenn diese gemeinsam jeden Satz eindeutig identifizieren. Dies ist dann ein sogenannter kombinierter Primärschlüssel oder auch Verbundschlüssel. Die Wahl der Attribute für den Schlüssel wird so vorgenommen, dass die Attributkombination minimal identifizierend ist, d. h., sie darf nicht mehr Attribute enthalten, als nötig sind, um sie eindeutig zu machen.

Die zugehörigen Einstellungen finden Sie weiter rechts von den jeweiligen Feldeinstellungen. In unserem Fall ist es beispielsweise sinnvoll, den Produktnamen als Primärschlüssel zu kennzeichnen.

Wenn Sie den Primärschlüssel gesetzt haben, wird der zugehörige Eintrag in der Tabellenübersicht unterstrichen gekennzeichnet. Wollen Sie den Primärschlüssel einer anderen Tabelle zuweisen, klicken Sie einfach in der jeweiligen Zeile unter Aktion auf die Schaltfläche *Primärschlüssel*. phpMyAdmin gibt einen Hinweis aus, dass der Schlüssel neu gesetzt wird.

Als Nächstes gilt es, die zuvor erzeugte Tabelle mit Daten zu füllen. Dazu wechseln Sie zum Register *Einfügen*. Dort stehen Ihnen standardmäßig zwei Eingabeblöcke zur Verfügung, über die Sie die Datenbank manuell mit Daten füttern können.

Dass es sich um zwei Blöcke handelt, liegt an der Standardeinstellung der Konfigurationsdatei. Die für diese Einstellung zuständige Option *$cfg['InsertRow']* ist standardmäßig auf 2 gesetzt.



Das *Einfügen*-Formular dient dem manuellen Füttern der Datenbank.

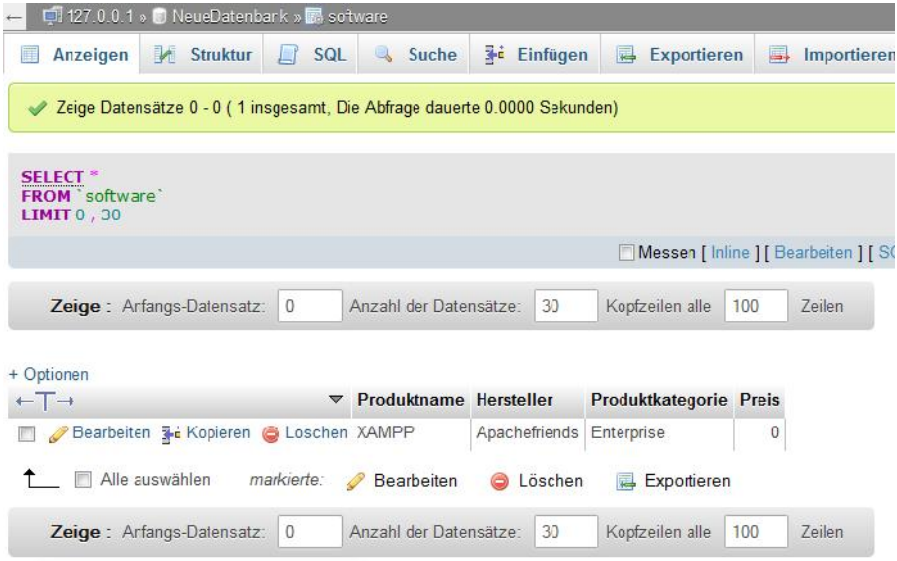
Unter *Wert* füttern Sie die Tabelle mit den entsprechenden Informationen und klicken abschließend auf *OK*. Im unteren Dialogbereich können Sie außerdem wählen, ob Sie mit der Eingabe weiterer Datensätze fortfahren wollen. Anschließend landen Sie wieder in der Tabellenübersicht, in der das ausgeführte Kommando sowie die Tabellen aufgeführt werden.

Die Eingabefelder des *Einfügen*-Dialogs sind standardmäßig zweizeilig. Das ist nicht immer sinnvoll, denn gelegentlich will man mehrzeilige Inhalte in der Tabelle hinterlegen. Glücklicherweise lassen sich diese Einstellungen bearbeiten. Öffnen Sie die phpMyAdmin-Konfigurationsdatei und passen Sie diese entsprechend nachfolgendem Beispiel an:

```
$cfg['CharTextareaCols']  = 50
$cfg['CharTextareaRows']  = 3
```

Schon hat man ein Textfeld, das 50 Zeichen breit und 3 Zeichen hoch ist. Diese Einstellungen wirken sich auf alle *CHAR*- und *VARCHAR*-Felder aus.

Die eingefügten Daten können Sie über das Register *Anzeigen* abrufen. Wie Sie nachstehender Abbildung entnehmen können, werden die Einträge listenförmig aufgeführt.



Über das Register *Anzeigen* können Sie die gespeicherten Daten einsehen.

Die Anzahl der Datensätze in der Ansicht können Sie über die Einstellungen *Zeige* anpassen. Standardmäßig werden die Datensätze untereinander aufgeführt. Auch die horizontale und nebeneinander angeordnete Ansicht steht zur Verfügung. Über die Datensatzliste können Sie auch neue Einträge erzeugen.

Handelt es sich um sehr aufwändige Datensätze, so erlaubt die Anzeigen-Ansicht auch das einfache Blättern zwischen den Übersichten. Bei mehreren Datensätzen steht außerdem eine Sortierfunktion zur Verfügung. Um einen Datensatz zu bearbeiten, klicken Sie auf das Stift-Symbol, das den Eintrag editiert. Entsprechend gehen Sie beim Löschen vor. Außerdem stehen Druck- und Exportfunktionen im Browse-Modus zur Verfügung.

Wenn Sie den Mauszeiger über die Datensatzliste führen, so stellen Sie fest, dass phpMyAdmin die Zeilen abhängig von der durchführten Aktion mit verschiedenen Farben kennzeichnet. Führen Sie den Zeiger über einen Datensatz, so wird dieser blau hinterlegt. Das sorgt für mehr Benutzerfreundlichkeit und auch für mehr Sicherheit, da Sie immer wissen, was gerade geschieht.

Da die voreingestellten Farben nicht jedermanns Sache sind, können Sie diese Einstellungen wieder über die Konfigurationsdatei *layout.inc.php* (Sie finden sie im Ordner *Themes*) anpassen. Die zugehörigen Einstellungen sind:

```
$cfg['BrowsePointerColor']
$cfg['BrowseMarkerColor']
```

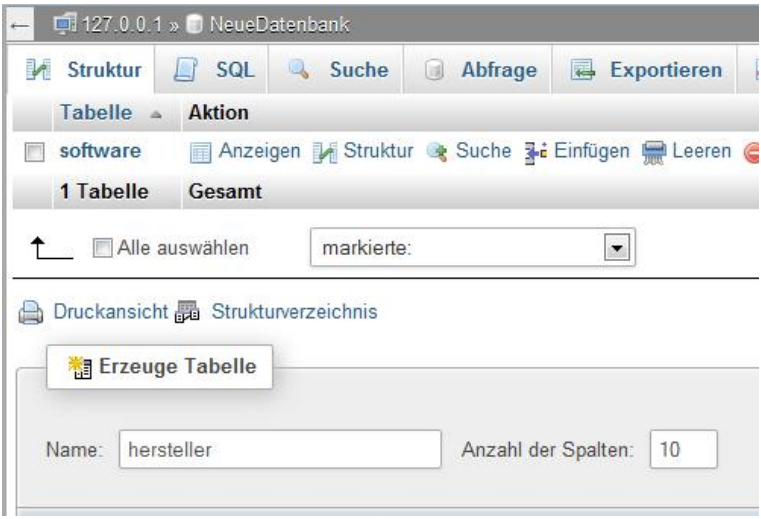
Damit das farbliche Hervorheben funktioniert, muss die Option *$cfg['BrowsePointerEnable']* auf *TRUE* gesetzt sein, wie es standardmäßig der Fall ist.

Das unmittelbare Bearbeiten von Tabelleneinträgen.

Die Einfügen-Ansicht hat eine weitere tolle Eigenschaft zu bieten: Sie können bestehende Einträge unmittelbar in der Tabellenübersicht bearbeiten. Dazu klicken Sie doppelt in die betreffende Zelle, um diese in den Bearbeitungsmodus zu versetzen. Nehmen Sie die gewünschten Änderungen vor und klicken Sie außerhalb der Tabelle, um die Änderung zu übernehmen.

In der Praxis erweitert man eine bestehende Datenbankstruktur oft mit zusätzlichen Tabellen. Wir wollen entsprechend unserem Beispiel die Informationen des Herstellers verfeinern und erzeugen dazu eine Tabelle mit Herstellerdetails.

Dazu öffnen Sie die Datenbankübersicht von *neueDatenbank*, bezeichnen die neue Tabelle in der Datenbank mit Hersteller und weisen ihr zehn Felder zu.



Eine neue Tabelle mit herstellerspezifischen Einstellungen entsteht.

Nach dem Bestätigen mit *OK* landen Sie in der Tabellenansicht, in der Sie entsprechend obiger Beschreibung die Tabellenfelder, die Typen, Feldlängen etc. definieren. So könnte man in unserem Beispiel folgende Felder einführen: *Firmenname*, *Straße*, *Postleitzahl*, *Stadt*, *Land*, *Telefon*, *Fax*, *Web*, *E-Mail* und *Ansprechpartner*. Natürlich sind auch hier weitere Verfeinerungen möglich.

Die Details für die Hersteller-Tabelle werden ausgearbeitet.

Auch hier können Sie wieder Kommentare, den Tabellentyp und die Sortierung festgelegen. Nach dem Speichern der Feldeinstellungen landen Sie wieder in der Tabellenübersicht, wo die durchgeführten Aktionen sowie die Tabellendetails angezeigt werden. Wenn Sie nun in die Anzeigenansicht wechseln, können Sie die Tabelle mit neuen Daten füttern.

4.7 Daten und Strukturen anpassen

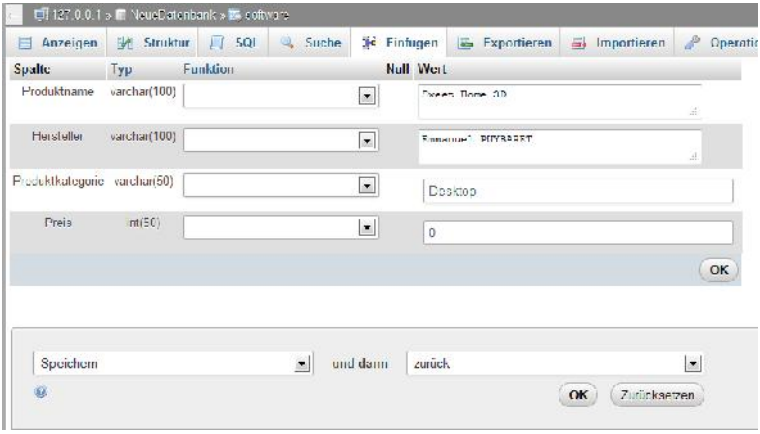
Einer der zentralen Vorzüge von Datenbanken ist, dass sich Datenbestände einfach aktualisieren und erweitern lassen und diese aktualisierten Informationen unterschiedlichen Mechanismen wie beispielsweise Content-Managementsystemen zur Verfügung stellen kann, durch die sie weiter verarbeitet oder für die Darstellungen aufbereitet werden.

In der Praxis müssen Daten bearbeitet, gelöscht und ergänzt werden. Schauen wir uns also an, wie Sie Daten mithilfe von phpMyAdmin im Datenbankserver anpassen. Um Tabellen zu bearbeiten, öffnen Sie diese und wechseln Sie in den Ansichtsmodus. Über das Stiftsymbol können Sie eine Tabelle editieren, über das Löschen-Symbol können Sie sie löschen. Die Position der Icons wird über folgende Konfigurationsoptionen bestimmt:

```
$cfg['PropertiesIconic'] = TRUE
$cfg['ModifyDeleteAtLeft'] = TRUE
$cfg['ModifyDeleteAtRight'] = FALSE
```

Für die Option *PropertiesIconic* können Sie die Werte *TRUE*, *FALSE* und *BOTH* setzen. Verwenden Sie *FALSE*, werden die Editier- und Löschfunktionen als Links angezeigt. *BOTH* zeigt die Icons und den Text an.

Klicken Sie auf das Editier-Symbol, öffnet sich der in nachstehender Abbildung dargestellte Dialog. Dieser ist recht flexibel ausgelegt. Hier können Sie nicht nur die bestehenden Werte und Funktionen bearbeiten, sondern die geänderten Werte auch als neuen Datensatz speichern – sofern das gewünscht ist. Aktivieren Sie hierzu die Option *Als neuen Datensatz speichern*.



Das Editieren eines Tabelleneintrags.

Unterhalb der Tabellenreihen finden Sie eine weitere wichtige Funktion, mit der Sie verschiedene Befehle alle Einträge auf einmal anwenden können. Klicken Sie hierzu auf *Alle auswählen* und wählen Sie dann aus dem Auswahlmenü die gewünschte Funktion aus, beispielsweise das Löschen, Drucken oder Exportieren.

Wie Sie obiger Abbildung sehr schön entnehmen können, erlaubt der Editierdialog auch die Verwendung von Funktionen, die auf Felder angewendet werden können. Diese Funktionen werden auf die Zeichenketten angewendet, die Sie in das Textfeld Wert eingeben.

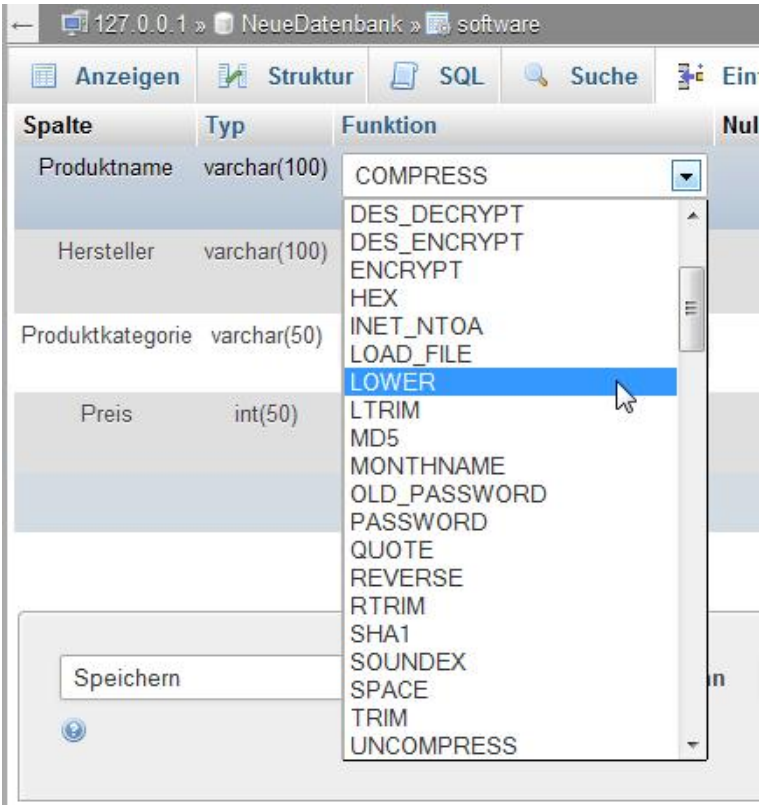
Insgesamt stehen Ihnen mehrere Duzend Funktionen zur Verfügung. Die wichtigsten sind in nachstehender Tabelle zusammengefasst (Details zu allen übrigen Funktionen finden Sie in der MySQL-Dokumentation unter *http://dev.mysql.com/doc/*):

Funktion	Beschreibung
ASCII (zeichenkette)	Das Editieren eines Tabelleneintrags. Diese Funktion gibt den ASCII-Code-Wert des äußersten linken Zeichens der Zeichenkette *zeichenkette* zurück.
CHAR(N,...)	Interpretiert die Argumente als Ganz-zahlen und gibt eine Zeichenkette zurück, die aus den Zeichen besteht, die durch die ASCII-Code-Werte dieser Ganzzahlen gegeben sind.
SOUNDEX (zeichenkette)	Gibt eine Soundex-Zeichenkette von *zeichenkette* zurück. Zwei Zeichenketten, die fast gleich klin-

	gen, sollten identische Soundex-Zeichenketten haben. Eine Standard-Soundex-Zeichenkette ist 4 Zeichen lang, aber die SOUNDEX()-Funktion gibt eine beliebig lange Zeichenkette zurück.
LOWER (zeichenkette)	Diese Funktion gibt die Zeichenkette *zeichenkette* zurück, bei der alle Zeichen in Kleinschreibung gemäß dem aktuellen Zeichensatz-Mapping (Vorgabe ist ISO-8859-1 Latin1) umgewandelt wurden. Aus *SOFTWARE-schmiede* wird dann *software-schmiede*.
UCASE	Diese Funktion gibt die Zeichenkette *zeichenkette* zurück, bei der alle Zeichen in Großschreibung gemäß dem aktuellen Zeichensatz-Mapping umgewandelt wurden. Aus *firma* wird dann *FIRMA*.
PASSWORD (zeichenkette)	Diese Funktion berechnet eine Passwort-Zeichenkette aus dem Klartext-Passwort zeichenkette. Diese wird eingesetzt, um MySQL-Passwörter zum Speichern in der Password-Spalte der user-Berechtigungstabelle zu verschlüsseln.
MD5 (zeichenkette)	Diese Funktion berechnet eine MD5-Prüfsumme für die Zeichenkette. Der Wert wird als eine 32 Stellen lange hexadezimale Zahl zurückgegeben.
ENCRYPT (zeichenkette[,salt])	Diese Funktion verschlüsselt *zeichenkette* unter Verwendung des Unix-crypt()-Systemaufrufs. Das salt-Argument sollte eine Zeichenkette mit zwei Zeichen sein.
LAST_INSERT_ID ([ausdruck])	Diese Funktion gibt den letzten automatisch erzeugten Wert zurück, der in eine *AUTO_INCREMENT*-Spalte eingefügt wurde.
USER()	Gibt den aktuellen MySQL-Benutzernamen zurück.
CONCAT (zeichenkette1,zeichenkette2,...)	Diese Funktion gibt die Zeichenkette zurück, die durch die Verkettung der Argumente entsteht. Gibt *NULL* zurück, wenn ein Argument *NULL* ist. Die Funktion unterstützt auch mehr als zwei Argumente.

Die Verfügbarkeit der Befehle wird ebenfalls über die phpMyAdmin-Konfigurationsdatei gesteuert. Sie können diese gezielt mit folgendem Abschnitt einschränken:

```
$cfg['RestrictFunctions'] = array(
    'FUNC_CHAR'   => array(
        'ASCII',
        'CHAR',
        'SOUNDEX',
        'LCASE',
        'UCASE',
        'PASSWORD',
        'MD5',
        'SHA1',
        'ENCRYPT',
        'LAST_INSERT_ID',
        'USER',
        'CONCAT'
    ),
```



Die Auswahl von Funktionen, die Sie anwenden können.

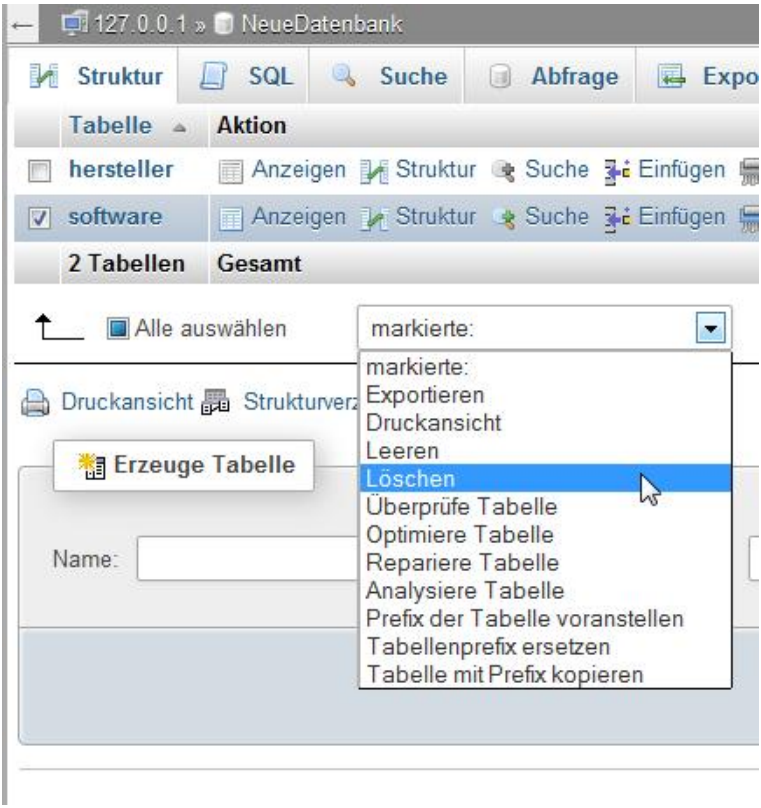
Neben dem Bearbeiten von Datensätzen unterstützt phpMyAdmin auch verschiedene Löschvorgänge, insbesondere das Löschen von

- einzelnen Reihen in einer Tabelle
- mehreren Reihen in einer Tabelle
- allen Reihen in einer Tabelle
- allen Reihen in mehreren Tabellen

Vor dem endgültigen Löschvorgang erfolgt eine Sicherheitsabfrage, ob die Daten tatsächlich entfernt werden sollen.

Die drei erstgenannten Aktionen sind recht einfach durchzuführen. Dazu markieren Sie einfach eine einzelne, mehrere oder alle Datenreihen und führen dann den Befehl *Löschen* aus. phpMyAdmin fragt sicherheitshalber nach, ob die angegebene(n) Reihe(n) tatsächlich gelöscht werden soll(en). Den Löschvorgang schließen Sie mit einem Klick auf *OK* ab.

Um alle Reihen aus mehreren Tabellen zu löschen, wechseln Sie zur Datenbankansicht, markieren dort die gewünschten Tabellen und führen dann aus dem Auswahlmenü die Funktion *Löschen* aus.

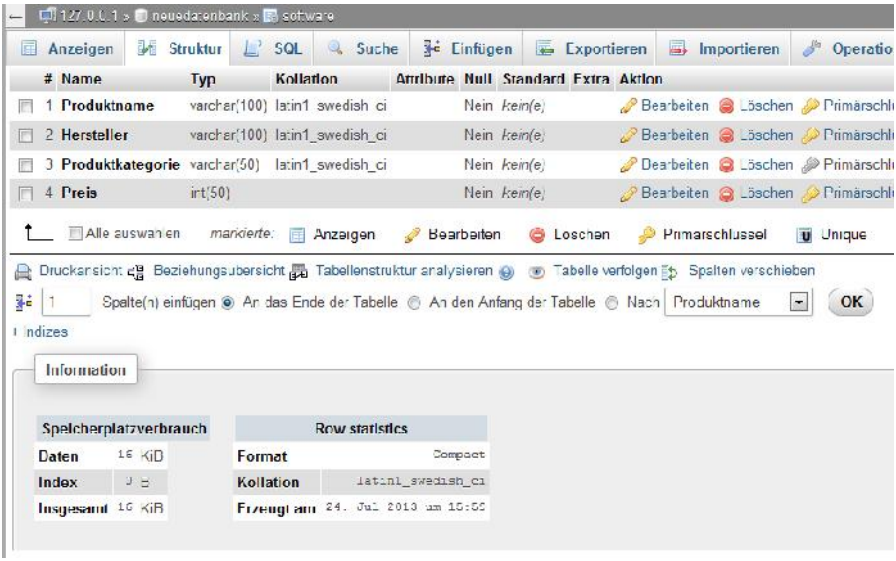


So einfach ist das Löschen einer Tabelle: Markieren und aus dem Auswahlmenü den *Löschen*-Befehl verwenden.

Wenn Sie ganze Tabellen löschen, klicken Sie in der oberen Symbolleiste auf *Löschen*. Natürlich lassen sich auch ganze Datenbanken löschen. Dazu wechseln Sie zur Datenbank-Übersicht, markieren die zu löschende Datenbank und klicken im unteren Dialogbereich auf die Schaltfläche *Löschen*.

4.7.1 Tabellenstruktur bearbeiten

Eine weitere wichtige Anforderung an moderne Datenbankmanagementsysteme ist, dass sie die Bearbeitung der Datenbankstruktur, genauer der Tabellenstruktur erlauben. Auch für diesen Aufgabenbereich ist phpMyAdmin gerüstet. Ein wichtiges Hilfsmittel für die Bearbeitung der Tabellenstruktur ist die Strukturansicht. Auf diese Ansicht greifen Sie zu, in dem Sie über die Navigationsleiste die gewünschte Tabelle auswählen und dann im Arbeitsbereich auf *Struktur* klicken.



Die Strukturansicht der erzeugten Tabelle erlaubt die Umstrukturierung.

Anhand eines Beispiels wird deutlich, wie Sie in der Praxis bei der Umstrukturierung und beim Ausbau vorgehen – und warum das sinnvoll ist. Dazu kehren wir zur oben erzeugten Tabelle *Software* zurück und stellen uns vor, dass für die Software weitere Informationen wie beispielsweise eine Beschreibung oder die verfügbaren Sprachversionen in der Datenbank aufgeführt werden sollen.

Um eine oder auch mehrere neue Zeilen einzufügen, geben Sie unter *Spalte(n) hinzufügen* die gewünschte Anzahl an. phpMyAdmin geht standardmäßig davon aus, dass die neuen Zeilen am Ende der Tabelle angefügt werden. Daher ist auch die Option *An das Ende der Tabelle* aktiv.

Soll die neue Zeile an den Anfang gesetzt werden, so aktivieren Sie die Option *An den Anfang der Tabelle*. Außerdem können Sie die neue Zeile über das Auswahlmenü *Nach* an eine beliebig zu bestimmende Position setzen. Die neue Zeile wird durch einen Klick auf *OK* erzeugt und an die gewünschte Position gesetzt.

Sollen die neuen Felder nicht untereinander, sondern nebeneinander angeordnet werden, so muss einmal mehr die phpMyAdmin-Konfigurationsdatei angepasst werden. Dort finden Sie die beiden relevanten Einstellungen:

```
$cfg['DefaultDisplay'] = 'horizontal'
$cfg['DefaultPropDisplay'] = 'horizontal'
```

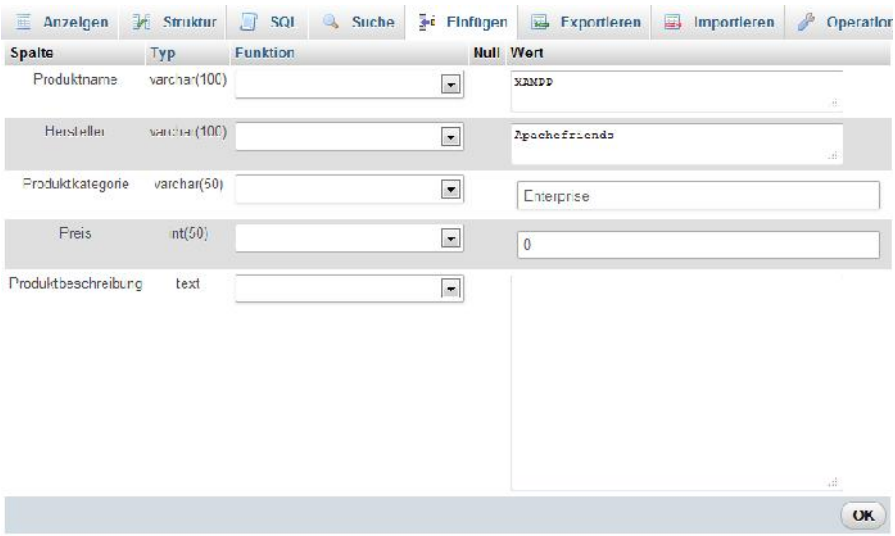
Die obere Option ist für die allgemeine Darstellung der Tabellenzeilen zuständig, die untere bestimmt die Anordnung der Zeilen, die geändert bzw. neu hinzugefügt werden.

Sollen neue bzw. zu ändernde Zeilen nebeneinander angeordnet werden, so setzen Sie den Wert auf *vertical*.

4.7.2 Mit Text arbeiten

In Datenbanken werden nicht nur kurze Daten wie beispielsweise Kontaktinformationen verwaltet, sondern oft auch Produkt- oder Servicebeschreibung. Da es sich bei Textelementen oftmals um mehr oder minder aufwändige Textbausteine handelt, sollten diese auch in den Datenbankentwurf und die Struktur einfließen.

Wir wollen an unser Beispiel anknüpfen und erzeugen in der Tabelle *Software* das Feld *Produktbeschreibung*. Wichtig dabei: Wählen Sie als Feldtyp die Option *Text* aus. Über die phpMyAdmin-Konfigurationsdatei können Sie das Layout des Eingabefeldes anpassen.



Das erweiterte Textfeld vereinfacht die Eingabe größerer Textbausteine.

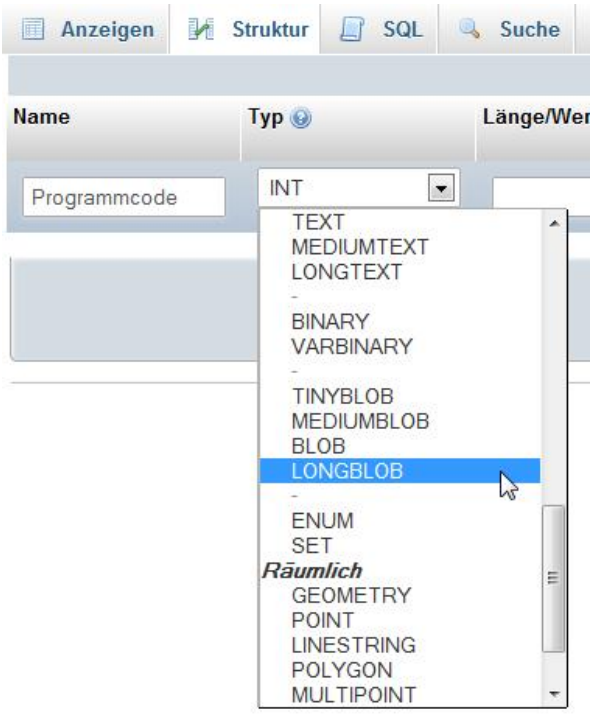
Nachdem Sie das neue Textfeld erzeugt haben, wechseln Sie in den Eingabemodus. Hier präsentiert sich Ihnen ein Eingabefeld entsprechend obiger Abbildung. Die Größe des Textfelds wird in der phpMyAdmin-Konfigurationsdatei mit folgender Einstellung definiert:

```
$cfg['TextareaCols']        = 40
$cfg['TextareaRows']        = 7
```

Das bedeutet, dass ein Textfeld 40 Zeichen breit und 7 Zeilen hoch ist. Sollten diese Voreinstellungen nicht den jeweiligen Anforderungen entsprechen, so können Sie sie beliebig anpassen. Geht der Text über den vorgegebenen Platz hinaus, ist er über die Scroll-Leiste verfügbar. Die phpMyAdmin-Konfigurationsdatei unterstützt einen weiteren Schalter für die Konfiguration von Textfeldern:

```
$cfg['LongtextDoubleTextarea'] = TRUE
```

Dieser sorgt für eine Doppelung der Textfeldgröße für Langtextfelder. Natürlich sollten Sie die erzeugten Textfelder auch nutzen und über die *Einfügen*-Ansicht füllen.



Ein neues Feld als Ablage für Binärdaten entsteht.

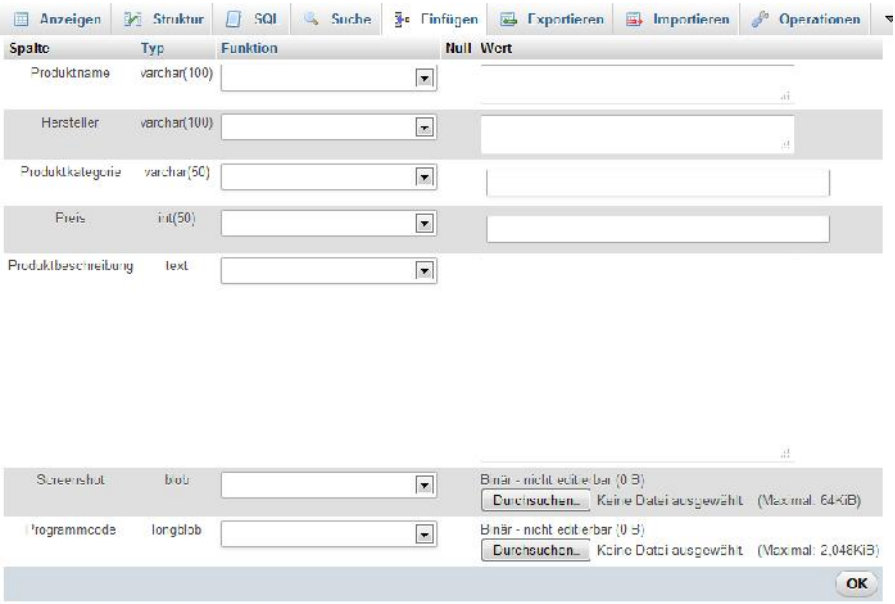
4.7.3 Binärdaten verwalten

Sie können in einer Datenbank natürlich nicht nur ACSII-basierte Daten, sondern auch binäre Daten verwalten. Konkret können Sie in MySQL beispielsweise Grafiken, Programme, Musikdateien etc. in der Ablage hinterlegen. Für die Verwaltung von Binärdaten ist die Einführung eines entsprechenden Feldes vom Typ BLOB (Binary Large Object) erforderlich. Ein BLOB ist ein großes Binärobjekt, das eine variable Menge von Daten enthalten kann. Man unterscheidet zwischen vier BLOB-Typen:

- TINYBLOB
- BLOB
- MEDIUMBLOB
- LONGBLOB

Diese unterscheiden sich nur hinsichtlich der maximalen Länge der Werte, die sie aufnehmen können. Wir wollen in unserer Datenbank zwei Felder einführen, die binäre Daten verwalten: Screenshot und Programmcode. Nach dem Speichern sind die beiden neuen Felder verfügbar.

Wechseln Sie nun zur jeweiligen Tabelle und zur Strukturansicht und fügen Sie entsprechend obiger Beschreibung ein neues Feld hinzu, in dem Sie in das Eingabefeld *Felder hinzufügen* den Wert 1 eingeben und die Position bestimmen. Klicken Sie auf *OK* und weisen Sie dann dem neuen Feld die Bezeichnung *Screenshot* zu. Entsprechend gehen Sie mit dem Feld *Programmcode* vor.



Die beiden neuen BLOB-Felder dienen als Ablage für binäre Daten.

4.7.4 ENUM- und SET-Typ

Wenn es darum geht, Datenbanktabellen mit Informationen zu füttern, sind zwei weitere Typen von besonderer Bedeutung: *ENUM* und *SET*. Beide Typen dienen dazu, eine Liste möglicher Werte zu repräsentieren. Der Unterschied zwischen beiden: Während man beim ENUM-Typ lediglich einen Wert aus einer Liste vor-

definierter Werte wählen kann, erlaubt *SET* die Verwendung mehrerer Werte in einer Zelle.

Etwas genauer: Ein *ENUM* ist ein Zeichenkettenobjekt, dessen Wert normalerweise aus einer Liste zulässiger Werte ausgesucht wird, die explizit bei der Spaltenspezifizierung während der Tabellenerzeugung aufgezählt werden. Der Wert kann unter bestimmten Umständen auch eine leere Zeichenkette oder *NULL* sein.

Ein ENUM-Feld entsteht.

Ein *SET* ist ebenfalls ein Zeichenkettenobjekt, das 0 oder mehrere Werte haben kann, wovon jedes aus einer Auflistung zulässiger Werte stammen muss, die bei der Tabellenerzeugung festgelegt wurden. *SET*-Spaltenwerte, die aus mehrfachen *SET*-Elementen bestehen, werden angegeben, indem die Elemente durch Kommas getrennt werden. *SET*-Elemente dürfen selbst keine Kommas enthalten. Eine Spalte, die z. B. als *SET("eins", "zwei") NOT NULL* festgelegt wurde, kann folgende Werte haben:

```
""
"eins"
"zwei"
"eins,zwei"
```

Wichtig ist außerdem, dass SET maximal 64 unterschiedliche Elemente besitzen kann.

Anhand eines Beispiels wird der Einsatz des Feldtyps deutlich. Dazu wechseln Sie wieder in die Tabellenansicht der Tabelle *Software* und erzeugen ein neues Feld.

Dieses bezeichnen Sie mit *Lizenz*, wählen als Feldtyp *ENUM* und geben als Wert folgendes an:

```
'GPL', 'Kommerziell', 'Sonstige'
```

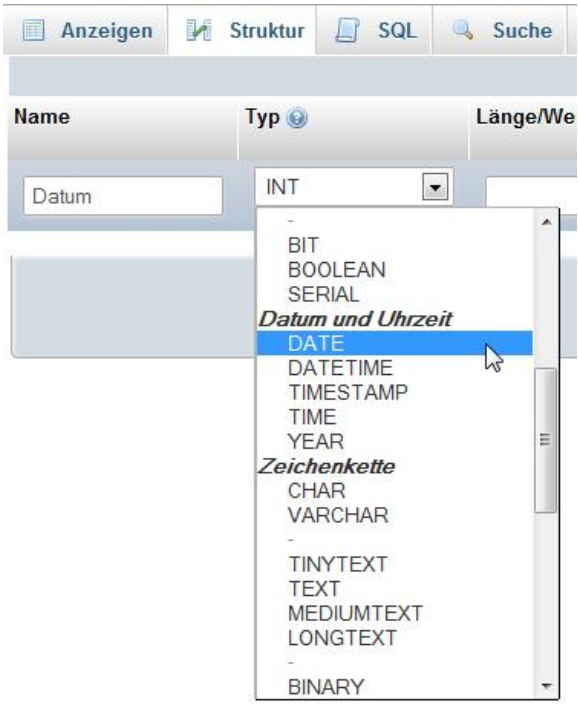
Über das Register *Einfügen* kann nun für jedes Softwareprodukt die zutreffende Lizenz aus dem Auswahlmenü ausgewählt werden.

Abschließend erzeugen Sie ein neues Feld mit einem Klick auf *Speichern*. Dann wechseln Sie zum Einfügen-Register. Dort finden Sie in der Zeile *Lizenz* das Auswahlmenü mit den drei Optionen *GPL*, *Kommerziell* und *Sonstige*.

Bei der *ENUM*-Auswahlliste können Sie wie oben beschrieben, lediglich einen Wert zuordnen. Anders ist das bei der *SET*-Variante. Hier können Sie über ein Auswahlmenü mehrere Einträge markieren.

4.7.5 Umgang mit Zeitwerten

Mithilfe von phpMyAdmin können Sie in einer MySQL-Datenbank auch Zeitinformationen verwalten. Hierfür kommen insbesondere die Datums- und Zeit-Typen *DATETIME*, *DATE*, *TIMESTAMP*, *TIME* und *YEAR* zum Einsatz. Jeder dieser Typen hat einen zulässigen Wertebereich sowie einen Nullwert, der benutzt wird, wenn man einen unzulässigen Wert speichern will.



Das Auswahlmenü bietet Ihnen verschiedene Zeittypen an.

Dabei sollten Sie beachten, dass MySQL das Speichern von bestimmten Datumswerten zulässt, wie beispielsweise 1999-11-31, auch wenn diese an sich nicht gültig sind. Der Grund hierfür: Datumsüberprüfungen liegen in der Verantwortung der Applikation, nicht des SQL-Servers.

Wie gehen Sie nun mit diesen Datentypen um? Einsatzbereiche für eine Datumsinformation gibt es zu Genüge. In der bisher erzeugten Datenbank wäre beispielsweise die Angabe von Interesse, wann eine Software zum ersten Mal auf dem Markt positioniert und wann das letzte Release veröffentlicht wurde.

Entsprechend diesem Beispiel wollen wir ein neues Feld *Markteinführung* erzeugen. Dazu öffnen Sie die Tabelle *Software* und erzeugen ein neues Feld, bezeichnen dieses mit *Markteinführung* und wählen als Typ *DATE*.

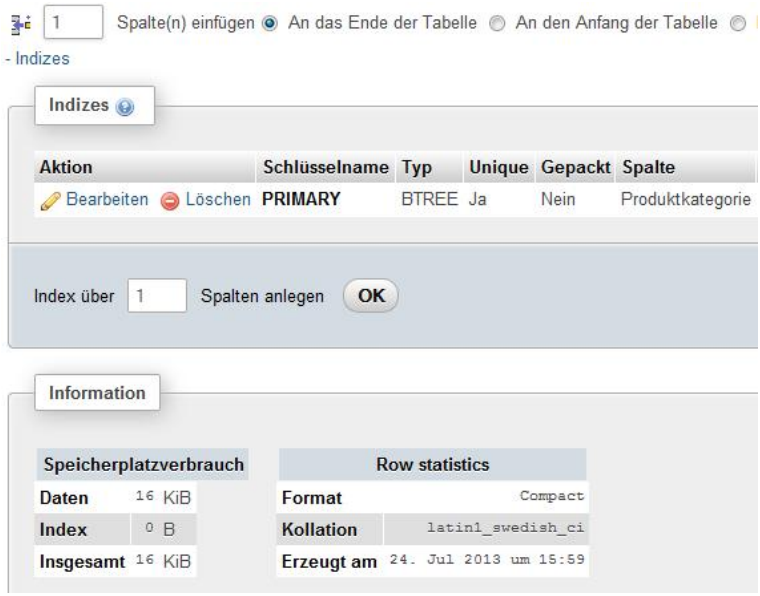
Nachdem Sie das neue Feld mit einem Klick auf *Speichern* gesichert haben, wechseln Sie zum *Einfügen*-Dialog. Dort taucht dann das Datum-Eingabefeld auf. Über das Kalender-Icon öffnen Sie ein Pop-up-Fenster, das die Terminwahl vereinfacht.

Erzeugen Sie ein *DATETIME*- oder *TIMESTAMP*-Feld, so kann über das Pop-up-Fenster auch der Zeitpunkt bestimmt werden.

4.7.6 Umgang mit Indizes

Datenbanken verwenden Indizes, um Zeilen mit einem bestimmten Spaltenwert schnell aufzuspüren. Ohne solche Kennzeichnung müsste MySQL bei der Datensuche beim ersten Datensatz anfangen und dann durch die gesamte Tabelle lesen, bis die relevanten Zeilen gefunden werden.

Es versteht sich von selbst, dass dieser Vorgang umso länger dauert, je größer die Tabelle ist. Wenn die Tabellen für die in Frage kommenden Zeilen einen Index besitzen, kann MySQL schnell eine Position finden. Bei einer Tabelle mit tausend Zeilen ist dieser Vorgang laut MySQL-Website mindestens 100-mal schneller als sequentielles Lesen.



Die Index-Details zu einer Datenbanktabelle.

MySQL unterstützt verschiedene Index-Typen. Die MySQL-Indizes *PRIMARY*, *UNIQUE* und *INDEX* sind in so genannten B-Bäumen gespeichert. Zeichenketten

werden automatisch Präfix-komprimiert, ebenso wie Leerzeichen am Ende. In der Strukturansicht haben Sie Zugriff auf die Index-Einstellungen einer Tabelle. Klicken Sie dazu auf den Link, um damit die Index-Funktionen aufzuklappen.

phpMyAdmin unterstützt verschiedene Index-Typen. Man unterscheidet insbesondere zwischen Einzel- und Mehrfeldindizes. Die zugehörigen Einstellungen sind über die Strukturansicht verfügbar. Dort erkennen Sie direkt, um welchen der beiden Typen es sich im Einzelfall handelt.

Wenn Sie einen Index-Eintrag über eine oder mehrere Spalten hinweg hinzufügen wollen, so geben Sie einfach die Anzahl der Indizes an und bestätigen mit *OK*. Es öffnet sich das in nachstehender Abbildung dargestellte Formular, in dem Sie die Details wie Indexnamen, Typ, Felder und Größen festlegen.

Nach dem Speichern finden Sie den neu erzeugten Index in der Strukturübersicht. Dort kann er wieder editiert werden.

Ein neuer Index-Eintrag entsteht.

Speziell für die Anforderungen von Volltextsuchen in der Datenbank wurde der Indextyp *FULLTEXT* geschaffen. Er unterstützt insbesondere Textfelder und kann für die gezielte Indizierung dort gespeicherter Daten verwendet werden. Besonders einfach ist das Setzen von Indexeinträgen übrigens über die Feldliste. Dort klicken Sie unter *Aktion* einfach auf den gewünschten Indextyp, und schon wird er in der Indexübersicht aufgeführt.

Über die *Aktion*-Spalten ist es ein Leichtes, einen Index zu setzen.

Ob die Indizes den gewünschten Effekt einer schnellen Suche erzielen, lässt sich mittels Stichproben herausfinden. Führen Sie einfach verschiedene Datenbankabfragen durch, und zwar einmal mit einem indizierten Begriff und das andere Mal mit einem nicht indizierten Begriff. Aus den Bearbeitungszeiten lässt sich exakt auslesen, wie groß die zeitlichen Unterschiede bei der jeweiligen Installation sind. In unserem Beispiel führen Sie dazu auf dem SQL-Dialog den folgenden Befehl aus:

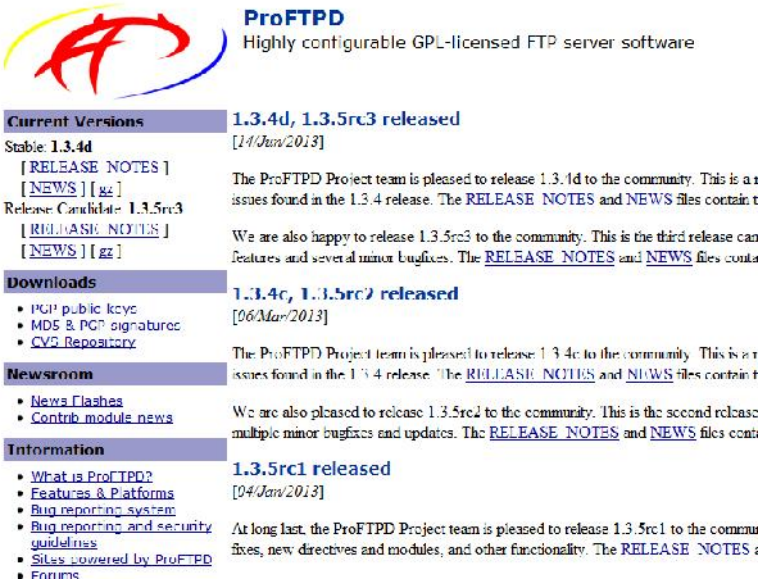
```
SELECT *
FROM `Software`
WHERE Preis =1000
LIMIT 0 , 30
```

In der Ergebnisausgabe finden Sie den Verweis *SQL erklären*, dem Sie nützliche Informationen entnehmen können.

5 ProFTPD

Ein weiteres zentrales Werkzeug einer XAMPP-Installation ist der FTP-Server ProFTPD. Er zählt zu den verbreitetsten FTP-Servern für Unix-Plattformen (Linux, BSD, Solaris etc.), Mac OS X und Windows (unter Cygwin). Sie benötigen ihn beispielsweise, um Inhalte auf Ihre XAMPP-Installation von Drittsystemen zu übertragen.

Im Unterschied zur Windows-Variante von XAMPP ist unter Linux leider keine grafische Schnittstelle für die Administration des FTP-Servers integriert. Unter Windows kommt mit FileZilla allerdings auch ein anderer Server zum Einsatz. Schade, denn es gibt einige ganz brauchbare Lösungen. Daher müssen Sie sich auf die Konfiguration und Nutzung des Servers auf Konsolenebene beschränken.



Auf der ProFTPD-Homepage finden Sie jede Menge Informationen rund um den FTP-Server.

5.1 ProFTPD-Basics

Für den Einsatz von ProFTPD sprechen verschiedene Punkte:

- ProFTPD ist recht einfach zu konfigurieren.
- Es ist ein sehr bewährter Server mit einem hohen Reifegrad.
- Der FTP-Server unterstützt Virtual Hosts.
- Die Benutzerauthentifizierung per SQL, LDAP und RADIUS ist möglich.
- Und vieles mehr …

Der ProFTPD ist bereits seit Langem im XAMPP-Paket integriert. Kein Wunder angesichts der interessanten Funktionen. XAMPP installiert den ProFTPD-Server in sein Standardverzeichnis */opt/lampp/*. Sie steuern den Server über die ProFTPD-Konfigurationsdatei */opt/lampp/etc/proftpd.conf*. In ihr legen Sie fest, wer den Server nutzen darf, ob der Zugriff geschützt erfolgt und ob Sie virtuelle FTP-Hosts einrichten wollen.

Editieren Sie diese mit einem Editor Ihrer Wahl, um die ProFTPD-Konfiguration entsprechend Ihren Anforderungen anzupassen.

Bevor Sie sich allerdings an das Bearbeiten der Konfigurationsdatei machen, sollten Sie zwei Dinge wissen, die beim Zusammenspiel von ProFTPD und XAMPP wichtig sind:

- ProFTPD ist so konfiguriert, dass sich der Benutzer *nobody* mit dem Passwort *lampp* Zugriff auf den FTP-Server verschaffen kann (siehe Sicherheitscheck).
- Der Zugriff ist auf das Verzeichnis */opt/lampp/htdocs* beschränkt.

Beide Einstellungen können Sie natürlich mit Eingriffen ändern. Die ProFTPD-Konfigurationsdatei Ihrer XAMPP-für-Linux-Installation sieht standardmäßig wie folgt aus:

```
# Grundlegende ProFTPD-Konfigurationsdatei proftpd.conf.
# Sie richtet einen einfachen FTP-Server mit einem
# anonymen Log-in ein. Die Konfiguration geht davon aus,
# dass Sie die Benutzer/Gruppe nobody und ftp für die
# typischen FTP-Operationen verwenden.

ServerName                  "ProFTPD"

ServerType                  standalone
```

```
DefaultServer             on

# Port 21 ist der Standard-FTP-Port.

Port                      21


# Umask 022 ist eine gute Einstellung, um zu verhindern,
# dass neue Dateien und Verzeichnisse von Gruppen und
# weltweit gelesen werden können.

Umask                     022


# Um DoS-Attacken zu verhindern, sollten Sie die Anzahl
# der Kindprozesse auf maximal 30 beschränken.

MaxInstances              30


# Hier bestimmen Sie die Benutzer und Gruppen, die den
# Server nutzen.

User                      nobody

Gruppe                    nogroup


# Normalerweise sollten die Dateien überschrieben
# werden können.

<Directory /opt/lampp/htdocs/*>

AllowOverwrite            on

</Directory>


# Diese Einstellung ist für den Webserver-Content relevant.

DefaultRoot /opt/lampp/htdocs


# Der Benutzer nobody hat das Passwort lampp
# (hier verschlüsselt).

UserPassword nobody wRPBu8u4YP0CY


# Der Benutzer nobody ist kein normaler Benutzer, daher
# muss hier die Shell deaktiviert werden.
```

```
RequireValidShell off

# Der Benutzer nobody kann auch in der Datei
# /etc/ftpusers eingetragen sein. Hiermit ignorieren
# Sie die Einstellungen in dieser Datei.

UseFtpUsers off
```

Wie Sie voranstehendem Beispiel entnehmen können, ist die Grundkonfiguration recht einfach. Sie kann allerdings auch sehr umfangreich werden, wie wir noch sehen werden.

5.2 ProFTPD-Konfiguration

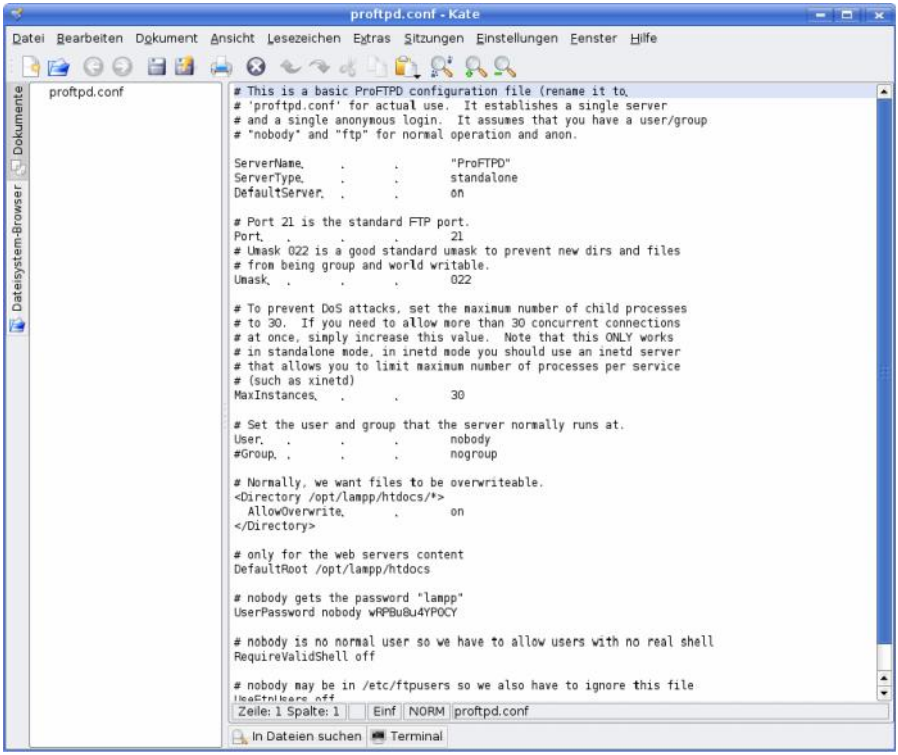
Mit die wichtigste Aufgabe der ProFTPD-Konfigurationsdatei ist die Steuerung des Zugriffs auf den Server. Standardmäßig liest der ProFTPD die */etc/passwd*-Datei ein, um User zu authentifizieren. Sie müssen also einfach nur einen neuen System-Benutzer anlegen, damit sich dieser per FTP anmelden kann.

Gelegentlich braucht man schon mal virtuelle User, die nicht im System existieren. Auch hierfür gibt es eine einfache Lösung: Und zwar lassen sich diese mit der AuthUserFile-Anweisung anlegen.

Wie bereits oben erwähnt, unterstützt ProFTPD eine weitere Möglichkeit, Benutzer zu authentifizieren: Sie können auf SQL-Datenbanken, einen LDAP-Verzeichnisdienst oder auf RADIUS zurückgreifen. Diese Funktionen werden mit den Modulen *mod_sql*, *mod_ldap* und *mod_radius* realisiert.

Für die Konfiguration des anonymen Zugangs ist der <*Anonymous*>-Bereich der Konfigurationsdatei zuständig. Enthält Ihre Konfiguration keinen <*Anonymous*>-Bereich, ist ein anonymer Zugang nicht möglich. In der <*Anonymous*>-Direktive gibt die User-Angabe in der Sektion an, welcher Username als anonymer Zugang benutzt wird. Anonyme Zugänge werden grundsätzlich automatisch gechrooted, also eingesperrt.

Alle normalen, nicht anonymen Zugänge können mit der Defaultroot-Anweisung eingesperrt werden. Damit beschränken Sie den Zugriff Ihrer Benutzer auf ein anzugebendes Verzeichnis. Gleichzeitig verhindern Sie, dass diese Zugriff auf höhere Verzeichnisstrukturen haben.



Mit einem Editor wie Kate ist es ein Leichtes, Änderungen an der ProFTPD-Konfigurationsdatei vorzunehmen.

Wenn Sie auch einen virtuellen FTP-Server mit den <*VirtualHost*>-Bereichen erstellen wollen, müssen Sie einige Dinge beachten. So muss sichergestellt sein, dass bei der Verwendung von DNS-Namen der DNS-Name auf eine andere IP als den Defaultserver verweist. Oft wird angenommen, dass virtuelle Server unter ProFTPD ähnlich wie der Apache agieren. Dem ist leider nicht so, da das FTP-Protokoll keine auf Namen basierenden virtuellen Server unterstützt. Daher sind virtuelle Server nur bei unterschiedlichen IP-Adressen möglich oder wenn sie unterschiedliche Ports verwenden.

Wenn Sie unterschiedliche Ports verwenden wollen, sollten Sie beachten, dass bei aktivem Transfer der Kontrollport-1 als Datenport verwendet wird, also bei Port 21 der Port 21-1=20.

Der ProFTPD bietet Ihnen verschiedene Optionen zur Beschränkung des Zugriffs und der Ressourcen. Viele Seiten haben bestimmte Verzeichnisse für Upload bzw. Download, andere erlauben kein Listen der Verzeichnisse etc. Dieses Verhalten erzielen Sie durch die richtige Kombination der <*Directory*>- und <*Limit*>-Direktiven.

Der Einsatz der Directory-Anweisung ist in der Regel recht einfach. Hiermit steuern Sie die Rechte für Ihre Verzeichnisse. Beachten Sie zunächst, dass der FTP-Server mit verschachtelten Directory-Angaben nichts anfangen kann. ProFTPD bestimmt automatisch den Bezug von Directory-Pfadangaben, abhängig von den angegebenen Verzeichnissen und der jeweiligen Konfiguration.

Achten Sie außerdem bei der Pfadangabe darauf, immer den absoluten Pfad zu verwenden, und zwar unabhängig davon, ob das Verzeichnis ggf. in einer geschützten Umgebung angesprochen wird, also durch *anonymous* oder *defaultroot*. Beachten Sie allerdings, dass es auch zwei zulässige Ausnahmen von dieser Regel gibt:

- **Ausnahme 1**: Der Pfad besitzt das ~-Präfix.
- **Ausnahme 2**: Der Pfad liegt innerhalb des Anonymous-Bereichs.

Soll die Anweisung in den Anonymous-Bereich eingetragen werden, können Sie auch einen relativen Pfad verwenden (ohne das führende /). Er wird dann relativ zur anonymen Verzeichnisangabe ausgewertet.

Als ProFTPD-Administrator sollten Sie außerdem die Befehle *APPE*, *RETR*, *STOR* und *STOU FTP* kennen. Hier wird die Directory-Pfadangabe mit angehängten Dateinamen überprüft. Dies wird meistens keine Auswirkung haben, jedoch gibt es Sonderfälle. Angenommen, Sie verwenden /*, um die Limit-Anweisungen auf die Unterverzeichnisse eines Verzeichnisses zu beschränken, nicht jedoch auf das Verzeichnis selbst. Die folgende Beispielkonfiguration zeigt, wie man dem Benutzer User anonyme Uploads nur in das Unterverzeichnis *upload* erlaubt.

```
<Anonymous ~ftp>
User ftp
Group ftp
UserAlias anonymous ftp
<Limit WRITE>
DenyAll
</Limit>
```

```
<Directory upload/*>
<Limit STOR>
AllowAll
</Limit>
</Directory>
</Anonymous>
```

Sie können Zugriffsbeschränkungen auch mit der Datei *.ftpaccess* (die Apache-Konfiguration lässt grüßen) in der *proftpd.conf* für bestimmte Verzeichnisse überschreiben.

Ein sehr wichtiges Mittel sind die Limit-Anweisungen. Damit können Sie komplexe und detaillierte Zugriffsrechte definieren, wobei Sie beispielsweise festlegen, wer welche FTP-Befehle ausführen kann. Auch bei diesen Einstellungen gibt es wieder verschiedene Dinge zu beachten.

Mit am Schwierigsten ist es, ein Verständnis für die Reihenfolge der Verarbeitung zu entwickeln, in der Limit-Anweisungen ausgewertet werden.

Zunächst einmal unterscheiden wir zwischen drei Arten von Befehlen: Raw, den eigentlichen FTP-Befehlen, Gruppen von FTP-Befehlen und dem ALL-Keyword:

- **Raw-FTP-Befehle**: Das sind die eigentlichen FTP-Befehle inklusive der RFC-konformen X-Varianten.
- **Gruppen von FTP-Befehlen**: Hier unterscheidet man zwischen verschiedenen Gruppen:
    - DIRS (FTP-Befehle, die mit Verzeichnissen zu tun haben): CDUP, CWD, LIST, MDTM, NLST, PWD, RNFR, STAT, XCUP, XCWD, XPWD.
    - LOGIN: Client-Log-ins
    - READ (FTP-Befehle, die etwas mit dem Lesen zu tun haben): RETR, SIZE.
    - WRITE (FTP-Befehle, die mit dem Schreiben zu tun haben): APPE, DELE, MKD, RMD, RNTO, STOR, STOU, XMKD, XRMD.
- **ALL**: Alle FTP-Befehle.

Wichtig für die Reihenfolge: Limit-Anweisungen, die Raw-Befehle verwenden, haben die höchste Priorität, gefolgt von Limit-Anweisungen, die Befehlsgruppen verwenden. Anweisungen mit dem ALL-Keyword haben die niedrigste Priorität.

Enthält nun eine Limit-Anweisung sowohl Raw-Befehle als auch Gruppen, so kommt es auf die Reihenfolge der Limit-Anweisungen in der *proftpd.conf* an, die die FTP-Befehle verwenden.

Limit-Blöcke werden meist innerhalb einer Directory-Anweisung in der *proftpd.conf* verwendet. Das bedeutet, dass die Limit-Anweisung auch für die Unterverzeichnisse rekursiv gültig ist, solange keine bessere Beschränkung gefunden wird, deren Directory-Angabe besser passt. Das bedeutet, dass Sie z. B. erst einmal alle FTP-Befehle verbieten können, um dann in Unterverzeichnissen die notwendigen READ- oder WRITE-Befehle zu erlauben (z. B. in *pub* oder *incoming*).

Vorsicht ist bei der Verwendung von *AllowUser* geboten. Man verwendet diese Direktive, um einen einzelnen User bestimmte Befehle ausführen zu lassen. ProFTPD benutzt die gleiche Funktion, um *AllowUser* und *AllowGroup* (und andere Befehle) auszuwerten. Die Auswertung erfolgt als logisches UND, und so müssen alle Angaben stimmen, damit der Befehl ausgeführt werden darf.

Bei AllowGroup ist das sinnvoll und erleichtert Ihnen die Administration. Keinen Sinn macht es bei AllowUser, da ein User ja eindeutig identifiziert ist. Das können Sie umgehen, indem Sie die User einzeln auflisten. Aus

```
AllowUser klaus,thomas,michael
```

wird dann folgende Konfiguration:

```
AllowUser klaus
AllowUser thomas
AllowUser michael
```

Sie können auch folgende Konfiguration verwenden:

```
AllowUser OR  klaus,thomas,michael
```

Vorsicht ist auch bei der Reihenfolge der Allow- und Deny-Einträge geboten. Vorsicht deshalb, weil es hier Unterschiede zwischen ProFTPD und Apache gibt. Wenn Sie beim Apache die Reihenfolge *Allow,Deny* verwenden, so bedeutet das, dass der Zugang grundsätzlich verweigert wird, außer wenn der Zugang vorher

explizit erlaubt wird. Die Reihenfolge *Deny,Allow* hingegen erlaubt bei Apache grundsätzlich den Zugang, außer wenn dieser vorher ausdrücklich verboten wurde.

Beim ProFTPD ist das dummerweise anders. Hier erlaubt die Reihenfolge *Allow,Deny* grundsätzlich den Zugang, solange er nicht durch eine *Deny*-Direktive verboten wird. Die Konfiguration *Deny,Allow* verweigert also den Zugriff grundsätzlich, sofern er nicht ausdrücklich erlaubt wurde.

Hier ein Beispiel zur konkreten Verwendung von *<Limit>*. Sie zeigt eine häufige Konfiguration, bei der nur der Upload in das Verzeichnis zulässig ist:

```
<Directory /path/to/uploads>
<Limit ALL>
DenyAll
</Limit>
<Limit CDUP CWD XCWD XCUP>
AllowAll
</Limit>
<Limit STOR STOU>
AllowAll
</Limit>
</Directory>
```

Mit dem <Limit ALL>-Bereich wird die Verwendung aller FTP-Befehle innerhalb des /path/to/uploads-Verzeichnisses blockiert.

Als Nächstes werden die FTP-Befehle bestimmt, die Sie zulassen wollen. Die CDUP- und CWD-Befehle sollten Sie zulassen, damit die User in dieses Verzeichnis wechseln können und wieder heraus. Dann lassen Sie die Ausführung von *STOR* und *STOU* zu, damit die Benutzer Dateien in das Verzeichnis hochladen können.

Ein weiteres Beispiel zeigt, wie Sie ein sogenanntes blindes Verzeichnis erstellen, in dem der User zwar Dateien hoch- und herunterladen kann, aber nicht zu sehen bekommt, was in dem Verzeichnis ist:

```
<Directory /path/to/dir>
<Limit LIST NLST>
DenyAll
```

```
</Limit>
</Directory>
```

Wie Sie voranstehendem Beispiel entnehmen können, ist die Konfiguration mit minimalem Aufwand erstellt. Standardmäßig sind hier alle Befehle zugelassen, lediglich die beiden FTP-Befehle *LIST* und *NLST* sind ausgenommen, die zum Listen des Verzeichnisinhalts verwendet werden.

Sie können auf diesem Weg auch den FTP-Zugang nur für bestimmte User freigeben. Dazu verwenden Sie die Befehlsgruppe *LOGIN*:

```
<Limit LOGIN>
AllowUser peter
AllowUser michael
AllowGroup ftpuser
DenyAll
</Limit>
```

Voranstehendes Beispiel erlaubt den Zugriff nur den Usern *peter* und *michael*. Allen anderen Usern wird der Zugang verweigert.

Wie kann man nun einen Account einrichten, der Dateien in ein Verzeichnis up- oder downloaden darf, nicht aber Dateien in dem Verzeichnis löschen darf? Unter Linux ist das mit einem typischen Dateisystem nicht möglich, da Schreibrechte immer auch das Recht zum Löschen von Dateien implizieren. Unter dem ProFTPD ist es indes möglich:

```
<Directory /path/to/dir>
<Limit DELE>
AllowUser ftpadm
DenyAll
</Limit>
</Directory>
```

Voranstehende Konfiguration erlaubt nur dem Benutzer *ftpadm* das Löschen von Dateien, allen anderen nicht.

Wenn Ihr FTP-Server nicht nur zu internen Testzwecken verwendet wird, sondern womöglich global verfügbar ist, so sollten Sie die Funktionen zur Server-Einschränkung nutzen, um sich beispielsweise vor DoS-Attacken zu schützen.

ProFTPD stellt Ihnen verschiedene Funktionen für die Einschränkung der Verbindungen zur Verfügung. Sie müssen nur auf den jeweiligen Anwendungsbereich abgestimmt genutzt werden. Die relevanten Direktiven im Überblick:

- **MaxInstances**: Sie beschränkt die Gesamtzahl der Verbindungen.
- **MaxClients**: Diese Direktive beschränkt die Anzahl der Verbindungen pro Server/virtuellem Host.
- **MaxClientsPerHost**: Sie beschränkt die Anzahl der Clients, die sich von einem Host aus anmelden können.
- **MaxClientsPerUser**: Diese Direktive beschränkt die Anzahl der Verbindungen, die gleichzeitig unter dem gleichen Usernamen aufgebaut werden können.
- **MaxHostsPerUser**: Hiermit beschränken Sie die Anzahl der Rechner, von denen sich jemand mit dem gleichen Usernamen einloggen kann.

Der Server stellt Ihnen weitere Direktiven zur Auswahl, mit denen Sie das System gezielt beschränken können. Sie können beispielsweise die intensive Belastung der CPU und/oder des Arbeitsspeichers pro FTP-Verbindung mit Hilfe der Direktiven *RLimitCPU* und *RLimitMemory* beschränken. Hier zwei Beispiele für eine sinnvolle Beschränkung:

```
RLimitCPU session 10
RLimitMemory session 4096
```

Voranstehende Beispiele beschränken die Benutzung der CPU und des Speichers auf die einzelnen Sessions.

Sie können die Beschränkung aber auch auf einen Serverprozess konfigurieren. In diesem Fall könnte es wie folgt aussehen:

```
RLimitMemory daemon 8192 max
```

Mit der Verwendung der Direktive *RLimitCPU* sollte man allerdings sorgsam umgehen, da ein permanent laufender Daemon dieses Limit unter Umständen erreicht. Einen guten Wert werden Sie nur durch eigene Tests ermitteln.

Eine weitere Anforderung: Die Beschränkung der herunterlad- bzw. uploadbaren Dateien. Sie können die Größe der Dateien mit den beiden Direktiven *MaxRetrieveFileSize* und *MaxStoreFileSize* steuern.

Für die Ressourcen-Einschränkung können Sie auch einige Server-Module verwenden. Hier sind insbesondere die drei folgenden relevant:

- *mod_diskuse*
- *mod_load*
- *mod_quotatab*

5.3 Performance-Tuning

Wie bei jedem Server-System stellt sich irgendwann einmal die Frage, wie man das System tunen kann. Auch hier hat der ProFTP-Server eine Vielzahl an Stellschrauben zu bieten, an denen Sie drehen können.

Stellen Sie zunächst sicher, dass die Ident- und DNS-Abfragen abgeschaltet sind. Die entsprechende Konfiguration sieht wie folgt aus:

- *IdentLookups off*
- *UseReverseDNS off*

Der ProFTPD fragt standardmäßig bei jeder neuen Verbindung diese Werte ab. Je nach Antwortzeit des Ident- und des DNS-Servers kann dieses das Einloggen spürbar verzögern – im ungünstigsten Fall sogar bis zum Timeout, der mehrere Sekunden dauern kann.

Eine weitere Ursache für lange Einlog-Vorgänge sind sehr große */etc/passwd*- und/oder */etc/group*-Dateien. Da diese Dateien Zeile für Zeile abgearbeitet werden, kann das bei sehr langen Listen auch länger dauern. Ist das bei Ihnen auch der Fall, sollten Sie die Verlagerung der Benutzerverwaltung nach LDAP oder SQL in Erwägung ziehen.

Gelegentlich ist auch schon einmal PAM an Verzögerungen schuld – vorausgesetzt, Sie verwenden diesen Mechanismus überhaupt. Ob tatsächlich PAM daran schuld ist, lässt sich recht einfach mit dem Deaktivieren testen:

```
<IfModule mod_auth_pam.c>
    AuthPAM off
</IfModule>
```

Bei eher schwachbrüstigen Systemen kann auch das Auflisten von Verzeichnissen innerhalb einer FTP-Session die I/O des Servers belasten. Das wird insbesondere durch das rekursive Listen der Verzeichnisse verursacht, gerade bei vielen Unterverzeichnissen. Um dies zu unterbinden, passen Sie Ihre Konfiguration wie folgt an:

```
ListOptions +R strict
```

Bei voranstehender Konfiguration wird durch die Verwendung der Option *-R* das Listen der Verzeichnisse verhindert. Die Angabe *strict* bestimmt, dass Clients diese Angabe nicht überschreiben können. Außerdem kennt ProFTPD einige ListOptions-Einstellungen. Hier einige sinnvolle Einstellungen, um die Tiefe der Rekursion zu beschränken:

```
ListOptions "" maxdepth 3
ListOptions "" maxdirs 10
ListOptions "" maxfiles 1000
```

Mit der ersten Zeile wird die maximale Tiefe der Rekursion beschränkt, die zweite Zeile begrenzt die maximale Anzahl von Verzeichnissen, die auf einmal gelistet werden können, und die dritte Zeile limiert die maximale Anzahl der Dateien, die auf einmal gelistet werden können.

Es bietet sich ein weiterer Weg an, das Listen von Verzeichnissen zu beschleunigen: Schalten Sie die Überprüfung auf .ftpaccess-Dateien in den einzelnen Verzeichnissen ab. Diese Überprüfung wird nämlich bei jedem Verzeichniswechsel durchgeführt – und das muss ja wirklich nicht sein. Also schalten Sie dies ab:

```
AllowOverride off
```

Es gibt eine Vielzahl weiterer Einstellungen, die sich auf die Server-Performance auswirken. Selbst die Protokollierung der Server-Aktivitäten hat darauf Auswirkungen. Der FTP-Server verwendet den Syslog für seine Protokolle. Der aber ist bekannt dafür, dass er nicht sonderlich skaliert und unter hoher Last auch schon einmal zusammenbricht. In diesen Fällen ist es sinnvoll, die Protokolle direkt in Dateien zuschreiben, anstatt sie an den Syslog zu übergeben.

Genau hierfür sind die Direktiven *ServerLog* und *SystemLog* zuständig. Unter Umständen kann es auch sinnvoll sein, das Loggen von *utmp/wtmp* zu deaktivieren, um den Overhead zu reduzieren. Die zugehörige Einstellung hierfür lautet:

```
WtmpLog off
```

Schließlich können Sie auch einige Configure-Optionen für das Performance-Tuning verwenden, um den ProFTPD zu optimieren. Dabei sind insbesondere die Optionen *--enable-tunable-buffer-size* und *--enable-sendfile* von Interesse. Mit der Sendfile-Option können Sie zwar nicht die Übertragung an sich beschleunigen, dafür aber die Disk-I/O reduzieren.

Ein weiterer Kniff: Erhöhen Sie die Puffergröße mit der Option *--enable-buffer-size*. Dann schreibt der ProFTPD die Daten in größere Pakete und benötigt daher deutlich weniger aufwendige Systemaufrufe. Die Erhöhung dieses Werts auf 8092 Byte (8 kb) sollte die Übertragungsgeschwindigkeit bereits erheblich verbessern.

5.4 ProFTPD für Fortgeschrittene

Der FTP-Server bietet Ihnen eine Vielzahl von erweiterten Einstellungsmöglichkeiten und Funktionen. Zwei dieser Möglichkeiten sollen hier noch angesprochen werden, da sie gerne genutzt werden.

5.4.1 Sichere Verbindung

Eine wichtige Anforderung an den Betrieb eines FTP-Servers ist der Aufbau einer gesicherten Verbindung zwischen FTP-Client- und Server. ProFTPD unterstützt sowohl FTPS als auch SFTP. FTPS wurde als TLS-Erweiterung für FTP eingeführt, SFTP stellt als SSH-Subsystem nur einen FTP-ähnlichen Service zur Verfügung, der auf das SSH-Protokoll aufsetzt. Der Vorteil von SFTP: Es lässt sich einfacher durch NAT-Gateways hindurch verwenden. Allerdings bringt auch SFTP einige Nachteile mit sich. So besitzt SSH/SFTP keine eingebaute chroot-Funktion und die Authentifikation über eine SQL-Datenbank oder ein LDAP-System erfordert ein zusätzliches PAM-Modul.

Da aufseiten der Clients FTPS breit unterstützt wird, schauen wir uns an, wie man diese Sicherungsform verwendet.

Zunächst müssten Sie ProFTPD mit *mod_tls* installieren. Bei den meisten Linux-Distributionen ist ProFTPD samt mod_tls verfügbar. Um zu prüfen, ob der FTP-Server mit *mod_tls* übersetzt wurde, verwenden Sie folgenden Befehl:

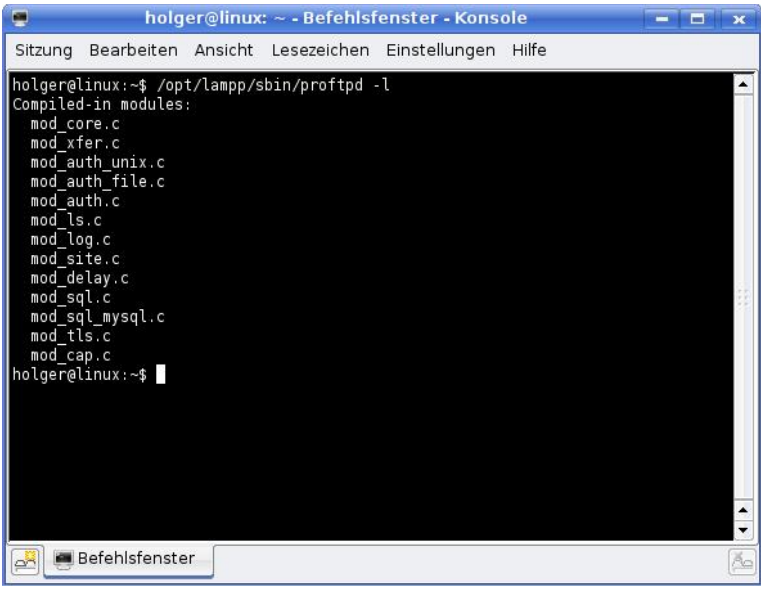
```
~$ /opt/lampp/sbin/proftpd -l
Compiled-in modules:
mod_core.c
...
```

```
mod_tls.c
...
```

Ist das nicht der Fall, sollten Sie es mit den entsprechenden Kommandos nachholen:

```
./configure --with-modules=mod_tls && make
make install (als root)
```

Die resultierende Binärdatei sollte nun auch TLS-Unterstützung bieten. Vergessen Sie nicht, sich ein gültiges Zertifikat zu besorgen, sofern Sie noch keines besitzen. Alternativ können Sie auch eine eigene CA einrichten und mit diesen Keys signieren.



Der Parameter *-l* gibt die Liste der kompilierten Module aus.

Als Nächstes müssen Sie die ProFTPD-Konfigurationsdatei anpassen. Diese könnte dann wie folgt aussehen:

```
# cat /opt/lampp/etc/proftpd.conf
ServerName "ProFTPD mod_tls-Demo"
ServerType standalone
DefaultServer on
Port 21
Umask 022
MaxInstances 30
User nobody
Group nogroup
DefaultRoot ~
AllowOverwrite on
# TLS
<IfModule mod_tls.c>
TLSEngine on
TLSLog /opt/lampp/etc/proftpd_tls.log
TLSProtocol TLSv1
TLSRequired off
TLSVerifyClient off
TLSRSACertificateFile /opt/lamp/etc/ftpcert/host.cert
TLSRSACertificateKeyFile /opt/lampp/etc/ftpcert/host.key
</IfModule>
```

Nach einem Neustart des FTP-Servers steht einer gesicherten Verbindung nichts mehr im Wege.

5.4.2 Benutzerverwaltung mit MySQL

Es gibt verschiedene Gründe, warum man die Benutzerverwaltung mit Hilfe von MySQL bewältigen kann. Auf diesem Weg können Sie die FTP- von den System-Usern trennen. Ein weiterer Vorteil: Sie können andere Passwörter für die FTP-

User verwenden. Das schafft zusätzlichen Schutz für Ihr System, auch wenn es für den Benutzer umständlicher ist, mit mehreren Passwörtern zu hantieren. Schließlich können Sie die User mit einem übersichtlichen Webfront-end verwalten.

Um mit MySQL kommunizieren zu können, müssen Sie zunächst sicherstellen, dass das Modul *mod_sql* installiert ist. Prüfen Sie dies mit obigem Kommando. Sollte es nicht der Fall sein, müssen Sie erst sicherstellen, dass folgende Pakete installiert sind:

- ProFTPD-Sourcecode
- MySQL-Server
- MySQL-Client
- MySQL-Header
- MySQL-Libraries

Dann können Sie die ersten MySQL-Tabellen anlegen. Richten Sie zunächst einen Benutzer ein, der die ProFTPD-Tabellen anlegen darf. Dazu können Sie beispielsweise zu phpMyAdmin greifen, das ja auch in XAMPP integriert ist. Dann werden die Tabellen angelegt.

Laden Sie sich daraufhin die Tabellenbeschreibung (*http://www.proftpd.de/files/pro-ftpd_sql.sql*) herunter. Mit dem Kommando *mysql -u "USERNAME" -p < proftpd_sql.sql* installieren Sie die notwendigen Tabellen. Ersetzen Sie USERNAME durch den zuvor angelegten Benutzer.

Sollte das MySQL-Modul noch nicht verfügbar sein, sollten Sie es nachträglich einrichten. In der Regel ist das bei XAMPP nicht erforderlich.

Als Nächstes stehen nur noch einige Anpassungen der ProFTPD-Konfigurationsdatei an. Das SQL-Modul bietet Ihnen die Möglichkeit, beispielsweise die User- und Gruppenverwaltung, verschiedene Arten, die Passwörter zu verschlüsseln, die Integration von Quota oder Access-Kontrollen zu realisieren.

Hier ein Beispiel für eine einfache Konfiguration, bei der ProFTPD und MySQL miteinander kommunizieren:

```
SQLAuthTypes Plaintext

SQLAuthenticate users*

SQLConnectInfo db@localhost username password

SQLDefaultGID 65534

SQLDefaultUID 65534
```

```
SQLMinUserGID  100
SQLMinUserUID  500
SQLUserInfo ftp username password uid gid homedir shell
```

Einige Einträge bedürfen der Erläuterung. Mit dem Eintrag *SQLAuthTypes Plaintext* legen Sie fest, dass die Passwörter unverschlüsselt angelegt werden.

Das Sternchen hinter dem Eintrag *SQLAuthenticate users* sorgt dafür, dass nur die SQL-Datenbank zur Authentifizierung benutzt wird. Normale Linux-Benutzer haben also keinen Zugang zum System.

Mit den Default-Werten legen Sie fest, welche UID und GID genommen werden, wenn entweder die in der SQL-Datenbank angegebenen kleiner als die Mindestwerte (stehen darunter) sind oder keine angegeben werden. Die letzte Zeile bestimmt den Tabellennamen (in unserem Beispiel *ftp*) sowie die Feldbezeichnungen von *username*, *password* etc.

5.4.3 Beispielkonfiguration

Oben haben Sie eine einfache Konfigurationsdatei kennengelernt, die nur für einfachste FTP-Server-Aufgaben taugt. Hier ein erweitertes Beispiel, das neben TLS auch MySQL unterstützt (Die Erläuterungen finden Sie in der Konfigurationsdatei):

```
# Konfigurationsbeispiel mit MySQL- und TLS-Support.
# Einzelne Direktiven oder ganze Bereiche wurden durch ein
# Kommentarzeichen ("#") deaktivert und sind bei Bedarf
# wieder einfach zu reaktivieren.
#
ServerType standalone
PidFile /var/run/proftpd.pid
MaxInstances 30
MaxConnectionRate 4
SocketBindTight off
UseReverseDNS off
RootRevoke on
```

```
DefaultServer on
MultilineRFC2228 on
<IfModule mod_delay.c>
DelayEngine off
DelayTable /var/run/proftpd/proftpd.delay
</IfModule>
<IfModule mod_tls.c>
TLSProtocol SSLv23
</IfModule>
# Log-Formate definieren
SystemLog NONE
LogFormat default "%h %l %u %t \"%r\" %s %b"
LogFormat auth "%v [%P] %h %t \"%r\" %s"
LogFormat write "%h %l %u %t \"%r\" %s %b"
# ----------------------------------------
# globale Einstellungen
# ----------------------------------------
<Global>
User nobody
Group nogroup
# ----------------------------------------
# Log-in
# ----------------------------------------
ServerIdent on "FTP server ready."
DeferWelcome on
DisplayConnect /etc/proftpd.msg
IdentLookups off
UseFtpUsers off
RequireValidShell off
TimeoutLogin 60
```

```
MaxLoginAttempts 3
MaxClientsPerHost 3
# ----------------------------------------
# Authentifikation: Standard
# ----------------------------------------
<IfModule !mod_sql.c>
AuthOrder mod_auth_unix.c
<Limit LOGIN>
DenyGroup !ftpuser
</Limit>
</IfModule>
# ----------------------------------------
# Authentifizierung per SQL
# ----------------------------------------
<IfModule mod_sql.c>
AuthOrder mod_sql.c
SQLConnectInfo db@localhost sqluser pass
SQLUserInfo ftp userid passwd uid gid homedir NULL
SQLAuthTypes Plaintext
SQLAuthenticate users
SQLMinUserUID 1024
SQLMinUserGID 555
SQLNegativeCache on
</IfModule>
# ----------------------------------------
# TLS Standards
# ----------------------------------------
<IfModule mod_tls.c>
TLSEngine off
TLSTimeoutHandshake 60
```

```
TLSRequired off

TLSVerifyClient off

TLSOptions NoCertRequest

TLSLog /var/log/proftpd/tls.log

# TLSCACertificateFile /etc/ssl/certs/CA.cert # CA-Cert op-
tional

</IfModule>

# ------------------------------------------

# Post-Login, Timeouts

# ------------------------------------------

PassivePorts 49152 65534

DisplayLogin welcome.msg

DisplayFirstChdir .message

AllowOverride off

TimeoutIdle 600 # Inaktivitaet

TimeoutNoTransfer 3600 # keine Datenuebertragung (Listing,
File, ...)

TimeoutStalled 300 # haengende Datenuebertragung

TimeoutSession 7200 # Gesamtdauer einer Session

# ------------------------------------------

# Session

# ------------------------------------------

DefaultRoot ~

DenyFilter \*.*/

ListOptions "-An +R" strict

UseGlobbing off

ShowSymlinks on

TimesGMT on

# ------------------------------------------

# Up- & Download

# ------------------------------------------
```

```
AllowOverwrite on
AllowRetrieveRestart on
HiddenStores on
DeleteAbortedStores on
AllowStoreRestart off # widerspricht sonst "DeleteAborted-
Stores"
# ------------------------------------------
# Datei & Verzeichnis
# ------------------------------------------
Umask 0017 0007
### hierher alle <Directory>-Bloecke
# ------------------------------------------
# Anonymous FTP
# ------------------------------------------
# <Anonymous /home/ftp>
# User ftp
# Group ftpuser
# UserAlias anonymous ftp
#
# MaxClients 5 # weniger anonymous-User als Reg.User
# MaxRetrieveFileSize 512 Mb # max. Downloadgroesse
#
# # Geschwindigkeit von Up- und Downloads
# # auf 255 K/sec. beschränken
# TransferRate APPE,RETR,STOR,STOU 255
#
# <Directory *>
# HideNoAccess on
# <Limit WRITE>
# DenyAll
# IgnoreHidden on
```

```
# </Limit>
# </Directory>
# </Anonymous>
# ----------------------------------------
# Logging
# ----------------------------------------
WtmpLog off
TransferLog /var/log/proftpd/xferlog
# Record all logins
ExtendedLog /var/log/proftpd/auth.log AUTH auth
# Logging file/dir access
ExtendedLog /var/log/proftpd/access.log WRITE,READ write
# Paranoia logging level....
ExtendedLog /var/log/proftpd/paranoid.log ALL default
# fuer Debug: alle mod-MySQL-Kommentare
#SQLLogFile /var/log/proftpd/sql.log
</Global>
# ----------------------------------------
# Standard-Server
# ----------------------------------------
DefaultAddress 192.168.1.1
ServerName meinserver.tld
ServerAdmin hostmaster@meinserver.tld
# MasqueradeAddress meinserver.dyndns.org
<IfModule mod_tls.c>
TLSEngine on
TLSRSACertificateFile /etc/ssl/certs/meinserver.tld.cert
TLSRSACertificateKeyFile /etc/ssl/certs/meinserver.tld.key
</IfModule>
# ----------------------------------------
```

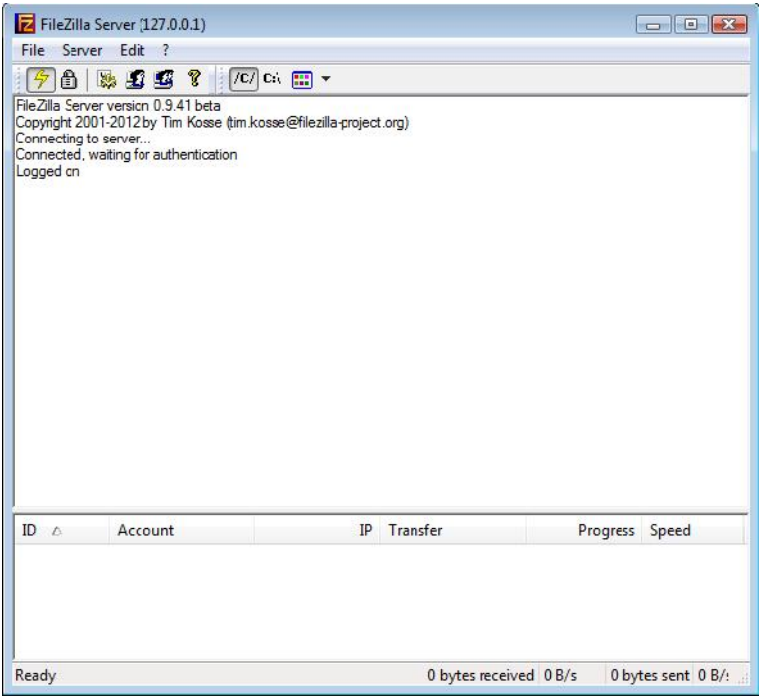
```
# Virtuelle Hosts
# ----------------------------------------
<VirtualHost 192.168.1.2>
ServerName server2.meinserver.tld
ServerAdmin hostmaster@meinserver.tld
IfModule mod_tls.c>
TLSEngine on
TLSRSACertificateFile
/etc/ssl/certs/server2.meinserver.tld.cert
TLSRSACertificateKeyFile
/etc/ssl/certs/server2.meinserver.tld.key
</IfModule>
</VirtualHost>
```

Für weitere Informationen zu dem FTP-Server sei auf die Projekt-Site verwiesen. Dort finden Sie einen umfangreichen Dokumentationsbereich.

6 FileZilla-Server

Ein FTP-Server ist eine hervorragende Ergänzung eines Webservers, denn Sie können mit diesem Daten auf Ihr System übertragen. Was der ProFTPD für XAMPP für Linux ist, ist der FileZilla-Server für XAMPP für Windows.

Bei dem Begriff FileZilla wird der ein oder andere Leser vermutlich hellhörig. Da war doch was? Richtig, es gibt auch einen FileZilla-FTP-Client. Auch er ist frei verfügbar – so wie der Server – und stammt auch aus dem gleichen Projekt, dem FileZilla-Projekt (*http://filezilla-project.org*).



Ein erster Blick auf die Schnittstelle des FileZilla-Servers.

6.1 FileZilla-Quickstart

Der FileZilla-Server erlaubt das einfache Aufsetzen und die einfache Inbetriebnahme eines FTP-Servers. Der Server bietet neben einem einfachen Benutzer- und Gruppen-Management auch SSL-/TLS-Verschlüsselung, Up-/Downloadraten-Beschränkungen (global und pro Benutzer) sowie die Möglichkeit, Verbindungen auf bestimmte IP-Adressen sowohl auf Client- wie auf Serverseite einzuschränken. Über das Remote-Admin-Interface ist auch die Wartung von anderen Computern aus einfach möglich.

Der Zugriff auf den Server kann über verschiedene Wege erfolgen. Am Einfachsten ist, wenn Sie den Log-in-Dialog über das XAMPP Control Panel starten. Alternativ starten Sie den Server mit einem Doppelklick auf *FileZilla Server.exe* im FileZilla-Ordner. Der Zugriff über den Log-in-Dialog erfolgt über *FileZilla Server Interface.exe*.

Außerdem stehen Ihnen zwei Batchdateien zur Verfügung, mit denen Sie den Server starten bzw. anhalten können:

- *FileZillaFTP_start.bat*
- *FileZillaFTP_stop.bat*

Das Interessante an dem Server ist sicherlich die XML-basierte Konfigurationsdatei *FileZilla Server.xml*. In ihr sind die Einstellungen gespeichert, die Sie über die FileZilla-Server-Konfiguration anpassen können.

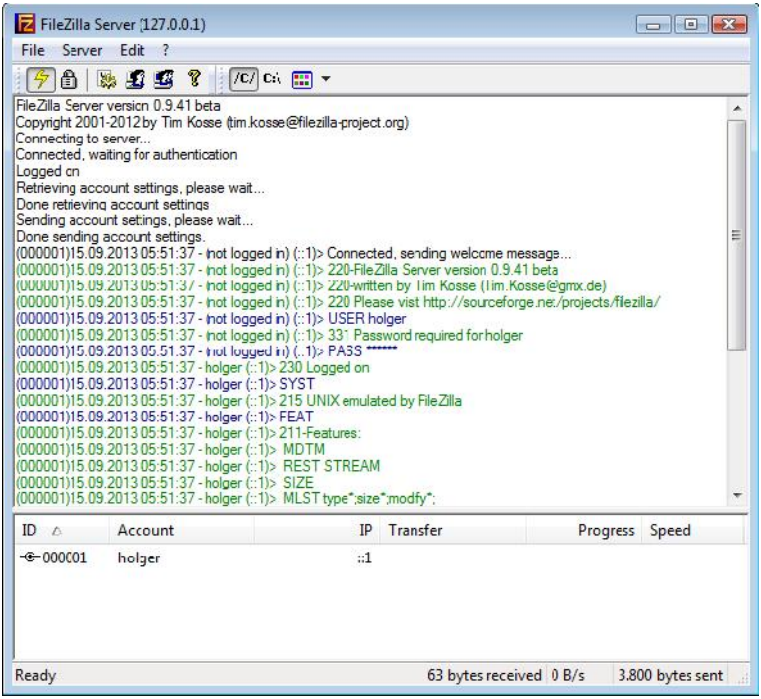
6.1.1 Konfiguration des FTP-Servers

Ein direkter Zugriff auf FileZilla über die XAMPP-Web-Schnittstelle ist nicht möglich. Hinter dem FileZilla-FTP-Link verbergen sich lediglich einige Informationen zum Server.

Um den FTP-Server verwalten zu können, greifen Sie über das Interface auf den Server zu. Der *Connect-to-Server*-Dialog verlangt die Eingabe der Server-Adresse, den Port und das administrative Passwort. Das Admin-Passwort muss bei einer lokalen Installation nicht angegeben werden. Mit einem Klick auf *OK* stellen Sie die Verbindung zum Server her.

Der FileZilla-Server präsentiert Ihnen seine einfache Schnittstelle. Neben einer Menü- und Symbolleiste finden Sie zwei Darstellungsbereiche. Im oberen werden die Kommandos angezeigt, die der Server mit dem oder den FTP-Clients austauscht. Im unteren Bereich finden Sie die Verbindungen zu Clients.

Die wichtigsten Einstellungen des FileZilla-Interface sind über das Menü *Edit* verfügbar. Über dieses Menü bearbeiten Sie die Einstellungen und erzeugen Gruppen und Benutzer.



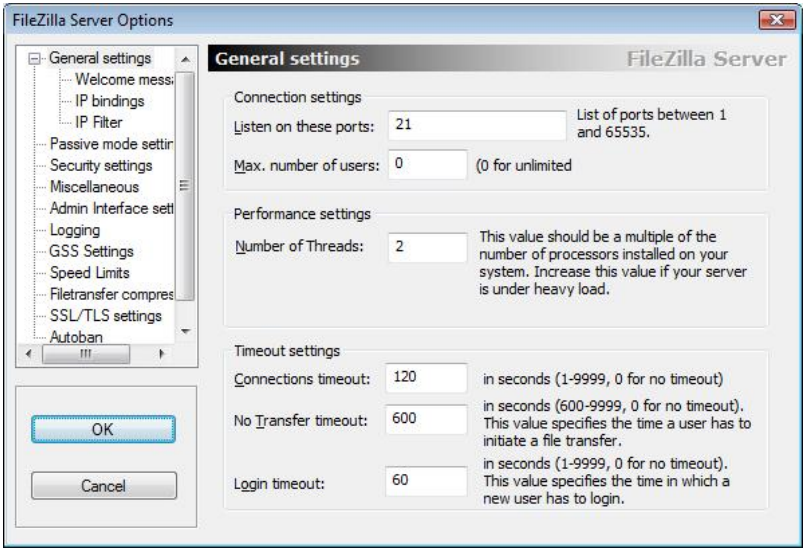
Der FileZilla-Server zeigt die Kommunikation mit einem FTP-Client an.

Schauen wir uns die wichtigsten administrativen Aufgaben an, die Sie mit dem FileZilla-FTP-Server zu erledigen haben. Führen Sie dazu den Befehl *Edit* > *Settings* aus. Der Server präsentiert Ihnen eine übersichtliche Konfiguration, über die Sie verschiedene allgemeine Einstellungen, die Sicherheitsoptionen, die Einstellungen für das Admin-Interface und vieles mehr anpassen können.

Welche Aktionen Sie zunächst durchführen, ist sicherlich von Fall zu Fall sehr unterschiedlich. Beim ersten Zugriff landen Sie in den allgemeinen Einstellungen (*General settings*). Sie können hier den Port und die maximale Anzahl an Benutzern anpassen. Wenn Sie eine unbegrenzte Anzahl an Usern zulassen wollen, behalten Sie unter *Max. number of users* die Standardeinstellung null bei.

Wenn Sie nur eine begrenzte Anzahl mit FTP-Diensten versorgen wollen, sollten Sie einen Wert verwenden, der sich an der tatsächlichen Benutzerzahl orientiert. Sie sollten im Untermenü *IP-Filter* auch die Möglichkeit nutzen, unerwünschte Benutzer explizit vom Zugriff auszuschließen.

Eine weitere sicherheitsrelevante Funktion trägt die Bezeichnung *Security settings*. Hier sind standardmäßig Server-zu-Server-Verbindungen unterbunden.



Die Einstellungen für das Admin-Interface.

Da der Admin-Account beim ersten Zugriff noch kein Passwort besitzt, sollten Sie das bei der ersten Konfigurationssession ändern. Wechseln Sie dazu zum Menü *Admin Interface settings*. Passen Sie eventuell den Port an, unter dem die Admin-Schnittstelle zu erreichen ist.

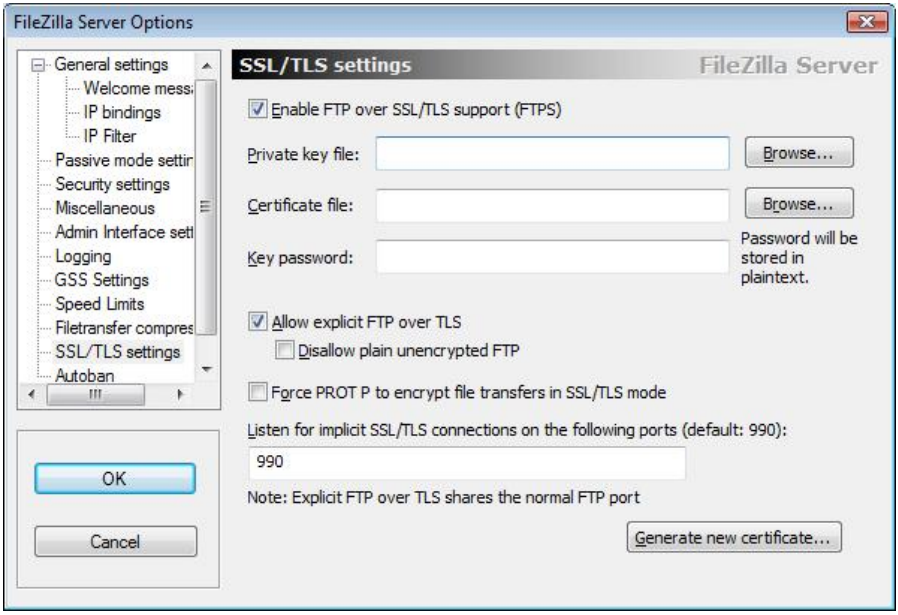
Mit den beiden folgenden Textfeldern können Sie die Bindung bzw. den Zugriff auf das Interface beschränken. Wenn der Zugriff nur von lokalen Rechnern möglich sein soll, so geben Sie unter *IP Addresses which are allowed to connect to the admin interface* beispielsweise *192.168.1.** an. Neben Platzhaltern können Sie auch einzelne IP-Adressen angeben.

Um Ihren Server vor Überlastung zu schützen, sollten Sie gegebenenfalls die Geschwindigkeitsgrenzen für Down- und Uploads setzen. Wechseln Sie zum Menü

Speed Limits und aktivieren Sie unter *Download Speed Limit* und/oder *Upload Speed Limit* die Begrenzungen. Sie haben dabei die Wahl zwischen zwei Schranken:

- Mit *Constant Speed Limit of x KB/s* bestimmen Sie die maximale Download- bzw. Upload-Geschwindigkeit pro User.
- Mit *Use Speed Limit Rules* können Sie zusätzliche Beschränkungen für bestimmte Wochentage und/oder Daten definieren.

Wenn Sie mit externen FTP-Clients oder -Servern Daten austauschen, so kann es sinnvoll sein, die Komprimierung unter *Filetransfer compression* zu aktivieren. Sie aktivieren die Kompression mit *Enable MODE Z support*. Beachten Sie allerdings, dass die Kompression aufseiten des Servers eine deutlich höhere Last zur Folge hat. Der Einsatz ist daher nur bei leistungsstarken Systemen zu empfehlen. Stellen Sie außerdem sicher, dass die Clients ebenfalls den Z-Modus unterstützen.



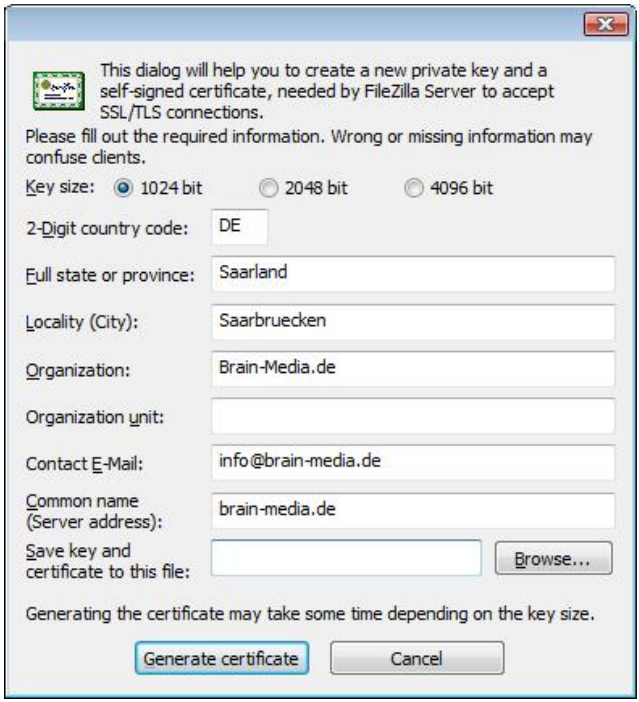
Die SSL-/TLS-Einstellungen des FTP-Servers.

6.1.2 Sicheres FTP

Sie können den FileZilla-FTP-Server auch für den SSL- bzw. TLS-gesicherten Zugriff konfigurieren. Die dafür notwendigen Einstellungen finden Sie unter *SSL/TLS settings*.

Aktivieren Sie zunächst die SSL-/TLS-Unterstützung, indem Sie das Kontrollkästchen *Enable SSL/TLS support* aktivieren. In die Eingabefelder *Private key file*, *Certificate key file* und *Key password* geben Sie den Pfad zu Ihren Schlüsseldateien bzw. das Passwort an. Wenn Sie gesicherte Verbindungen erzwingen wollen, aktivieren Sie außerdem die Option *Force explicit SSL/TLS*. Gegebenenfalls passen Sie den Port an, was aber meist nicht erforderlich ist.

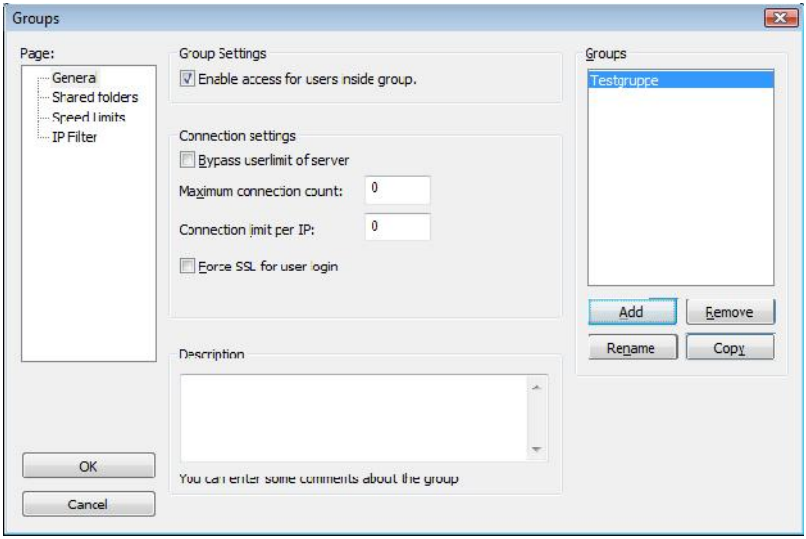
Wenn Sie über kein Zertifikat eines bekannten Zertifikat-Dienstes verfügen, können Sie über die Schaltfläche *Generate Certificate* ein eigenes selbstsigniertes Zertifikat erstellen. Für Testzwecke genügt das allemal. Nun müssen Sie nur noch Ihren Client für den Aufbau einer gesicherten Verbindung konfigurieren.



Ein selbst erzeugtes Zertifikat.

6.1.3 Benutzer- und Gruppenverwaltung

In der Grundkonfiguration kommt der FileZilla-FTP-Server neben dem Admin-Account mit zwei Benutzern und keiner Gruppe daher. Wenn Sie aber Ihren Benutzern bestimmte Inhalte und Dateiablagen zugänglich machen wollen, müssen Sie diese zunächst anlegen. In der Regel ist es am einfachsten, Gruppen einzurichten, diesen Gruppen spezifische Eigenschaften, wie das Home-Verzeichnis, die Speed-Limits und IP-Filter, zuzuordnen und dann im zweiten Schritt Benutzer zu erstellen und diese den Gruppen zuzuweisen. Sie können beispielsweise eine Gruppe für eine interne Abteilung A und eine für Abteilung B erzeugen. Sinn macht in einem solchen Beispiel auch eine dritte Gruppe mit spezifischen Eigenschaften für Benutzer, die von außen auf den FTP-Server zugreifen.

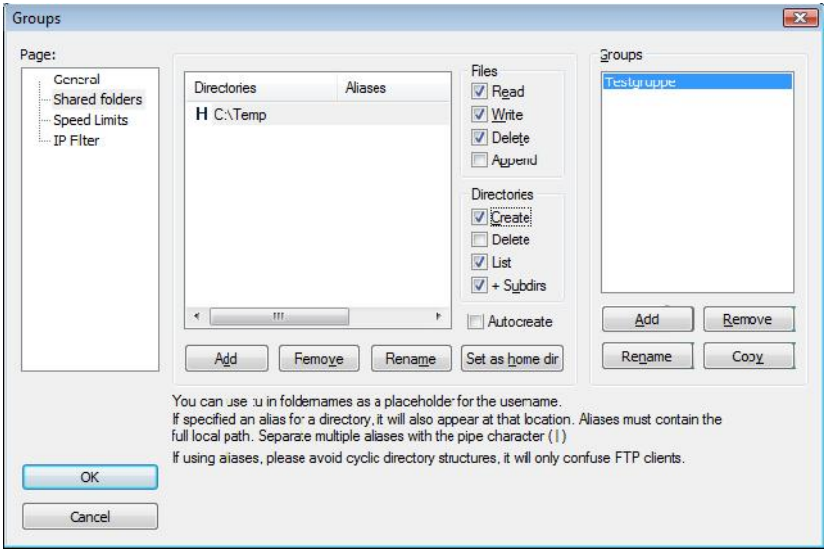


Die Gruppenverwaltung des FTP-Servers.

Da vom Handling beide Einstellungen nahezu identisch sind, beschränken wir uns hier auf die Gruppe. Um eine erste Gruppe zu erzeugen, führen Sie den Befehl *Edit> Groups* aus oder klicken auf das zugehörige Icon in der Symbolleiste. Im rechten Bereich werden die Gruppen erzeugt. Klicken Sie auf *Add* und weisen Sie der ersten Gruppe eine Bezeichnung zu.

Nun können Sie die Einstellungen der vier Seiten *General, Shared folders, Speed Limits* und *IP Filter* definieren. Aktivieren Sie zunächst auf der Seite *General* die

neue Gruppe. Ordnen Sie dann auf der Seite *Shared folders* der Gruppe einen Ordner zu. Da noch kein Ordner erstellt ist, den die Gruppe als Dateiablage verwenden könnte, klicken Sie auf *Add*, suchen den gewünschten Ordner bzw. erstellen ihn. Bestimmen Sie außerdem die Lese- und Schreibrechte für Ordner und Dateien. Standardmäßig sind lediglich das Lesen von Dateien und das Auflisten von Verzeichnissen und Unterverzeichnissen, nicht aber das Erzeugen und Löschen von Dateien und Ordnern innerhalb des angegebenen Gruppen-Ordners erlaubt. Sollen die Gruppenmitglieder beispielsweise auch Dateien in den Ordner ablegen können, aktivieren Sie unter *Files* die Option *Write*.



Die Gruppeneigenschaften einer ersten Testgruppe.

Passen Sie, sofern erforderlich, außerdem die Einstellungen für die Geschwindigkeitsbegrenzungen und die IP-Filter an. Diese Funktionen entsprechen den allgemeinen Programmeinstellungen, wie sie oben beschrieben sind. Nachdem Sie Ihre erste Gruppe erzeugt haben, können Sie sich an das Erstellen der ersten Benutzer machen.

Leider verfügt der Server nicht über eine Import- und Exportfunktion, mit der man beispielsweise bestehende Benutzerdaten importieren könnte.

6.1.4 FileZilla-Konfigurationsdateien

Wie bereits erwähnt, verwendet der FileZilla-Server XML-basierte Konfigurationsdateien, und zwar nicht nur für den Server, sondern auch für das Interface. Diese finden Sie wie alle anderen FileZilla-Dateien im Ordner *\XAMPP\FileZillaFTP*.

Die Konfigurationsdatei des Interface trägt die Bezeichnung *FileZilla Server Interface.xml* und sieht wie folgt aus:

```
<FileZillaServer>
 <Settings>
  <Item name="Last Server Port" type="numeric">14147</Item>
  <Item name="Last Server Password"
type="string">********</Item>
  <Item name="Always use last server" type="numeric">0</Item>
  <Item name="User Sorting" type="numeric">0</Item>
  <Item name="Start Minimized" type="numeric">0</Item>
  <Item name="Last Server Address"
type="string">127.0.0.1</Item>
 </Settings>
</FileZillaServer>
```

Die eigentliche Server-Konfigurationsdatei ist natürlich deutlich komplexer. Hier ein Ausschnitt aus einer typischen Konfiguration:

```
<FileZillaServer>
 <Settings>
  <Item name="Serverport" type="numeric">21</Item>
  <Item name="Number of Threads" type="numeric">2</Item>
  <Item name="Maximum user count" type="numeric">0</Item>
  <Item name="Timeout" type="numeric">120</Item>
  <Item name="No Transfer Timeout" type="numeric">120</Item>
  <Item name="Allow Incoming FXP" type="numeric">0</Item>
  …
   ...
 <SpeedLimits>
```

```
    <Download/>
    <Upload/>
   </SpeedLimits>
  </Settings>
  <Groups/>
  <Users>
   <User Name="anonymous">
   <Option Name="Pass"/>
   <Option Name="Group"/>
   <Option Name="Bypass server userlimit">0</Option>
   <Option Name="User Limit">0</Option>
   <Option Name="IP Limit">0</Option>
   <Option Name="Enabled">1</Option>
   <Option Name="Comments"/>
  <IpFilter>
   <Disallowed/>
   <Allowed/>
  </IpFilter>
  <Permissions>
  <Permission Dir="C:\xampp\anonymous">
   <Option Name="FileRead">1</Option>
<Option Name="FileWrite">0</Option>
   <IpFilter>
    <Disallowed/>
    <Allowed/>
   </IpFilter>
  <Permissions>
   <Permission Dir="C:\xampp\htdocs">
    …
   </Permission>
```

```
  </Permissions>
  <SpeedLimits DlType="0" DlLimit="10" ServerDlLimitBy-
pass="0" UlType="0" UlLimit="10" ServerUlLimitBypass="0">
  <Download/>
  <Upload/>
  </SpeedLimits>
  </User>
  </Users>
</FileZillaServer>
```

Die beiden Tools des FileZilla-Projekts scheinen kontinuierlich weiterentwickelt zu werden. Die Handhabung des Servers ist wirklich kinderleicht. So darf man sich denn schon jetzt auf kommende Versionen freuen.

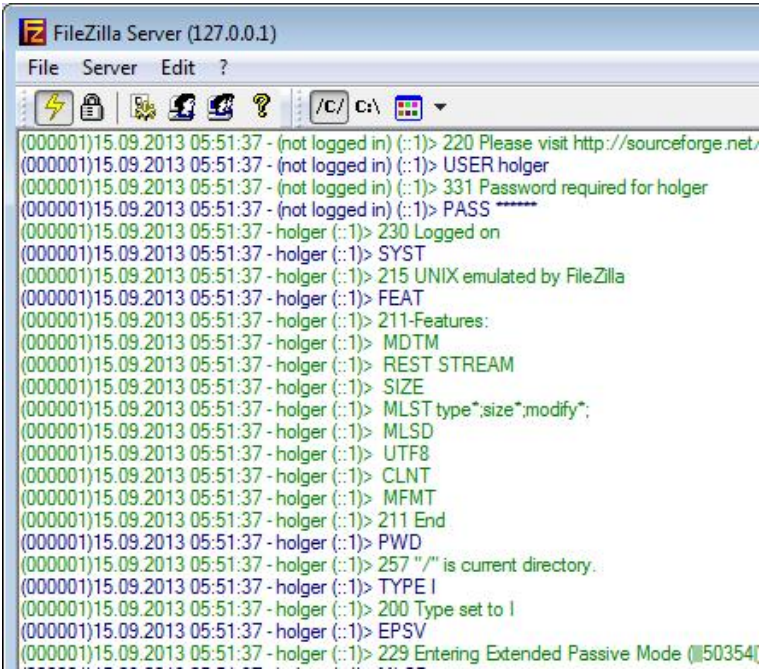
6.2 FileZilla im Detail

Sie haben in Sachen FileZilla inzwischen einen sehr guten Überblick, was der Server alles an Funktionen zu bieten hat. Werfen wir einen genaueren Blick auf den FTP-Server und seine Funktionen. Die Arbeitsfläche besteht in der Hauptsache aus dem Protokollfenster im oberen Bereich, das alle Befehle und Ereignisse auflistet, sowie im unteren Bereich aus einer Liste der bestehenden Verbindungen zu den Clients.

Die Größe dieser beiden Fenster ist variabel. Durch Ziehen mit der Maus an der Trennlinie zwischen beiden Fenstern können Sie die Größen der Fenster in Abhängigkeit voneinander verändern, und zwar bis zu dem Punkt, wo eines der Fenster ganz verschwindet. Im Folgenden werden die einzelnen Bestandteile des FileZilla-Servers beschrieben.

In der Menüleiste des FileZilla-Servers sind alle nötigen Befehle und Funktionen versammelt.

Fast alle Menübefehle sind auch als Schaltflächen in der Symbolleiste abrufbar. Während des gesamten Betriebs des Servers werden in diesem Fenster alle Aktionen und Ereignisse protokolliert.



Das Protokollfenster.

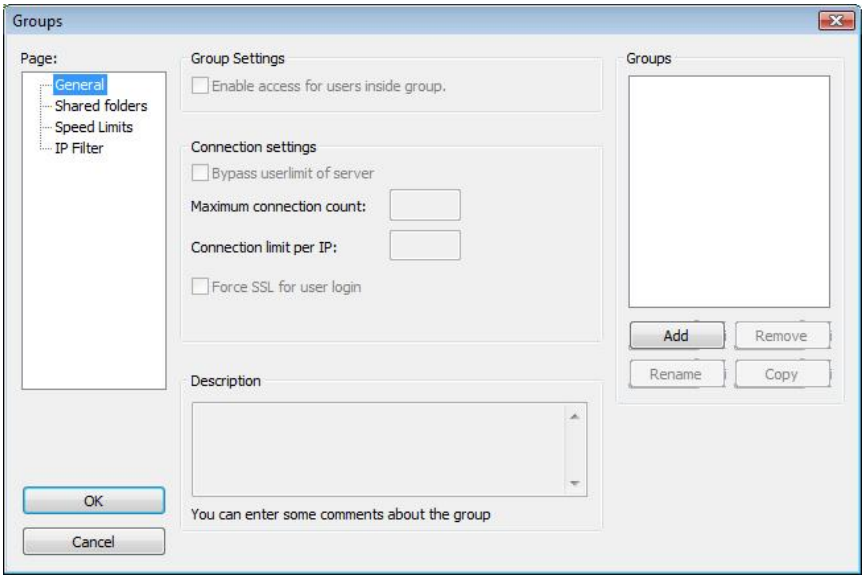
Die Angaben umfassen üblicherweise Datum und Uhrzeit der Protokollierung, Username bzw. not logged in, wenn keine Verbindung besteht, sowie einen FTP-Befehl oder FTP-Code.

Eine genaue Kenntnis der FTP-Befehle und FTP-Codes ist zwar nicht zwingend erforderlich, kann aber das Nachvollziehen dessen, was innerhalb des Netzwerks passiert, erleichtern. Eine Übersicht über die FTP-Befehle und FTP-Codes finden Sie im Anhang.

Im Verbindungsfenster werden alle bestehenden Verbindungen zu Clients angezeigt. Neben einer ID enthält die Liste den Account des Users und die IP-Adresse des Clients. Die Spalte *Transfer* zeigt an, ob gerade eine Übertragung stattfindet. In einem solchen Fall werden Fortschritt und Übertragungsrate in den beiden Spalten rechts angezeigt.

In der Statuszeile werden Systemmeldungen und ähnliche Information zum Programmgeschehen angezeigt. Sie zeigt folgende Informationen an:

- Die Mitteilung *Ready* am linken Rand der Statuszeile weist darauf hin, dass der Server aktiv ist.
- Die restlichen Felder geben Informationen zu gegenwärtigen oder bereits abgeschlossenen Übertragungen.
- Das erste Feld zeigt die am Server angekommene Datenmenge an.
- Das nächste Feld gibt im Fall, dass gerade eine Übertragung stattfindet, die Übertragungsrate an.
- Es folgen zwei Felder, welche die gleichen Angaben für Downloads zeigen: die vom Server gesendete Datenmenge sowie die Übertragungsrate einer gerade stattfindenden Datenübertragung.
- Zwei Signallämpchen am rechten Rand der Statuszeile leuchten rot, wenn gerade ein Upload (linkes Lämpchen) oder Download (rechtes Lämpchen) stattfindet.



Das Fenster zum Bearbeiten von Usergruppen.

6.2.1 Usergruppe anlegen/bearbeiten

Wenn Sie den FileZilla-Server zum ersten Mal gestartet haben, sollten Sie zunächst User und User-Groups anlegen.

Sobald Sie es mit mehr als einem oder zwei Usern zu tun haben, sollten Sie die Verwendung von User-Gruppen erwägen, denn damit können Sie die Eigenschaften und Berechtigungen der Benutzer am Einfachsten verwalten.

Zum Anlegen einer Usergruppe wählen Sie im *Edit*-Menü den Befehl *Groups* aus. Das Fenster, das sich nun öffnet, beinhaltet vier Seiten, die in dem Feld links angesteuert werden können. Das Feld *Groups* in der rechten Hälfte des Fensters ist auf allen vier Seiten vorhanden und kann so jederzeit eingesehen und bearbeitet werden. Zum Anlegen einer neuen Benutzergruppe klicken Sie auf den *Add*-Button.

Die Message-Box zum Anlegen einer Benutzergruppe.

Geben Sie in der darauf erscheinenden Message-Box den Namen der zu erstellenden Gruppe an. Nach Bestätigen der Eingabe mit *OK* kehren Sie zum Groups-Fenster zurück.

Nehmen Sie nun alle notwendigen Einstellungen für die neu angelegte Benutzergruppe vor, indem Sie die vier Seiten des Fensters durcharbeiten:

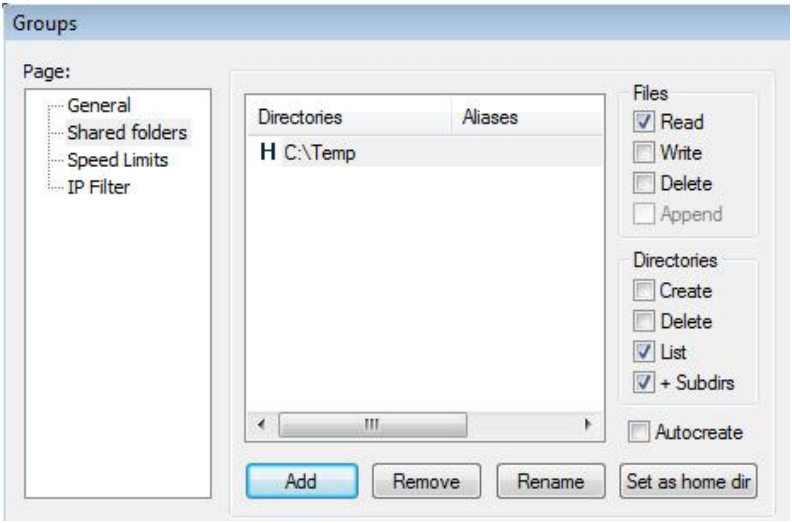
Generelle Einstellungen

Auf der ersten Seite (*General*) erlauben Sie im oberen Bereich den Zugriff für alle in der Gruppe enthaltenen User.

Im Bereich darunter können bestimmte Beschränkungen, z. B. die Anzahl zulässiger Verbindungen, festgelegt werden.

Verzeichniszugriff

Auf der zweiten Seite (*Shared folders*) legen Sie die Verzeichnisse fest, auf welche die Mitglieder der Gruppe zugreifen dürfen.



Die Verzeichniseinstellungen für Usergruppen.

In dem Feld, das diese Seite dominiert, werden alle Verzeichnisse gelistet, auf die die Gruppe zugreifen darf. Dahinter sind für jedes Verzeichnis sowie für die darin enthaltenen Dateien die Zugriffsrechte aufgeführt, die einzeln mit einem Häkchen aktiviert oder deaktiviert werden können.

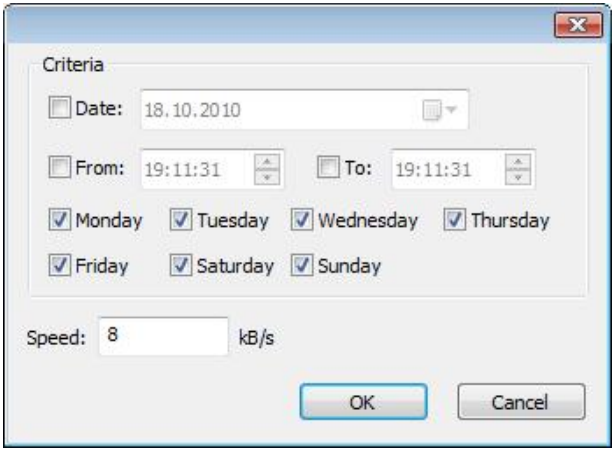
Die vier Schaltflächen unterhalb der Verzeichnisliste erlauben es Ihnen, Verzeichnisse hinzuzufügen (*Add*), zu löschen (*Remove*), umzubenennen (*Rename*) oder als Home-Verzeichnis für die Gruppe zu definieren (*Set as home dir*).

Bezogen auf Dateien umfassen die Berechtigungen das Lesen (*Read*), Schreiben (*Write*), Löschen (*Delete*) und Hinzufügen (*Append*).

Bei Verzeichnissen gibt es Berechtigungen für das Anlegen (*Create*), Löschen (*Delete*) und Auflisten (*List*) des jeweiligen Verzeichnisses. Außerdem können Sie vereinbaren, dass diese Rechte sich auf alle Unterverzeichnisse vererben (*+ subdirs*).

Auf der zweiten Seite (*Speed limits*) kann die Geschwindigkeit für Downloads und Uploads geregelt werden.

Neben der Eingabe von fixen oder Standardwerten können auch spezifische Regeln erstellt werden, mit welchen die Transfergeschwindigkeit für jeden der sieben Wochentage zu bestimmten Zeiten sekundengenau festgesetzt werden kann.



Die Message-Box zum Vereinbaren von Speed-Regeln.

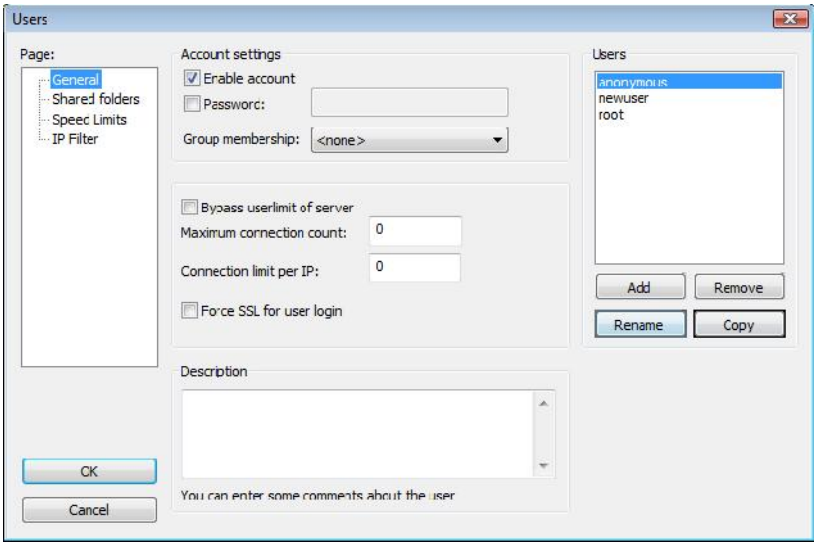
Zugangsfilter

Die vierte Seite (*IP Filter*) besteht lediglich aus zwei Eingabefeldern. Im oberen Feld können Sie bestimmte IP-Adressen von der Verbindung ausschließen. Außer einzelnen Adressen können Sie auch Platzhalter (* und ?) verwenden, um ganze Bereiche von Adressen zu erfassen. Hieraus ergibt sich der Sinn des unteren Feldes, denn dort kann das Verbindungsverbot für bestimmte Adressen wieder aufgehoben werden.

Standardmäßig darf sich jeder mit dem Server verbinden. Um die erlaubten Adressen streng zu limitieren, ist daher der am besten geeignete Weg, im oberen Feld zunächst alle Adressen von der Verbindung auszuschließen und dann im unteren Feld ausgewählte IP-Adressen wieder zuzulassen.

6.2.2 User anlegen/bearbeiten

Öffnen Sie dazu das Edit-Menü und klicken Sie den Befehl *Users* an. Das Fenster, das sich nun öffnet, beinhaltet vier Seiten, die in dem Feld links angesteuert werden können. Das Feld *Users* auf der rechten Seite des Fensters ist auf allen vier Seiten vorhanden und kann so jederzeit eingesehen und bearbeitet werden. Zum Anlegen eines neuen Users klicken Sie auf den *Add*-Button.



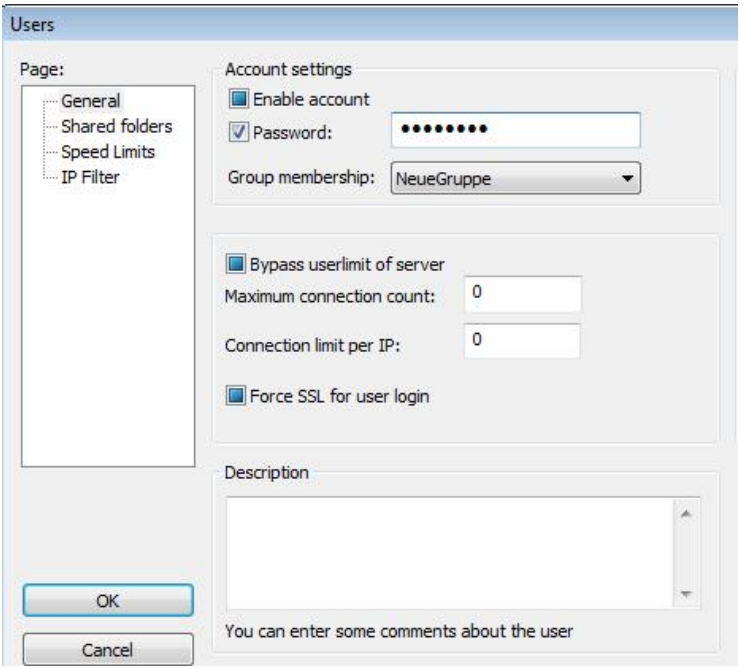
Der Dialog zum Bearbeiten von Usern.

Der Dialog zum Anlegen eines Users.

Eine Message-Box verlangt die Eingabe des Namens des neuen Users und der Gruppe, der er angehören soll. Nach Bestätigen der Eingabe mit *OK* kehren Sie zum *Users*-Fenster zurück.

Generelle Einstellungen

Auf der ersten Seite (*General*) werden allgemeine Einstellungen vorgenommen. Im oberen Bereich können Sie die Account-Settings des Users verwalten. Hier kann der Account aktiviert oder deaktiviert werden.



Die generellen Einstellungen für User.

Vergeben Sie ein Passwort für den User, indem Sie zunächst ein Häkchen in das entsprechende Kästchen klicken. Das Eingabefeld wird dann aktiviert, und Sie können ein Passwort eingeben. Dieses Passwort wird im Eingabefeld nicht angezeigt. Stattdessen wird für jedes Zeichen, das Sie eintippen, ein Asterisk * abgebildet.

Im Bereich darunter können bestimmte Beschränkungen festgelegt werden, z. B. die maximale Anzahl zulässiger Verbindungen oder eine Begrenzung der Verbindungen pro IP-Adresse.

Verzeichniszugriff

Auf der zweiten Seite (*Shared folders*) legen Sie die Verzeichnisse fest, auf die der User zugreifen darf. Dies funktioniert auf exakt die gleiche Weise wie für die Benutzergruppen. In einem Feld werden alle erlaubten Verzeichnisse gelistet, dahinter werden für das im Feld markierte Verzeichnis die Berechtigungen angezeigt. Die Schaltflächen im unteren Bereich dienen zum Hinzufügen, Löschen und Umbenennen der Verzeichnisse sowie zur Vereinbarung des Home-Verzeichnisses.

Übertragungsgeschwindigkeit

Auf der zweiten Seite (*Speed limits*) kann die Geschwindigkeit für Downloads und Uploads reguliert werden. Neben der Eingabe von fixen oder Standardwerten können auch spezifische Regeln erstellt werden, mit welchen die Transfergeschwindigkeit für jeden der sieben Wochentage zu bestimmten Zeiten sekundengenau begrenzt werden kann.

Zugangsfilter

Die vierte Seite (*IP Filter*) besteht lediglich aus zwei Eingabefeldern. Im oberen Feld können Sie bestimmte IP-Adressen von der Verbindung ausschließen. Außer einzelnen Adressen können Sie auch Platzhalter (* und ?) verwenden, um ganze Bereiche von Adressen zu erfassen. Hieraus ergibt sich der Sinn des unteren Feldes, denn dort kann das Verbindungsverbot für bestimmte Adressen wieder aufgehoben werden.

Standardmäßig darf sich jeder mit dem Server verbinden. Um die erlaubten Adressen streng zu limitieren, ist daher der am besten geeignete Weg, im oberen Feld zunächst alle Adressen von der Verbindung auszuschließen und dann im unteren Feld ausgewählte IP-Adressen wieder zuzulassen.

6.2.3 Der Betrieb des Servers

Das Hauptfenster des FileZilla-Servers stellt, wie bereits angedeutet, ein Protokollfenster dar, in dem alle Ereignisse Zeile für Zeile auflistet werden, angefangen beim Start des Servers selbst. Um verstehen und nachvollziehen zu können, was

hier im Einzelnen geschieht, ist es sinnvoll, sich Kenntnisse zu FTP-Befehlen anzueignen, die die Grundlage fast aller Einträge in dieser Liste bilden. Eine Übersicht über die wichtigsten FTP-Befehle finden Sie im Anhang.

Zur Inbetriebnahme des Servers wählen Sie im *Server*-Menü die Option *Active* aus. Dieser Befehl schaltet den Server zwischen Offline- und Online-Modus um. Im Offline-Modus (wenn vor *Active* kein Häkchen steht) können keine Verbindungen zum Server hergestellt werden.

Im Online-Modus kann der Server gesperrt werden. Klicken Sie dazu, ebenfalls im *Server*-Menü, die Option *Lock* an. Der Server ist nun gesperrt, und es werden keine neuen Verbindungen akzeptiert. Die bestehenden Verbindungen bleiben erhalten. Zum Entsperren klicken Sie die Option erneut an. Das Häkchen vor *Lock* verschwindet dann.

Wann immer eine Übertragung stattfindet, können Sie dies in der Verbindungsliste und in der Statuszeile genau verfolgen.

Die Verbindungsliste und die Statuszeile.

In der obigen Abbildung finden zeitgleich ein Upload und ein Download statt. In der Verbindungsliste werden die relevanten Informationen angezeigt. Auch wenn Sie die Verbindungsliste ausgeblendet haben (durch Ziehen mit der Maus), sehen Sie in der Statuszeile die gleichen Angaben noch einmal.

Aktiver und passiver Modus

Es sind zwei grundsätzliche Arten zu unterscheiden, wie der Server betrieben werden kann, nämlich im aktiven oder passiven Modus.

Aktives FTP bedeutet, der Client öffnet einen zufälligen Port > 1023 bei sich und teilt dem Server an Port 21 seinen offenen Port und seine IP-Adresse mit. Daraufhin schickt der Server eine Antwort an diesen Port. Für die Datenübertragung wird dann ein zusätzlicher dynamischer Port ausgehandelt, an den gesendet wird. Dabei läuft die Datenübertragung auf Serverseite über Port 20, wobei die zweite Verbin-

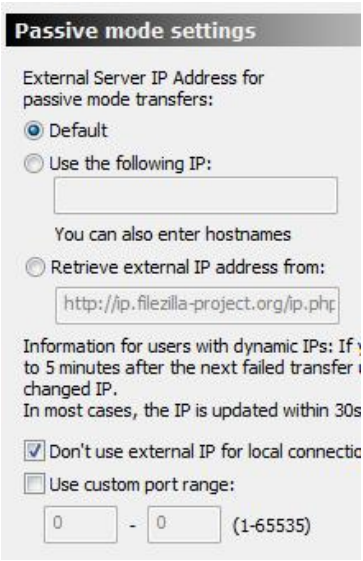
dung aufrecht erhalten bleibt, wodurch Server und Client auch während der Datenübertragung noch miteinander kommunizieren können.

In diesem Fall müssen an der Firewall des Servers Freigaben für Ports 21 und 20 vereinbart werden.

Passives FTP dagegen bedeutet, dass der Server keine Verbindung zum Client aufbauen muss. Beide Verbindungen werden vom Client veranlasst. Der Client sendet an den Server auf Port 21 ein PASV-Kommando und teilt ihm den Port mit, auf dem er lauscht, woraufhin der Server einen Port öffnet und diesen dem Client mitteilt. Die Kommunikation und Datenübertragung läuft dann zwischen diesen beiden Ports ab. An der Firewall des Servers muss also eine Freigabe für Port 21 vereinbart werden.

Passive mode settings

Die sogenannten PASV-Einstellungen sollten Sie verwenden, wenn Ihr Server hinter einem NAT-Router sitzt. Die IP-Adresse des Servers ist dann von außerhalb des Routers nicht zugänglich. Sie können nun die Verwendung der Default-Adresse vereinbaren oder eine bestimmte Adresse in das Feld darunter eingeben. Außerdem gibt es noch die Möglichkeit, die Adresse von einer Website zu beziehen.



Die Einstellungen für den passiven Modus.

Wenn Sie dynamische IPs verwenden, kann eine Änderung der IP dazu führen, dass es nach einem fehlgeschlagenen Transfer bis zu 5 Minuten dauert, bis der FileZilla Server die neue IP-Adresse erkennt. Die Verwendung externer IPs kann für lokale Connections unterbunden werden.

Unter *Use custom port range* können Sie einen Bereich von Ports angeben, die für Verbindungen benutzt werden sollen. Der Sinn dieser Funktion ist etwas umstritten, da man die Ports genauso auch dynamisch zuweisen lassen kann, wobei dann automatisch der nächste freie Port genommen wird.

6.2.4 Verschlüsselung

In Zeiten verstärkter Hacker-Angriffe sollte man Daten nach Möglichkeit nur verschlüsselt übertragen. Beim klassischen FTP sieht es da ganz schlecht aus, denn der komplette Datentransfer findet hier (inkl. Benutzername und Passwort!) unverschlüsselt statt.

Um die Übertragung von Daten sicherer zu machen, gibt es FTP-Erweiterungen, die FTP über SSL und somit eine Verschlüsselung des FTP-Traffics ermöglichen.

Hierfür gibt es verschiedene Implementierungen:

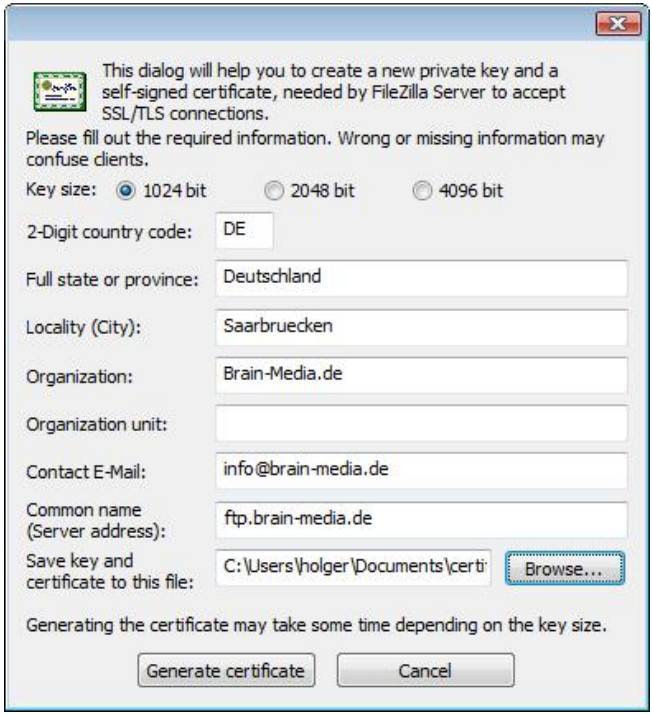
- FTPS (FTP über implizites TLS/SSL)
- FTPES (FTP über explizites TLS/SSL)
- mit dem Kommando *AUTH SSL*
- mit den Kommandos *AUTH TLS* und *PROT P*

Ein wichtiger Hinweis: Lediglich die letzte Variante (FTPES mit *AUTH TLS* und *PROT P*) wird von der IETF (Internet Engineering Task Force) empfohlen! Die beiden anderen Varianten werden als deprecated eingestuft und sollten in neuen Implementierungen nicht mehr verwendet werden. Details hierzu: *http://www.ford-hutchinson.com/~fh-1-pfh/ftps-ext.html#bad*.

Also ist der nächste wichtige Schritt zum Betrieb des Servers die Einrichtung der Verschlüsselung.

Klicken Sie dazu als Erstes auf den Menübefehl *Edit > Settings*, um die Server-Optionen zu bearbeiten, und wählen Sie in der Auswahlliste auf der linken Seite des Fensters die *SSL/TLS settings*. Setzen Sie dann ein Häkchen in das Feld *Enable FTP over SSL/TLS support FTPS*.

Falls noch kein SSL-Zertifikat vorhanden ist, können Sie sich über *Generate new certificate ...* ein neues selbstsigniertes Zertifikat ausstellen lassen. Klicken Sie auf die entsprechende Schaltfläche, um die Dialogbox zu öffnen.

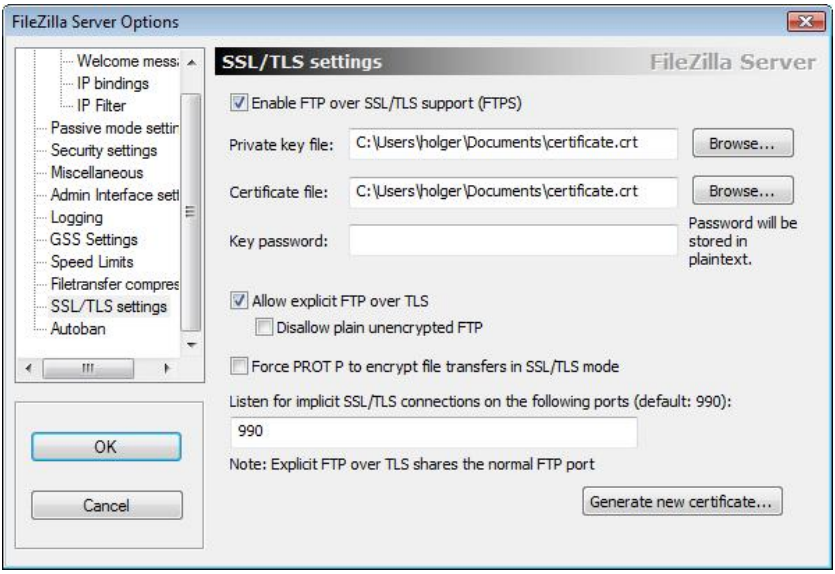


Die Generierung eines neuen Zertifikats.

Die Angaben in den einzelnen Feldern sind rein informativer Natur. Als Speicherort des Zertifikats empfiehlt sich der FileZilla-Programmordner. Die Datei findet sich dann unter *C:\Program Files\FileZilla Server\certificate.crt*.

Wurde das Zertifikat erfolgreich erstellt, erhalten Sie eine Bestätigung und die korrekten Pfade für die Zertifikatsdatei werden automatisch in die Einstellungen eingetragen.

Beachten Sie Folgendes: Wenn Sie das Zertifikat später an einen anderen Ort kopieren, müssen Sie die Pfade im SSL/TLS settings-Dialog von Hand anpassen.



Die SSL/TLS-Einstellungen des Servers.

Wenn Sie diese Einstellungen vorgenommen haben, ist der Server aktiv und wartet auf Verbindungen.

6.2.5 Weitere Einstellungen

Natürlich gibt es noch eine Anzahl weiterer Einstellmöglichkeiten, die von Fall zu Fall nützlich sein können.

Ports, Threads und Timeouts

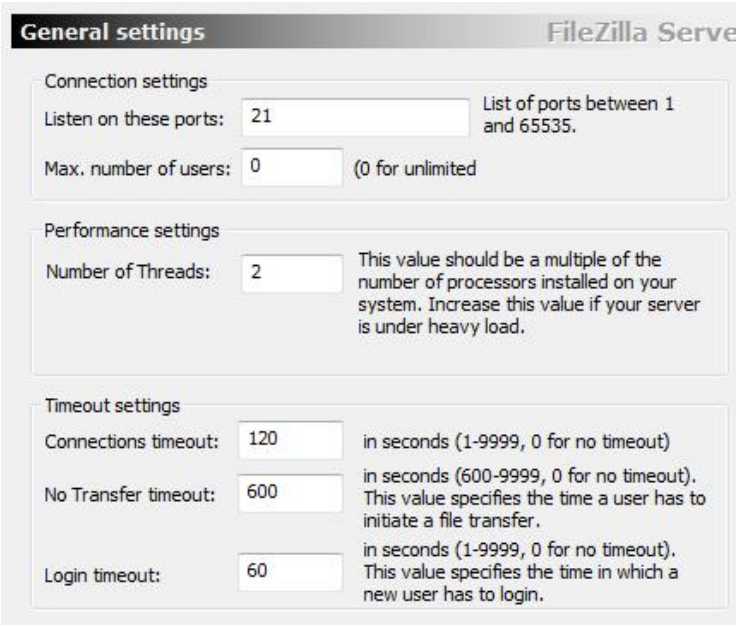
Wenn Sie im Auswahlfeld des Options-Fensters *General settings* wählen, können Sie unter dem Punkt *Connection settings* die Zahl der zugelassenen Ports und Benutzer einschränken. Im nächsten Feld kann die Anzahl der zu verwendenden Threads oder Ausführungsstränge eingestellt werden. Der eingegebene Wert sollte ein Vielfaches der Anzahl der Prozessoren sein, über die der Server verfügt. Bei starker Auslastung des Systems sollten Sie diesen Wert erhöhen.

Im Bereich *Timeout settings* kann im ersten Feld der generelle Connection Timeout in Sekunden eingestellt werden. Zulässige Werte reichen von 1 bis 9999. Wenn Sie 0 eingeben, bedeutet dies, es gibt keinen Timeout.

Der zweite Wert legt fest, wie viele Sekunden der Benutzer hat, um einen Transfer zu veranlassen, bevor er eine Timeout-Meldung erhält. Der Mindestwert ist hier 600, es sei denn, Sie geben 0 ein für gar keinen Timeout.

Der *Login timeout* schließlich bestimmt, wie viele Sekunden einem neuen Benutzer zugestanden werden, bis er sich eingeloggt haben muss. Zulässige Werte reichen hier wieder von 1 bis 9999. Wenn Sie 0 eingeben, gibt es keinen Timeout.

In allen drei Fällen machen Sie nichts falsch, wenn Sie einfach die vorgegebenen Werte übernehmen.



Die allgemeinen Verbindungseinstellungen.

Welcome message

Die Welcome message ist eigentlich selbsterklärend. Geben Sie hier einen Text ein, mit dem der Benutzer nach dem Login begrüßt wird. Jede Zeile darf maximal 75 Zeichen enthalten.

IP bindings

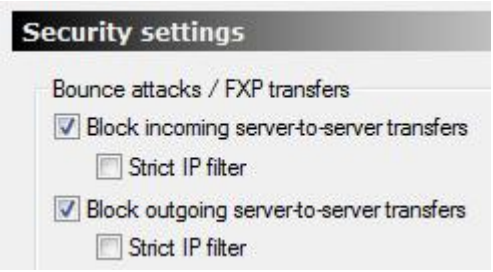
Diese Funktion verwenden Sie, wenn Ihr Rechner über mehr als eine Netzwerkanbindung verfügt, z. B. wenn Sie mehrere Netzwerk-Karten in Ihrem PC stecken haben. Jede dieser Karten hat dann eine eigene IP-Adresse. Mit der Funktion *IP binding*s bestimmen Sie, dass der Rechner nur an der oder den hier angegebenen IP-Adressen auf Verbindungen wartet. Sollen alle vorhandenen IP-Adressen gültig sein, geben Sie ein * ein.

IP Filter

Dies ist die gleiche Funktionalität wie bei der Benutzer- und Gruppenverwaltung. Hier gilt sie allerdings für den gesamten Server.

Sicherheitseinstellungen

Unter *Security Settings* können Sie in zwei getrennten Checkboxen jeweils eingehende und/oder ausgehende Server-to-Server-Transfers unterbinden. Dies dient der Abwehr von sogenannten Bounce Attacks und der Unterbindung von FXP-Transfers.



Die Sicherheitseinstellungen bzgl. Bounce Attacks und FXP-Transfer.

Wenn Sie in eins der Kästchen (oder in beide) ein Häkchen setzen, prüft der IP-Filter vor jedem Transfer die IP-Adresse der Remote-Seite. Wenn diese nicht mit der IP des Steuerkanals übereinstimmt, wird die Übertragung abgebrochen.

Wenn Sie *Strict IP Filter* angewählt haben, wird die komplette IP-Adresse mit der Remote-IP des Steuerkanals verglichen. Dies kann allerdings bei Proxy-Servern zu Problemen führen, wenn sie mehrere IPs verwenden.

Ohne strikten IP-Filter werden lediglich die ersten drei Teile der IP geprüft, was den Schutz vor Bounce- und FXP-Attacken natürlich mindert. Letztendlich müssen Sie also einen Kompromiss zwischen größtmöglicher Sicherheit und Kompatibilität schließen. Die Empfehlung des Programmherstellers ist, alle FXP-Transfers zu sperren und den strikten IP-Filter nur für eingehende Verbindungen zu aktivieren.

Automatische Sperre von IP-Adressen

Autoban ist ebenfalls eine sicherheitsrelevante Einstellmöglichkeit. Legen Sie hier fest, wie viele Versuche ein Benutzer hat, die korrekten Login-Daten einzugeben. Standardmäßig werden eingehende Verbindungen nach einigen Fehlversuchen abgebrochen.

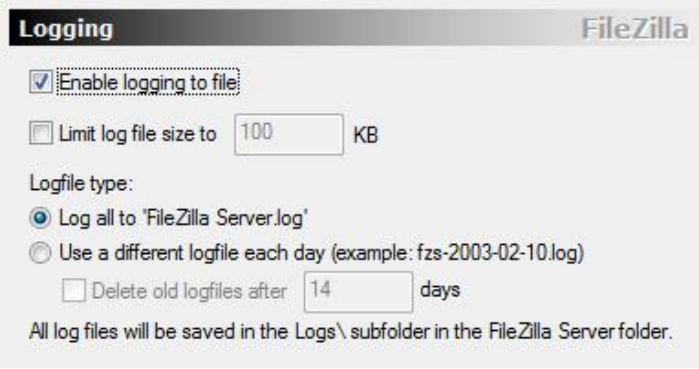
Das automatische Sperren von IP-Adressen.

Zusätzlich können Sie eine automatische Sperre vereinbaren. Hierbei geben Sie einen Wert für die Anzahl von Fehlversuchen an, die Sie einem Benutzer innerhalb einer Stunde zugestehen. Der vorgegebene Wert ist 10. Hat ein Benutzer sich innerhalb einer Stunde zehnmal versucht einzuloggen und dabei nicht die richtigen Daten verwendet, wird seine IP-Adresse automatisch gesperrt.

In einem weiteren Eingabefeld können Sie bestimmen, für wie lange die Sperre wirksam bleibt. Gültige Werte sind zwischen 1 und 999 Stunden.

Log-File

Wenn Sie möchten, dass alle Log-in-Vorgänge in einer Datei gespeichert werden, können Sie dies unter *Logging* definieren.



Das Anlegen eines Log-Files.

Im oberen Kästchen erlauben Sie das Anlegen einer Log-Datei. Darunter haben Sie die Möglichkeit, die Größe der Datei zu begrenzen. Unter *Logfile type* schließlich können Sie festlegen, ob eine einzige Datei verwendet wird oder jeden Tag eine neue. Im letzteren Fall werden alte Dateien nach einer gewissen Anzahl von Tagen gelöscht. Diesen Wert können Sie wiederum selbst bestimmen.

Die Datei oder Dateien werden im Logs-Unterverzeichnis des FileZilla-Serververzeichnisses angelegt. Die Bandbreite für Verbindungen kann unter *Speed Limits* eingestellt werden. Die Vorgehensweise ist identisch mit der beim Anlegen von Benutzern und Gruppen.

Bei Verwendung der MODE Z ftp-Protokollerweiterung ist ein komprimierter Dateitransfer möglich. Die Einstellungen dazu finden Sie unter *Filetransfer compression*.

Erlauben Sie zunächst MODE Z-Unterstützung, indem Sie das obere Kästchen markieren. Geben Sie dann die minimale (zwischen 1 und 8) und maximale (8 oder 9) Komprimierungsstufe ein.

Um eine unnötige Belastung der CPU zu vermeiden, sollte MODE Z nicht innerhalb lokaler Netzwerke verwendet werden. Dies können Sie sicherstellen, indem Sie ein Häkchen in die mit *Exclude private IP address ranges* benannte Checkbox

setzen. In dem großen Eingabefeld können Sie auch explizit IP-Adressen von der Benutzung von MODE Z ausschließen.

6.2.6 Die Schaltflächen und Menüs im Einzelnen

Dieser Abschnitt dient als Befehls-Referenz. Es listet alle Menübefehle des FileZilla-Servers auf und gibt an, in welchem der Menüs der jeweilige Befehl zu finden ist. Außerdem werden, wo vorhanden, die zu den Befehlen gehörenden Schaltflächen abgebildet. Zu jedem Befehl bzw. jeder Schaltfläche wird eine kurze Erläuterung gegeben.

Button	Befehl	Menü	Funktion
-	*Connect to server...*	*File*	Öffnet das Server-Interface.
-	*Disconnect*	*File*	Schließt die Verbindung.
-	*Quit*	*File*	Schließt alle Verbindungen und beendet das Programm.
	*Active*	*Server*	Aktiviert/deaktiviert den Server bzw. schaltet zwischen Online- und Offline-Betrieb um.
	*Lock*	*Server*	Sperrt/entsperrt den Server. Bei gesperrtem Server werden keine Verbindungen akzeptiert.
	*Settings*	*Edit*	Öffnet einen umfangreichen Dialog zur Einstellung von Programmparametern.
	*Users*	*Edit*	Öffnet den Dialog zur Benutzerverwaltung.
	*Groups*	*Edit*	Öffnet den Dialog zur Benutzergruppenverwaltung.
	*About...*	*Help*	Versions-Info zu FileZilla Server
	-	-	Schaltet die Pfadanzeige um.

Button	Befehl	Menü	Funktion
	-	-	Schaltet die Pfadanzeige um.
	-	-	Sortiert die angemeldeten Clients wahlweise nach: • User-ID • Account • IP

7 E-Mail mit XAMPP für Windows

Wenn Sie auf Ihrer XAMPP-Installation eine Applikation aufsetzen wollen, die E-Mail-Funktionalität verlangt, beispielsweise eine Groupware-Umgebung wie eGroupWare oder einen Online-Shop wie osCommerce, so benötigen Sie einen Mailserver, der den E-Mail-Versand abwickelt. Wenn Sie mit Linux arbeiten, ist das alles kein Problem, denn jede Linux-Distribution kommt mit verschiedenen E-Mail-Servern daher, die sich einfach in Betrieb nehmen lassen. Anders ist das bei Windows. Hier stellt das Betriebssystem nicht das benötigte Messaging-System zur Verfügung.

XAMPP für Windows hält hierfür gleich zwei Lösungen für Sie parat: das Mercury Mail Transport System und Fake sendmail. Das Mercury-Mail-System ist ein vollwertiger POP3-, IMAP- und SMTP-Server mit vielen professionellen Zusatzfunktionen, bei Fake sendmail handelt es sich um ein Tool, das den Mail-Versand über einen SMTP-Server erlaubt, selbst aber keine „echten" Messaging-Funktionen bereitstellt. Wir konzentrieren uns in diesem Kapitel auf den Mercury-Mailserver.

7.1 Der Mercury/32-Mailserver

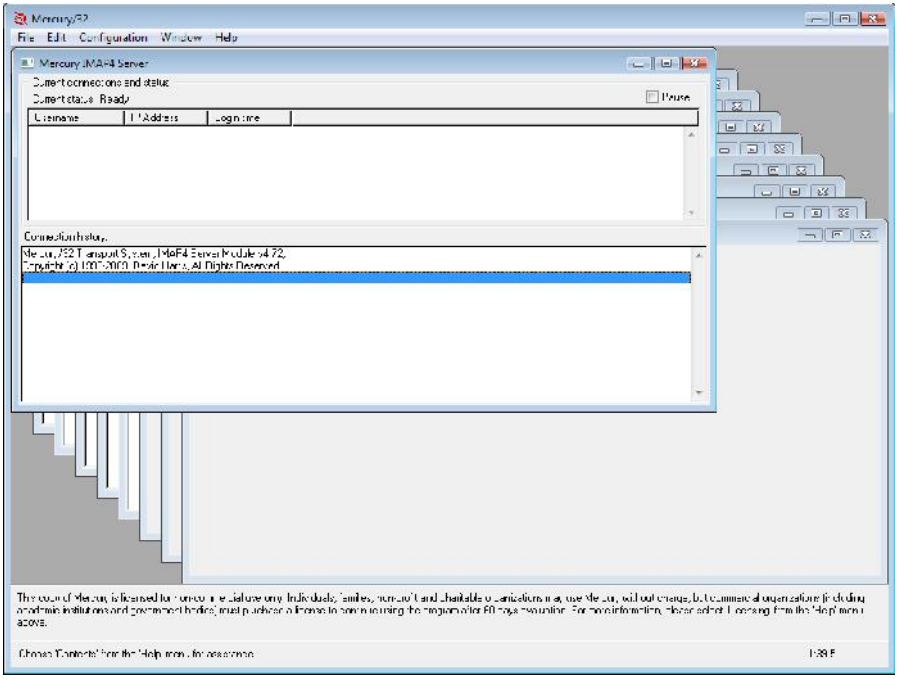
Mit dem Mercury/32-Mailserver (*http://www.pmail.com*), der in XAMPP 1.8.3 in Version 4.62. vorliegt, steht Ihnen ein sehr leistungsfähiges und flexibles Mail-System zur Verfügung. Im Unterschied zu anderen Komponenten des XAMPP-Pakets unterliegt es nicht der GPL, sondern einer speziellen Lizenz des Entwicklers David Harris, der auch für die Entwicklung des Pegasus Mail-Clients verantwortlich ist. Beachten Sie, dass der Einsatz von Mercury MTS, so die Abkürzung, für schulische, nicht-wirtschaftliche Institutionen etc. frei ist. Bei der kommerziellen Nutzung fällt eine benutzerzahlabhängige Lizenzgebühr an. Sie beginnt bei 75 US Dollar für bis zu 15 User. Details finden Sie in der Hilfe des Mailservers.

Anhand der exakten Bezeichnung Mercury/32 Mail Transport System erkennen Sie, dass der Server für die Ausführung auf Windows-32-Bit-Betriebssystemen entwickelt wurde.

7.1.1 Mercury-Quickstart

Die Feature-Liste ist sehr beachtlich. Hier eine Auswahl interessanter Eigenschaften:

- Der Server ist vergleichsweise schlank und schnell. Eine vollständige Installation von Mercury belegt gerade einmal 1,5 MB Plattenspeicher und rund 3 MB des Hauptspeichers unter Windows bei normalem Einsatz. Nach Angaben des Entwicklers kann der Mailserver mehr als 8.000 Mails pro Stunde bei entsprechend ausgestatteten Systemen bearbeiten.
- Die Konfiguration und Wartung gestaltet sich dank der grafischen Benutzungsoberfläche sehr einfach.



Ein erster Blick auf die Administrationszentrale von Mercury/32.

- Auf Grundlage der Filtertechnik von Pegasus Mail bietet Mercury verschiedene Filtermöglichkeiten auf dem Server, die nahezu jede Aktion erlauben. Sie können beispielsweise jede eingehende Mail an eine bestimmte Adresse weiterleiten, ausdrucken oder ähnliche Aktionen ausführen.
- Das POP3-Modul von Mercury kann Mails von verschiedenen POP3-Boxen abholen und an lokale Benutzer verteilen. Auch die sogenannten Domain-Mailboxes werden unterstützt.

- Dank des Schedulers können Sie die Verbindungszeiten und den Betrieb bei Dial-Up-Verbindungen zeitlich steuern.
- Statistische Auswertungen: Der Mailserver präsentiert Ihnen auf Wunsch unterschiedliche grafische Auswertungen, beispielsweise über Mail-Durchsatz, Sicherheitsalarme etc.
- Über die Plug-in-Schnittstelle werden auch spezielle Netzwerkarchitekturen unterstützt. Es sind beispielsweise Plug-ins für Novell Netware Bindery und das NDS verfügbar.
- Über ein spezielles Servermodul können POP3-Nutzer ihr Passwort ändern.
- Der Mercury-Mailserver unterstützt automatische Antworten und automatisches Weiterleiten eingehender E-Mails.
- Über die drei Ebenen des Managements für SMTP-Relaying haben Sie die Kontrolle, wer den Server für das Versenden von E-Mails verwenden darf.
- Der Mail-Server bearbeitet automatisch Listen-Anmeldungen und Abmeldungen, Dateiablieferungen per Mail, Nachschlagen in Adressbüchern und Mailinglistenmanagement.
- Der Server bietet Unterstützung für Mailinglisten, inklusive öffentlicher und privater Listen, moderierte und anonyme Listen, alle mit konfigurierbaren Funktionalitäten. Mercury-Listen können eine unbegrenzte Zahl an Teilnehmern besitzen, und ein einzelner Mercury-Server kann eine unbegrenzte Zahl an Listen verwalten.
- Mercury/32 verfügt über Module für End-to-End-Delivery und Relaying-SMTP.
- Der Server verfügt über umfangreiche Antispam-Funktionen.
- Die Autoresponder-Funktionen erlauben die Kontrolle über Format und Layout von automatisch generierten Nachrichten.
- Es versteht sich von selbst, dass der Mailserver hervorragend mit Pegasus Mail zusammenspielt. Das zeigt sich beispielsweise bei der Funktions- und Zugriffskontrolle über Netware-Gruppenzugehörigkeit.
- Über den integrierten PHP-Server ist das Publizieren von Pegasus Mail-Adressbüchern im Internet möglich.
- Unterstützung für mehrere Mail-Domains auf einem Server.

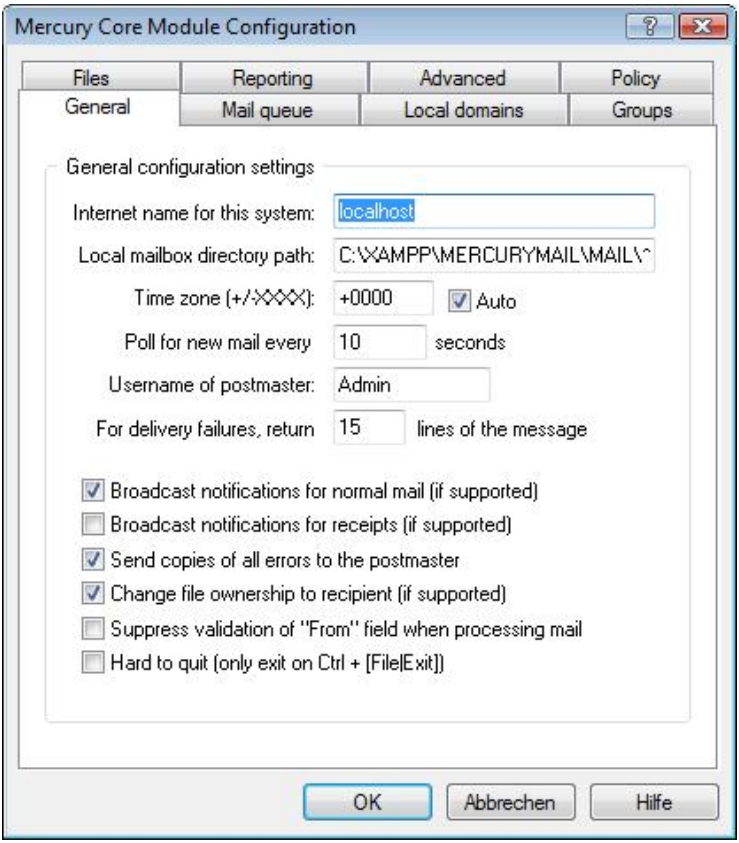
- Kontrollmöglichkeiten über die Verbindungen zu den verschiedenen Server-Modulen.
- Protokollfunktionen für ein- und ausgehende E-Mails.
- Neben SMTP und POP3 steht Ihnen auch ein IMAP4-Modul zur Verfügung.

Sie sehen: Die Liste ist recht lang, wobei längst nicht alle Funktionen genannt sind. Die vollständige Liste finden Sie unter *http://www.pmail.com/over-views/ovw_mercwin.htm*. Der Zugriff auf die Administrationszentrale erfolgt am einfachsten über das XAMPP Control Panel, über das Sie den Server starten und die Admin-Schnittstelle öffnen können. Alle relevanten Dateien des Mailservers finden Sie im XAMPP-Unterordner *MercuryMail*.

Bevor wir uns anschauen, wie man den Server konfiguriert, werfen wir einen kurzen Blick in das Innenleben des Servers. Dieser ist modular aufgebaut. Eigentlich besteht er aus zwei Teilen: dem Mercury-Kernmodul und den verschiedenen Protokollmodulen. Die Kernfunktionen sind in der Datei *Mercury.exe* implementiert. Er sorgt für die Übermittlung von ein- und ausgehenden Mails, stellt sicher, dass Mails lokal zugestellt werden, sorgt für das korrekte Routing und den jeweiligen Modulaufruf, kümmert sich um die Autoresponder-Funktionen etc. Die Module sind eigentliche Protokoll-Module, die dann vom Kern aufgerufen werden, wenn sie gefragt sind. Sie übernehmen dann Protokoll-spezifische Aufgaben. Die Module sind als DLLs implementiert. Es gibt elf Stück:

- **MERCURYS.DLL**: Das ist das SMTP-Server-Modul, das eingehende SMTP-Mails verarbeitet.
- **MERCURYC.DLL**: Das SMTP-Client-Modul für den Versand von ausgehenden SMTP-Mails.
- **MERCURYE.DLL**: Der SMTP-Delivery-Client für ausgehende SMTL-Mails.
- **MERCURYP.DLL**: Das POP3-Server-Modul, das den Zugriff von POP3-Clients erlaubt.
- **MERCURYF.DLL**: Ein einfacher Finger-Server.
- **MERCURYD.DLL**: Ein POP3-Client, der den Blick ins lokale POP3-Postfach erlaubt.

- **MERCURYX.DLL**: Das Scheduler-Modul, mit dem Sie das Starten und Herunterfahren der verschiedenen Module steuern können. Sie benötigen diese Funktion insbesondere bei Einwählverbindungen.



Die Konfiguration der Kernfunktionen.

- **MERCURYH.DLL**: Der PH-Query-Server für Directory-Services.
- **MERCURYW.DLL**: Dieses Modul erlaubt Benutzern das Ändern des eigenen Passworts.
- **MERCURYI.DLL**: Das IMAP4-Server-Modul mit den bekannten Funktionen von IMAP-Servern.

- **MERCURYB.DLL**: Das HTTP-Server-Modul erlaubt die webbasierte Verwaltung von Mailinglisten.

7.1.2 Einstieg in die Mercury-Administration

Entsprechend der Architektur des Servers ist zwischen der Konfiguration der Kern- und der Protokollmodule zu unterscheiden. Hinzu kommen administrative Funktionen für die Benutzerverwaltung. Im ersten Schritt sollten Sie die Domain-Frage klären: Unter welcher Domain soll Ihr Mailserver erreichbar sein? Wenn Sie das System lediglich intern einsetzen, genügt es, wenn Sie auf dem Register *General* unter *Internet name for this system* dann *localhost* beibehalten. Auf dem Register *Local Domains* finden Sie außerdem die Zuordnung von lokalem Server-Name und Internet-Name.

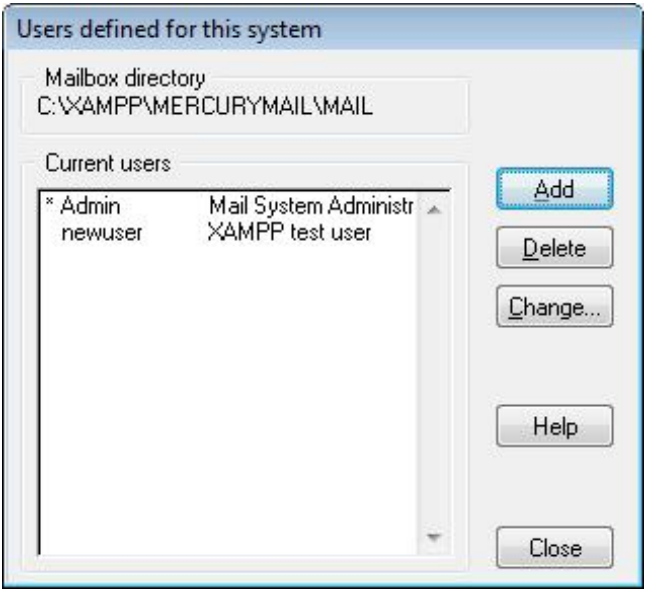
Soll Ihr Server auch von außen erreichbar sein, so müssen Sie auf diesen Registern gegebenenfalls die Einstellungen anpassen. Um eine neue lokale Domain einzurichten, klicken Sie auf *Add new domain* und geben im zugehörigen Dialog den lokalen und globalen Namen an.

Passen Sie gegebenenfalls auch den Pfad zu den lokalen Postfächern auf dem Register *General* an. Auch den Benutzernamen des Postmasters können Sie ändern. Funktionen wie die Policy-Verwaltung, über die ein mailserverweites Erstellen von Richtlinien möglich ist, das Reporting oder die erweiterten Einstellungen des Registers *Advanced* sind in der Regel echten Kennern des Mailservers vorbehalten.

Werfen wir lieber einen Blick auf die Funktionen, die auch beim lokalen Einsatz (bei Testumgebungen) wichtig sind. Eine dieser Funktionen ist sicherlich die Benutzerverwaltung. Die ist über das Menü *Configuration* > *Manage local users* zugänglich.

Bei einer Neuinstallation verfügt das Mercury MTS über drei vordefinierte Benutzer: *admin*, *postmaster* und *newuser*. Die beiden erstgenannten besitzen administrative Berechtigungen und sind für die Systemwartung und -pflege zuständig. Beide besitzen bei Ihrer XAMPP-Installation übrigens kein Passwort. Der Benutzer *newuser* besitzt das Passwort *wampp*.

Die Einstellungen für den Administrator und die Postmaster sollten Sie unbedingt anpassen, bevor Sie weitere Einstellungen verändern. Markieren Sie dazu den jeweiligen Eintrag in der Benutzerverwaltung und klicken Sie anschließend auf *Change*.



Die Benutzerverwaltung von Mercury präsentiert sich schnörkellos.

Um einen neuen Benutzer zu erzeugen, klicken Sie auf die Schaltfläche *Add*, weisen dem User eine Bezeichnung und das Passwort zu. Soll dieser auch sein Pegasus-Passwort ändern können, aktivieren Sie zudem die Option *Administrator previleges (for Pegasus Mail)*. Eine Import- und Exportfunktion stellt die Benutzerverwaltung leider nicht zur Verfügung. Lediglich für die Aliase gibt es das Konsolenprogramm *Malias.exe*. Die Passwörter werden übrigens in der Datei *passwd.pm* eines jeden Users gespeichert, die Sie im MAIL-Ordner der Mercury-Installation finden.

7.1.3 POP3- und SMTP-Konfiguration im Überblick

Die beiden Dienste POP3 und SMTP, der Eine für den Abruf der E-Mails, der Andere für den Versand, sind nach wie vor die wichtigen Services, mit denen Sie sich beim Betrieb eines Mailservers befassen müssen. Schauen wir uns daher an, welche Einstellungen hier von Bedeutung sind.

Um die POP3-Einstellungen aufzurufen, führen Sie den Befehl *Configuration > MercuryP POP3 Server* aus. Der zugehörige Dialog präsentiert Ihnen drei Register: *General*, *Connection Control* und *SSL*. Auf dem Register *General* bestimmen

Sie zunächst den Port, auf den der Server hört, und den Timeout-Wert. Es folgt die Konfiguration der IP-Schnittstelle. Es schließen sich einige allgemeine POP3-Einstellungen an, wie beispielsweise das Markieren von Mails, die der Client vollständig empfangen hat. Außerdem können Sie die Protokolldatei und das Verzeichnis für die Protokollierung bestimmen.

Über das Register *Connection Control* können Sie bestimmen, welche Verbindungen von Clients explizit angenommen bzw. verweigert werden. Um eine erste Kontrollregel zu definieren, klicken Sie auf die Schaltfläche *Add restriction* und bestimmen im zugehörigen IP-Adressbereich, wer Verbindung mit dem Server aufnehmen darf bzw. nicht darf.

Schließlich können Sie SSL- bzw. TLS-Unterstützung für Verbindungen mit POP3-Clients aktivieren. Sie müssen dazu lediglich die Sicherung aktivieren und den Pfad zum Zertifikat angeben. Über die Schaltfläche *Create* können Sie auch ein selbstsigniertes Zertifikat erzeugen.

Die Konfiguration des SMTP-Servers fällt etwas umfangreicher aus. Sie greifen über *Configuration* > *Mercury SMTP Server* auf diese zu.

Neben den drei Registern *General* für die allgemeinen Einstellungen, *Connection Control* für die Verbindungskontrolle und SSL finden Sie hier noch zwei weitere Register: *Spam control* und *Compliance*. Über das Register *Spam Control* können Sie eine sogenannte Blacklist erstellen und pflegen. Bei einer Blacklist (schwarze Liste) handelt es sich um eine Liste mit Domain-Namen, E-Mail-Adressen und IP-Adressen. Passt eine E-Mail zu einem der gelisteten Datensätze, kann sie beim Empfang speziell behandelt werden. Sie kann dann komplett abgelehnt, verzögert, gelöscht oder als Spam gekennzeichnet werden.

In der Standardkonfiguration verfügt das Tool über keine Einträge. Um einen entsprechenden Blacklist-Eintrag zu erstellen, klicken Sie auf dem Register *Spam Control* auf *Add*. Es öffnet sich die Blacklist-/Whitelist-Definition. Weisen Sie dem ersten Filter eine Bezeichnung und einen Hostnamen zu, auf den sie angewendet werden soll. Bestimmen Sie dann die Filterkriterien und anschließend die Folgeaktionen, wie das Ablehnen. Unter *Rejection text* können Sie auch einen Hinweis für die Spammer hinterlegen.

Auf dem Register *Compliance* können Sie schließlich verschiedene Restriktionen für bestimmte Nachrichtentypen definieren.

7.1.4 Konfiguration der Kernfunktionalität

Sie haben nun einen recht guten Überblick über das, was Sie alles mit dem Mercury-Mailserver anfangen können. Schauen wir uns als Nächstes die Details an.

Die Konfiguration des Mercury/32-Mailservers erfolgt über die Konfigurationsdatei *mercury.ini*. In dieser Datei sind alle Einstellungen hinterlegt, die Sie über das Menü *Configuration* an den Mailserver übergeben.

Wenn Sie einen Blick auf die Konfigurationsdatei werfen, werden Sie auch sehr schnell feststellen, dass Sie einfach zu lesen und zu verstehen ist. Die abgespeckte Variante:

```
#  MERCURY.INI generated by Mercury Setup


[General]

myname:          localhost    # Canonical name for this serv-
er

timezone:        +0000    # Time Zone to add to date fields

file_api:        1    # Use the file api instead of queues

mailqueue:       C:\xampp\MercuryMail\QUEUE    # Where mail
should be put for delivery

smtpqueue:       C:\xampp\MercuryMail\QUEUE    # Where the
SMTP client should look for mail

newmail_path:    C:\xampp\MercuryMail\MAIL\~N    # Where to
find the users' WinPMail mailboxes.

...


[Protocols]

MERCURYS.DLL

MERCURYP.DLL

MERCURYE.DLL

# MERCURYC.DLL

MERCURYD.DLL

MERCURYH.DLL

MERCURYF.DLL

MERCURYW.DLL

MERCURYX.DLL

MERCURYI.DLL

MERCURYB.DLL
```

```
[Mercury]
failfile:      C:\xampp\MercuryMail\MERCURY\failure.mer   #
Delivery failure notification template
confirmfile:   C:\xampp\MercuryMail\MERCURY\confirm.mer   #
Delivery confirmation template
aliasfile:     C:\xampp\MercuryMail\MERCURY\alias.mer     #
System-wide alias file


[MercuryC]
Host:             # mail mail host which relays for us
Failfile : C:\xampp\MercuryMail\MERCURY\failure.mer
Poll : 30
Scratch : C:\xampp\MercuryMail\SCRATCH
ReturnLines : 15
Timeout : 30
ESMTP : 1
POP3_Auth : 0
Logfile : C:\xampp\MercuryMail\LOGS\MERCURYC\~y-~m-~d.log
Log_Verbose : 0
Session_logging : C:\xampp\MercuryMail\SESSIONS\MERCURYC
Session_logmode : 0

[MercuryE]
Session_logging : C:\xampp\MercuryMail\SESSIONS\MERCURYE
Session_logmode : 0
Poll : 15
Timeout : 60
Logfile : C:\xampp\MercuryMail\LOGS\MERCURYE\~y-~m-~d.log
Log_Verbose : 0
DNS_Timeout : 20
```

```
DNS_Retries : 4
Transcripts : 1
MaxThreads : 10

[MercuryD]
Scratch : C:\xampp\MercuryMail\SCRATCH\MERCURYD
Timeout : 30
Poll : 120
Session_logging : C:\xampp\MercuryMail\SESSIONS\MERCURYD
Session_logmode : 0

[MercuryS]
Debug : 1
Logfile : C:\xampp\MercuryMail\LOGS\MERCURYS\~y-~m-~d.log
Timeout : 30
Relay : 0
Strict_Relay : 0
Allow_Illegals : 0
SMTP_Authentication : 0
Session_logging : C:\xampp\MercuryMail\SESSIONS\MERCURYS
Session_logmode : 0
Compliance_Settings : 0
Maximum_Failed_Rcpts : 4
Max_Relay_Attempts : 4
SSL_Mode : 0
ST_Blacklisting : 288
No_VRFY : 0
SMTP_ConnFlags : 0

[MercuryP]
```

```
Scratch : C:\xampp\MercuryMail\SCRATCH\MercuryP
Logfile : C:\xampp\MercuryMail\LOGS\MERCURYP\~y-~m-~d.log
Stack : 32768
Mark_Read : 1
SSL_Mode : 0
Login_Disabled : 0
UIDL_nul_list : 1
New_UIDs : 1
No_NUL_passwords : 1
Session_logging : C:\xampp\MercuryMail\SESSIONS\MERCURYP
Session_logmode : 0
Timeout : 60

[MercuryX]
Cmd_Wait: 1
IE4_Dialling: 0
Use_ETRN: 0
Clients_only: 0
Drain_queues: 1
Sunday: 0000,0000,0,0,0,0
...

[Domains]
localhost: localhost
localhost: [127.0.0.1]

[Maiser]
Maiser:          Maiser   # 'Username' of mail server account
Helpfile:        C:\xampp\MercuryMail\MERCURY\maiser.hlp   #
Help sent on failed maiser requests
```

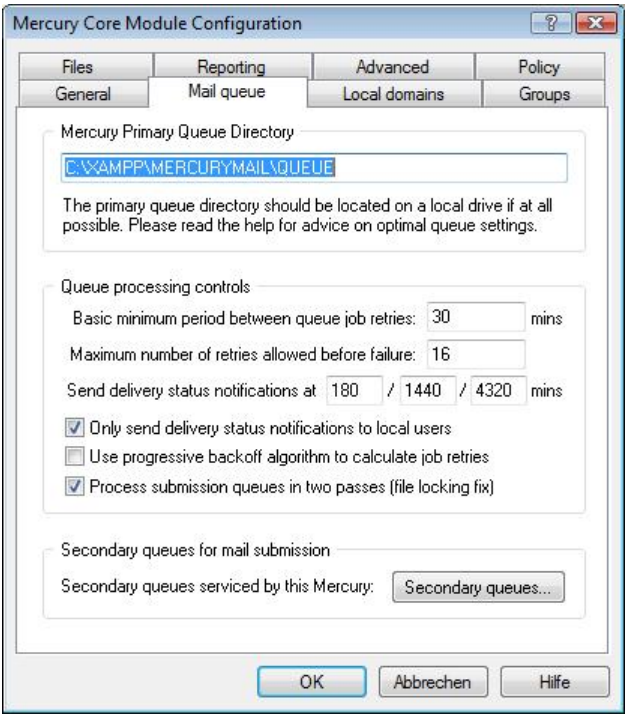
```
Lookupfile:      C:\xampp\MercuryMail\MERCURY\maiser.lkp   #
Format file for the 'lookup' command
Send_dir:        C:\xampp\MercuryMail\MERCURY\SENDABLE   #
Directory for the 'send' command
...

[MercuryH]
Logfile : C:\xampp\MercuryMail\LOGS\MERCURYH\~y-~m-~d.log
Timeout : 30

[MercuryI]
Scratch : C:\xampp\MercuryMail\SCRATCH\MERCURYI
Logfile : C:\xampp\MercuryMail\LOGS\MERCURYI\~y-~m-~d.log
Timeout : 120
Server_Port : 143
Charset : ISO-8859-1
...

[MercuryB]
Scratch : C:\xampp\MercuryMail\SCRATCH\MERCURYB
Logfile : C:\xampp\MercuryMail\LOGS\MERCURYB\~y-~m-~d.log
Timeout : 120
Server_Port : 2224
...

[Groups]
...

[Rewrite]

[Statistics]
```

```
StatFlags:    0  # Statistical reporting settings
STF_Hours:    24  # How often to write stat log files
STM_Hours:    24  # How often to e-mail stat log files
```

Bei der Konfiguration des Mailservers sind einige Dinge zu beachten, damit der Server korrekt arbeitet. Die wichtigsten Punkte, auf die Sie achten sollten sind folgende:

- Der Abschnitt *Local Domains* im Dialog *Core Module Configuration* muss eingerichtet sein.
- Sie müssen den Hostnamen in der Core-Konfiguration auf der Registerkarte *General* angeben.
- Das Warteschlangenverzeichnis muss ebenfalls auf der gleichnamigen Registerkarte angegeben werden.
- Sie müssen den Benutzernamen des lokalen Benutzers spezifizieren, der als Postmaster agiert.

Bei Ihrer XAMPP-Installation ist alles bereits so eingerichtet, dass Sie direkt mit dem Server loslegen können, aber Sie sollten sich bewusst sein, welche Einstellungen essentiell für den erfolgreichen Betrieb des Mailservers sind.



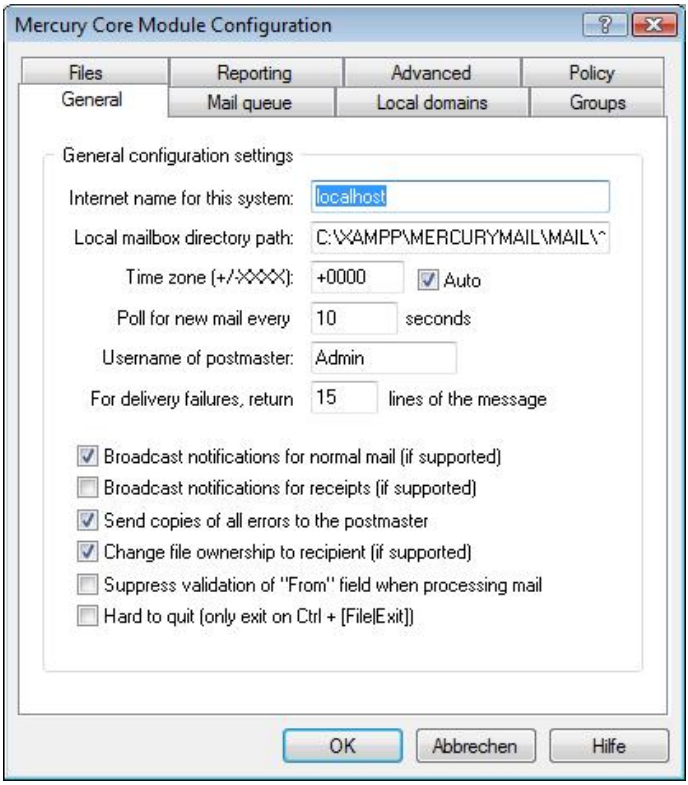
Die korrekte Konfiguration der Warteschlange ist genauso wichtig wie die des Hostnamens.

Wichtig ist außerdem, dass ein temporäres Verzeichnis für Mercury/32 zur Verfügung steht, in das der Server bei der Verarbeitung von E-Mails schreiben und lesen kann.

Die Einstellungen des Kernmoduls sind über den Befehl *Configuration> Core Module Configuration* verfügbar. Auf der Registerkarte *General* nehmen Sie verschiedene allgemeine Einstellungen des Kernmoduls vor. Die Einstellungen im Überblick:

- **Internet name of this system**: Geben Sie hier den Hostnamen an, unter dem Sie den Mailserver betreiben wollen. Mercury verwendet diese Eingabe, um verschiedene E-Mail-Adressen anzulegen, beispielsweise die des Postmasters. Es versteht sich von selbst, dass es sich dabei um einen vollqualifizierenden Domainnamen handeln muss, wenn Sie den Server nicht nur lokal, sondern auch global einsetzen wollen.

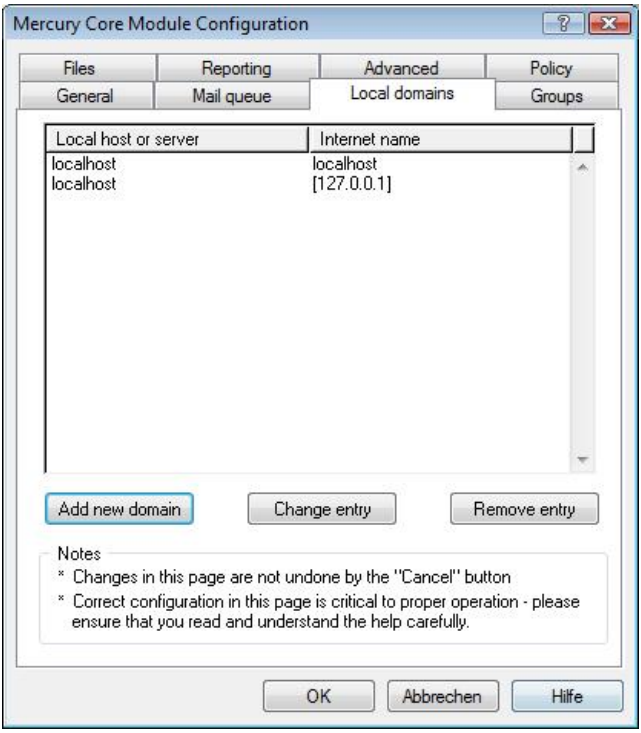
- **Local mailbox directory path**: Diese Einstellung ist nur dann relevant, wenn Sie ein sogenanntes Network Personality-Modul wie das NetWare-Modul, verwenden.
- **Timezone**: Geben Sie hier die Zeitzone in Relation zur GMT an. Am einfachsten verwenden Sie die automatische Zeitzonenoption durch Aktivieren der Option *Auto*. Sie sorgt dafür, dass Mercury die Zeiteinstellungen des verwendeten Betriebssystems verwendet.
- **Poll for new mail every x seconds**: Mit dem Wert in diesem Eingabefeld bestimmen Sie, nach wie vielen Sekunden Mercury prüft, ob E-Mails auf die Verarbeitung in der Warteschlange warten.
- **Username of Postmaster**: Geben Sie den Benutzernamen des Mailserver-Administrators an. Es versteht sich von selbst, dass dieser in der Benutzerverwaltung angelegt sein muss.
- **For delivery failures, return x lines of the message**: Kann Mercury eine E-Mail aus irgendeinem Grund nicht einer lokalen Mailbox zustellen, ruft es eine Template-Datei auf, die eine Standardfehlermeldung erzeugt und den Absender darauf hinweist, dass die Nachricht nicht zugestellt werden konnte. Mit dieser Einstellung geben Sie an, wie viele Zeilen an den Absender zurückgesendet werden.
- **Broadcast notifications for normal mail (if supported)**: Soll Mercury Broadcast-Meldungen versenden, dass neue Mails in dem Postfach eingegangen sind, aktivieren Sie diese Option.
- **Broadcast notifications for receipts**: Entsprechend kann Mercury auch Broadcast-Meldungen beim Eingang von Sendebestätigungen verschicken.
- **Send copies of all errors to the postmaster**: Standardmäßig erhält der Postmaster Kopien aller Fehlermeldungen. So kann er im Einzelfall entscheiden, ob Korrekturen oder andere Anpassungen der Mailserver-Konfiguration erforderlich sind.



Die allgemeinen Einstellungen von Mercury/32.

- **Change file ownership to recipient**: Verschiedene Netzwerkkomponenten unterstützen die Funktion der Dateibesitzerschaft, beispielsweise um die Speicherplatzbelegung zu berechnen. Wenn das von Ihnen verwendete System diese Möglichkeit unterstützt, versucht Mercury, dem Empfänger die Dateirechte zuzuweisen.
- **Suppress validation of „From“ field when processing mail**: Mercury versucht immer herauszufinden, ob die Informationen im From-Header-Feld gültig sind. Durch Aktivieren dieser Option können Sie die Prüfung unterdrücken.
- **Hard to quit**: Wenn Sie dieses Kontrollkästchen aktivieren, ignoriert Mercury alle Versuche, das Programm zu beenden. Ein Beenden des

Programms ist dann nur noch durch Drücken der *Ctrl*-Taste und der anschließenden Ausführung des Menübefehls *Datei> Exit* möglich.



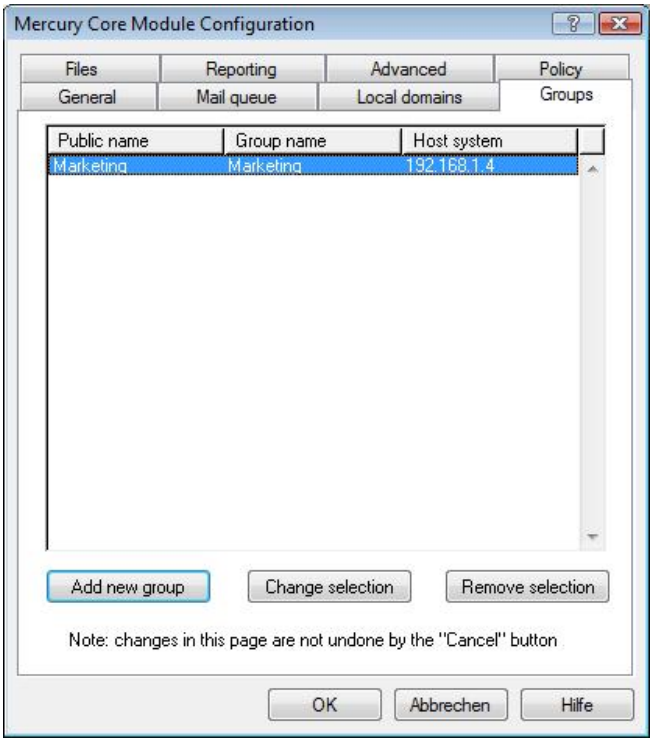
Die *Local domains*-Einstellungen.

Die Einstellungen der Registerkarte *Local domains* sind besonders wichtig – aber auch genauso fehleranfällig. Wenn Sie hier fehlerhafte Einstellungen vornehmen, kann das zu verschiedensten Problemen führen, beispielsweise zu Mail-Schleifen oder zur permanenten Unzustellbarkeit.

Auf dieser Registerkarte legen Sie all die Hostnamen an, Mercury verwendet hierfür vorzugsweise die Bezeichnung *Internet name*, die das System verwenden soll und zwar die, die als „lokal“ betrachtet werden können.

Wichtig dabei ist, dass Sie den Hostnamen und den Internet-Namen angeben, also den, den externe Benutzer verwenden. Wir zeigen Ihnen weiter unten anhand einer typischen Beispielkonfiguration, wie dies in der Praxis aussehen kann. Wenn Sie

den Mailserver lediglich intern einsetzen, genügt es, diesem eine interne IP-Adresse und einen Hostnamen zuzuweisen.

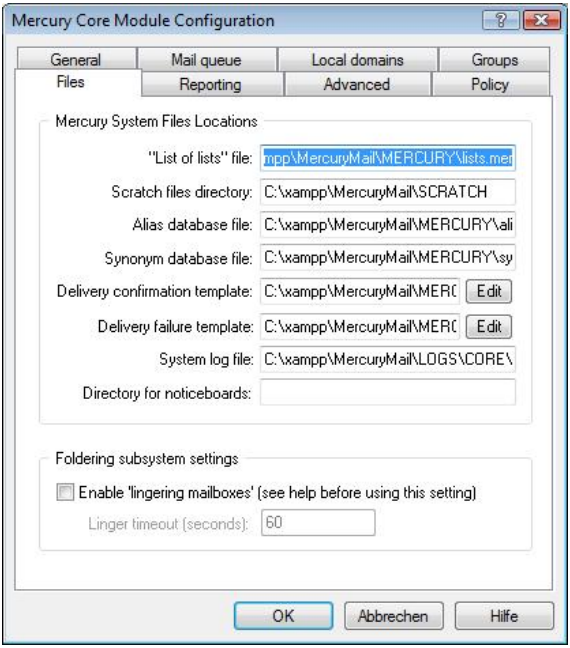


Die Gruppenverwaltung von Mercury.

Eigentlich sehen die E-Mail-Protokolle keine Gruppenfunktionen vor, allerdings findet man derlei Möglichkeiten in typischen Groupware-Umgebungen. Wenn Sie also über ein Netzwerk-Plug-in auch auf Gruppenfunktionen zugreifen wollen, erlaubt der Mercury-Mailserver auf der Registerkarte *Groups* das Anlegen von Gruppen.

Dazu klicken Sie einfach auf *Add new group* und weisen der Gruppe die gewünschte Bezeichnung und einen Namen zu. Sollte die Gruppenverwaltung auf dem gleichen System wie der Mercury-Mailserver ausgeführt werden, geben Sie hier den Hostnamen bzw. die IP-Adresse an. Wird die Lösung auf einem Drittsystem ausgeführt, verwenden Sie entsprechend dessen Daten.

Nehmen wir an, Netware wird auf dem System mit dem Hostnamen *netware-server.de* ausgeführt, und Sie wollen die Gruppe Support einrichten, so geben Sie unter *Public name* beispielweise *technischer_support* und unter *Group name* einfach *SUPPORT* an. Der Support ist dann unter *technischer_support@netware-server.de* erreichbar. Achten Sie darauf, dass Sie nicht den Domain-Namen Ihres Server-Systems verwenden.



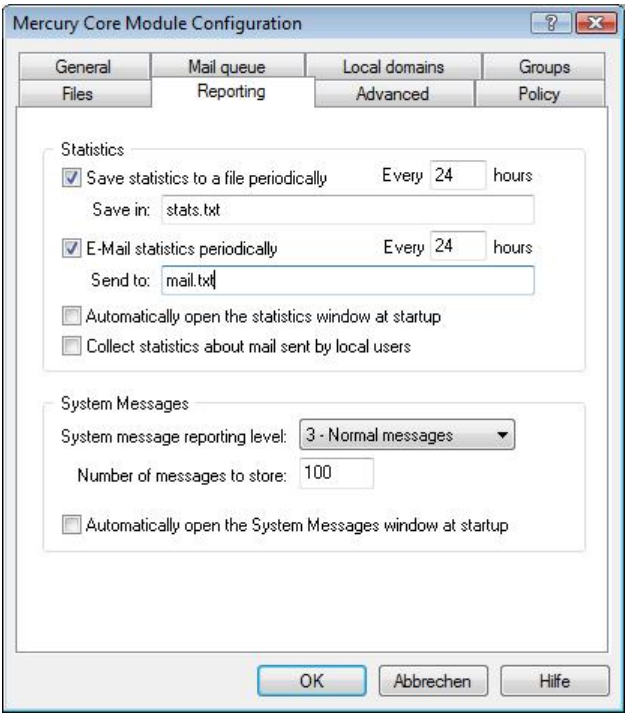
Die Konfiguration der Registerkarte *File*.

Auf der Registerkarte *File* finden Sie die Pfade zu verschiedenen Dateien, die mit bestimmten Funktionen des Mailservers verknüpft sind. In der Regel sind hier keinerlei Pfadanpassungen erforderlich. Lediglich bei zwei Dateien bietet sich eine Anpassung an und ist über die *Edit*-Schaltflächen möglich: Sie können die Templates für die Auslieferungsbestätigung und die fehlgeschlagenen Zustellungen bearbeiten.

Hier ein Beispiel für das Template, das dem Absender übermittelt wird, wenn seine Nachricht nicht an den oder die gewünschten Benutzer zugestellt werden konnte:

```
From: Mail Delivery System <postmaster@~n>
To: ~T
Date: ~D
Subject: Delivery failure notification
MIME-Version: 1.0
Content-Type: Multipart/Report; boundary=~Y

--~Y
Content-type: Text/plain; charset=US-ASCII
Content-description: Mail delivery failure report
Content-disposition: Inline

With reference to your message with the subject:
   "~S"

The local mail transport system has reported the following
problems it encountered while trying to deliver your message:

---------------------------------------------------------------
~R
---------------------------------------------------------------

Your mail message is being returned to you in the next part
of this message.
Should you need assistance, please mail postmaster@~n.
--~Y
Content-type: Message/RFC822
Content-description: Contents of original mail message
~M
--~Y--
```

Die Anpassung ist indes einfach: Klicken Sie einfach auf die *Edit*-Schaltfläche und bearbeiten Sie im Dateieditor den vorgefertigten Textbaustein. Sie können innerhalb eines Templates verschiedene Platzhalter verwenden. Eine Übersicht gibt Mercury aus, wenn Sie im Template-Editor auf die Schaltfläche *Help* klicken.

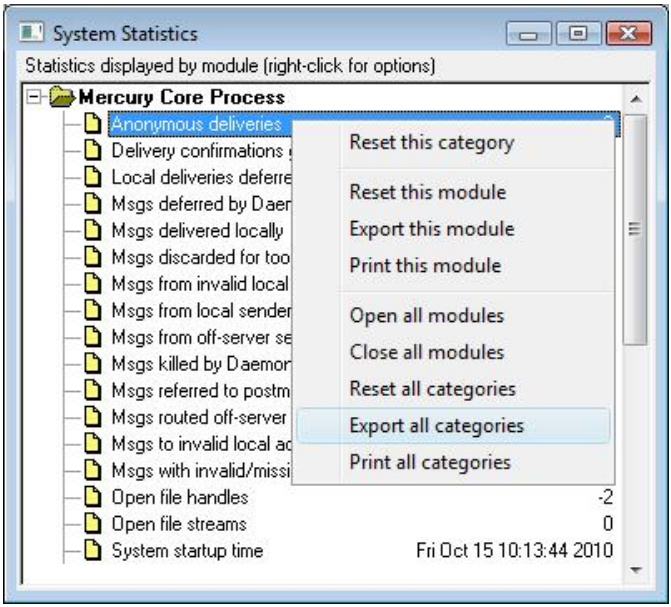


Auf der Registerkarte *Reporting* aktivieren Sie die Berichtfunktionen.

Eine der Stärken des Mercury-Mail-Systems sind Berichtfunktionen. Damit können Sie beispielsweise statistische Informationen über den Mail-Fluss sammeln. Beachten Sie, dass Sie hier nur die Konfiguration der statistischen Daten vornehmen. Die eigentlichen Daten sind über das Menü *Windows > Statistics* verfügbar. Dort können Sie dann für das Kernmodul, aber auch für alle Server und Mercury-eigenen Clients, die verfügbaren Informationen abrufen.

Diese Informationen sind sehr nützlich, wenn Sie sich auf die Fehlersuche machen. Sie können der Statistik beispielsweise entnehmen, wie viele Verbindungen been-

det oder wie viele verweigert wurden und ob es zu Problemen mit dem Passwort gekommen ist.



Die statistischen Informationen liefern Ihnen wertvolle Informationen zur Systemnutzung – gerade auch bei der Fehlersuche.

Für die Konfiguration der Reportfunktionen stehen Ihnen zwei Bereiche zur Verfügung. Im Bereich *Statistics* bestimmen Sie, in welcher Datei die Daten in welchen zeitlichen Abständen gespeichert werden. Auch der Versand per E-Mail alle x Stunden ist an die im Feld *Send to* anzugebende E-Mail-Adresse möglich.

Soll bei dem Programmstart von Mercury der Dialog mit den statistischen Informationen geöffnet werden, aktivieren Sie die Option *Automatically open the statistics window at startup*. Wenn Sie auch Daten über die lokalen Benutzer verwenden wollen, aktivieren Sie die Option *Collect statistics about mail sent by local users.*

Mit den Einstellungen des Bereichs *System Messages* bestimmen Sie, welche Information im Dialog *Window > System Messages* ausgegeben werden. Über das Auswahlmenü *System Level* bestimmen Sie den Grad der Nachrichten. Sie haben die Wahl zwischen sechs Optionen:

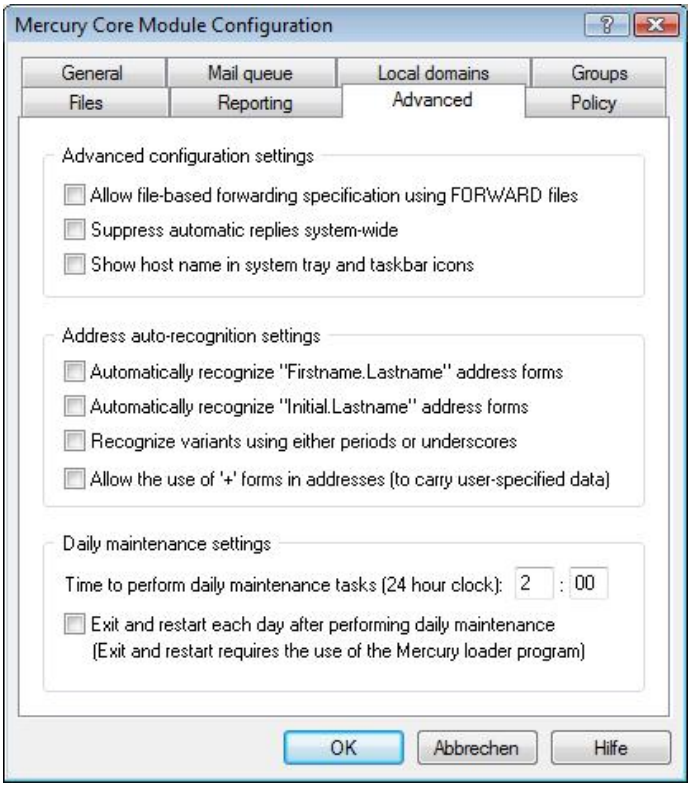
- 0 – No messages
- 1 – Urgent messages
- 2 – Significant messages
- 3 – Normal messages
- 4 – Informational messages
- 5 – Debugging messages

Standardmäßig ist die Option 3 aktiviert. In der Evaluierungs- oder Testphase kann es sinnvoll sein, die Stufe anzupassen. Unter *Number of messages to store* geben Sie an, wie viele Systemmeldungen gespeichert werden. Der Standardwert 100 ist in der Regel ausreichend hoch angesetzt.

Über das letzte Kontrollkästchen können Sie dafür sorgen, dass die Systemmeldungen beim Programmstart geöffnet werden.

Zwei weitere Registerkarten hat die Mercury-Konfiguration noch zu bieten: *Advanced* und *Policy*. Auf der Registerkarte nehmen Sie verschiedene erweiterte Einstellungen vor:

- **Allow file-based forwarding specification using FORWARE files**: Diese Funktion ist nur in Verbindung mit NetWare von Bedeutung.
- **Suppress automatic replies system-wide**: Soll Mercury keine systemweiten Antworten versenden, so aktivieren Sie diese Option. Beachten Sie, dass dabei keine Antworten unterdrückt werden, die durch Filterregeln definiert wurden.
- **Show host name in system tray and taskbar icons**: Sollen der Hostname im Windows-System-Tray und in der Symbolleiste angezeigt werden, wenn Sie den Mauszeiger über das Icon führen, aktivieren Sie diese Option.



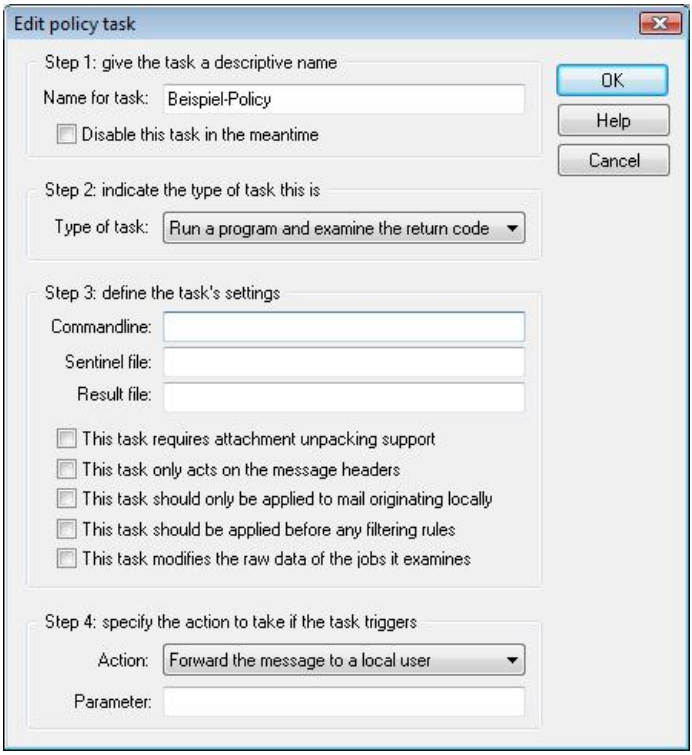
Die erweiterten Einstellungen des Mercury-Mailservers.

Es folgt der Bereich *Addess auto-recogniction settings*, in dem Sie folgende Einstellungen vornehmen:

- **Automatically recognize „Firstname.Lastname“ address forms**: Nehmen wir an, Sie betreiben die Domain *server.de*, so erkennt Mercury daraus automatisch die E-Mail-Adresse *klaus.meier@server.de*.
- **Automatically recognize „Initial.Lastname“ address forms**: Entsprechend kann Mercury die E-Mail-Adresse *klaus@server.de* und *k.meier@server.de* erkennen.
- **Recognize variants using either periods or underscores**: Hierbei handelt es sich um eine ähnliche Funktion, die allerdings auch den Unterstrich nutzt.

- **Allow the use of `+`forms in addresses**: Erlaubt die Verwendung von Pluszeichen in E-Mail-Adressen.

Unter *Daily maintenance settings* bestimmen Sie, in welchen zeitlichen Abständen der Mercury-Mailserver verschiedene Wartungsarbeiten durchführt. Mercury verlangt eine Eingabe im 24-Stundenformat. Bei der Standardeinstellung werden die Arbeiten beispielsweise um 2 Uhr nachts durchgeführt.



Das Einbinden von externen Programmen.

Die Bezeichnung der Registerkarte *Policy* scheint mir ein wenig unglücklich gewählt, da es bei den hier zur Verfügung stehenden Funktionen weniger um das Verwalten von Systemrichtlinien geht, sondern um die Einbindung von Drittprog-

rammen. Mit Hilfe der Policies können Sie beispielsweise folgende Aktionen ausführen:

- Ein- und ausgehende E-Mails auf Viren durch das Einbinden eines Virenscanners überprüfen.
- E-Mails auf Inhalte überprüfen.
- Nachrichten und/oder Attachments in bestimmte Verzeichnisse kopieren.
- Ausführung von beliebigen Systemfunktionen oder Drittprogrammen, um beispielsweise Daten zu sichern.

Die Nutzung der Funktion ist recht einfach: Auf der Registerkarte *Policy* legen Sie mit einem Klick auf *Add new task* eine neue Konfiguration an. Das Erstellen einer Policy umfasst vier Schritte:

1. Sie weisen der Policy eine Bezeichnung zu.
2. Sie bestimmen den Policy-Typ.
3. Sie geben den auszuführenden Befehl an.
4. Sie bestimmen die Aktion, die bei der Ausführung der Policy ausgelöst wird, beispielsweise das Löschen einer Nachricht.

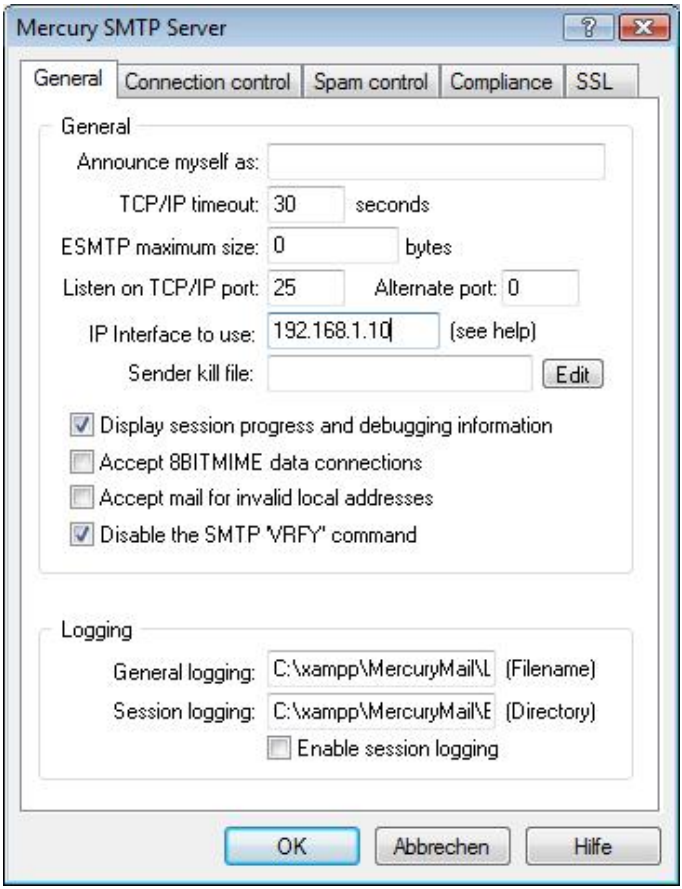
Damit kennen Sie die Konfiguration der wichtigsten Mailserver-Einstellungen und können sich als Nächstes der Konfiguration der verschiedenen Dienste zuwenden.

7.1.5 SMTP-Konfiguration im Detail

Der SMTP-Server ist die zentrale Komponente des Mercury-Mailservers. Sie erlaubt es, E-Mails zu versenden, und zwar sowohl innerhalb eines Netzwerks als auch nach draußen. Die Einstellungen für den SMTP-Server:

- **Announce myself as**: Hier tragen Sie die Bezeichnung des Servers ein, unter welcher der SMTP-Server im LAN ansprechbar ist.
- **TCP/IP timeout x seconds**: Hier bestimmen Sie die Dauer (in Sekunden), die der Server auf Daten des Clients wartet, bevor er die Verbindung als getrennt einschätzt.

- **ESMTP maximum size x bytes**: Hier bestimmen Sie die maximale Nachrichtengröße eines ESMTP-Clients. Beachten Sie, dass nicht alle Clients diese Einstellung unterstützen.
- **Listen on TCP/IP port**: Geben Sie hier den Port an, an dem der Server angesprochen wird. Standardmäßig verwendet man den Port 25.
- **IP Interface to use**: Wenn Ihr Server über mehrere IP-Schnittstellen verfügt, geben Sie hier die IP-Adresse an, die Mercury verwenden soll.



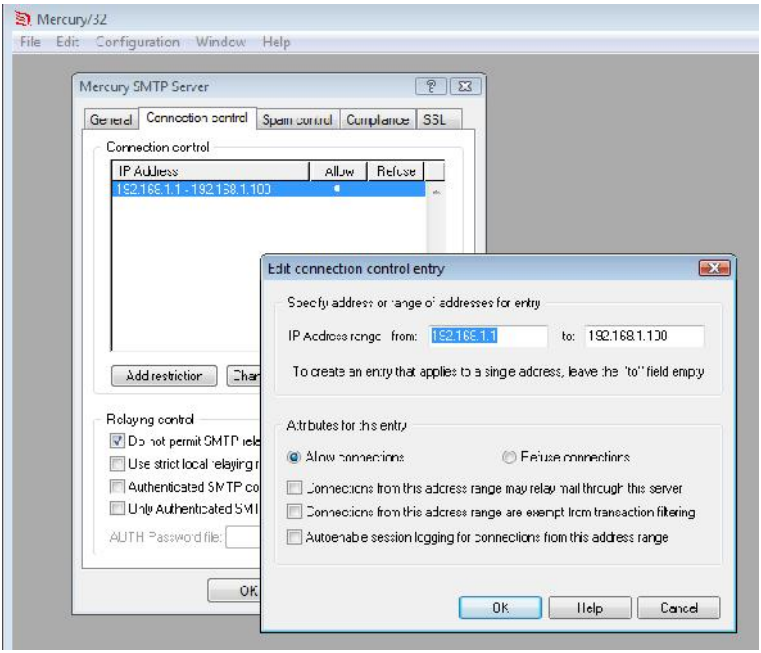
Die Konfiguration des SMTP-Servers.

- **Sender kill file**: Sie können in Mercury eine Liste mit E-Mail-Adressen angeben, von denen das System keine E-Mails annimmt. Geben Sie hier die Adressendatei an. Sie können dabei auch Platzhalter verwenden und so beispielsweise dafür sorgen, dass die E-Mails ganzer Domains nicht akzeptiert werden.
- **Display session progress and debugging information**: Diese Option ist standardmäßig aktiv und sorgt dafür, dass Mercury Details bei der Verarbeitung von E-Mails ausgibt.
- **Accept 8 Bit MIME data connections**: Wenn Sie diese Option aktivieren, kann Mercury die SMTP-Erweiterung 8BITMIME verwenden. Das bedeutet, dass der Mailserver auch E-Mails verarbeitet, die 8-Bit-Daten enthalten.
- **Accept mail for invalid local address**: Normalerweise nimmt Mercury keine E-Mail für Benutzer entgegen, die nicht in der Benutzerdatenbank existieren. Wenn Sie diese Option aktivieren, nimmt Mercury die Mails entgegen, schickt sie aber später an den bzw. die Absender zurück.
- **Disable the SMTP VRFY command**: Das SMTP-Kommando *VRFY* bietet Spammern die Möglichkeit zu überprüfen, ob eine E-Mail-Adresse gültig ist (*VRFY*). Sie sollten dem Spammer daher durch Aktivieren dieses Kontrollkästchen die Möglichkeit nehmen, die Prüfung vorzunehmen.

Den Abschluss der allgemeinen SMTP-Server-Einstellungen gibt die Logging-Konfiguration. Hier legen Sie fest, in welchen Protokolldateien die allgemeinen Aktivitäten und die Session-Informationen aufgezeichnet werden. Mercury erzeugt die allgemeine Protokolldatei nach dem Schema *Jahr-Monat-Tag.log*. In den Protokolldateien finden Sie wichtige Informationen, wenn Sie Fehlern und/oder Problemen auf der Spur sind.

Der SMTP-Server stellt Ihnen vier weitere Registerkarten für die Konfiguration zur Verfügung. Aus der Registerkarte *Connection control* können Sie festlegen, welche Schnittstellen des Systems für den E-Mail-Versand verwendet werden können und welche nicht – vorausgesetzt, Ihnen stehen mehrere zur Verfügung. In der Regel sind es ja mindestens zwei: *localhost* und die aktuelle IP-Adresse.

Bei einer XAMPP-Umgebung finden Sie auf der Registerkarte *Connection control* zunächst einen Eintrag: *localhost* mit der Berechtigung *Allow*. Der Mailserver kann also unter *localhost* Mails entgegennehmen und an die Empfänger weiterleiten – vorausgesetzt, es besteht eine Netzwerk- bzw. Internetverbindung.



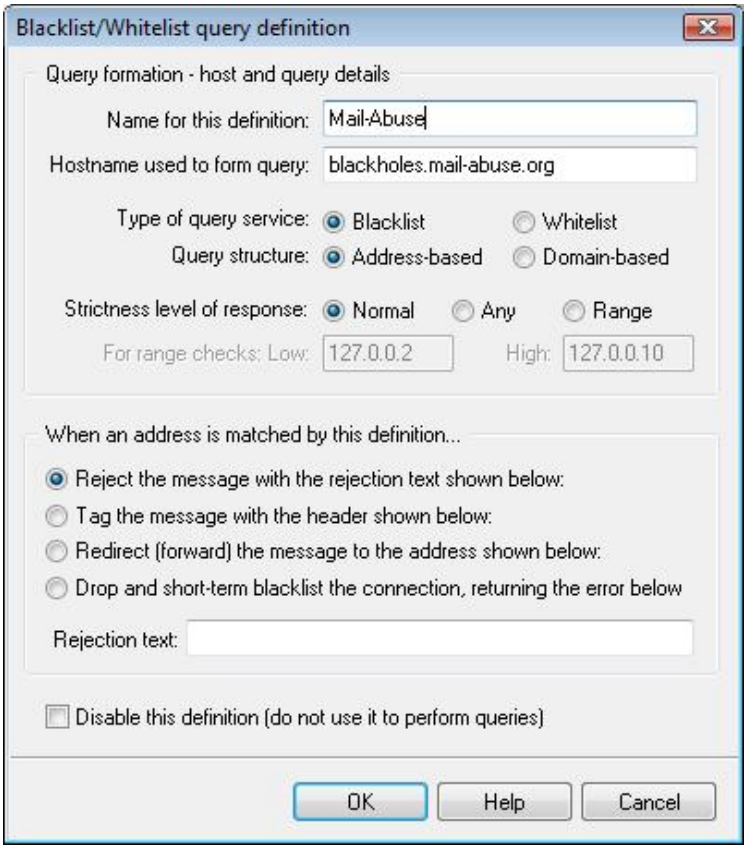
Das Bearbeiten der Verbindungskontrolle.

Die Verwendung der Verbindungskontrolle ist einfach: Um eine neue Einschränkung anzulegen, klicken Sie auf *Add restriction* und weisen der Konfiguration eine Adresse oder einen Adressbereich zu. Wenn Sie lediglich eine Adresse angeben wollen, lassen Sie das *to*-Feld frei. Unter *Attributes for this entry* bestimmen Sie, ob die Verbindung angenommen ober abgelehnt werden soll.

In der Einschränkungsübersicht können Sie auch die Verwendung der Authentifizierung aktivieren. Sie können authentifizierte und unsichere Verbindungen, aber auch nur authentifizierte SMTP-Verbindungen annehmen. In beiden Fällen müssen Sie die Passwortdatei mit den entsprechenden Informationen füttern.

Eine heute (leider) unerlässliche Funktion: Antispam-Schutz. Auch hierfür ist im SMTP-Server-Modul gesorgt. Der SMTP-Server unterstützt die beiden wichtigsten Techniken, die Schutz vor Spam bieten: Blacklist und Whitelist. Erstgenannte (man spricht auch von schwarzer Liste, Negativliste oder einfach nur Index) ist eine Liste mit Domains, E-Mail-Adressen und IP-Adressen, die in der Vergangenheit negativ aufgefallen sind. Passt eine E-Mail zu einem der gelisteten Datensätze, wird sie speziell behandelt. Das kann komplette Ablehnung, Verzögerung, Löschung oder Kennzeichnung als Spam (vergleiche auch Spamfilter und Greylis-

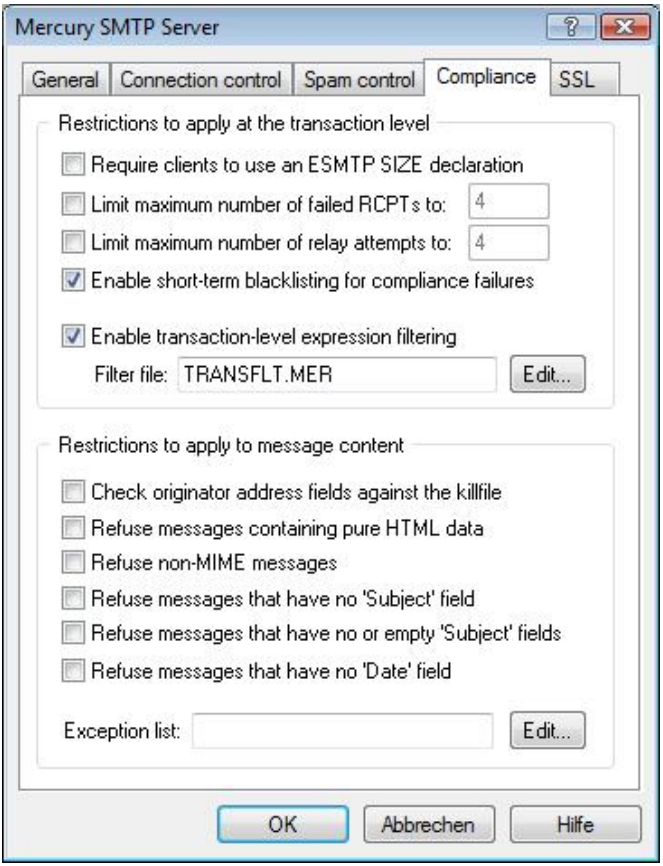
ting) sein. Sie können dabei auf lokale schwarze Listen oder aber Listen zugreifen, die auf zentralen Servern abgelegt sind (genannte Realtime Blackhole List, kurz RBL). Das Gegenstück zur schwarzen Liste bezeichnet man auch als Weiße Liste oder Positivliste (Whitelist).



Der Zugriff auf eine Realtime-Blacklist.

Die Nutzung der Antispam-Funktionen ist einfach: Klicken Sie auf *Add*, um auf einen RBL-Dienst zuzugreifen. Weisen Sie dem Eintrag eine Bezeichnung zu und geben Sie den Hostnamen an, unter der der Dienst erreichbar ist. Geben Sie außerdem an, ob es sich um einen Black- oder Whitelist-Service handelt. Ob Sie weitere Anpassungen aufseiten der Mercury-Konfiguration vornehmen müssen, erfahren

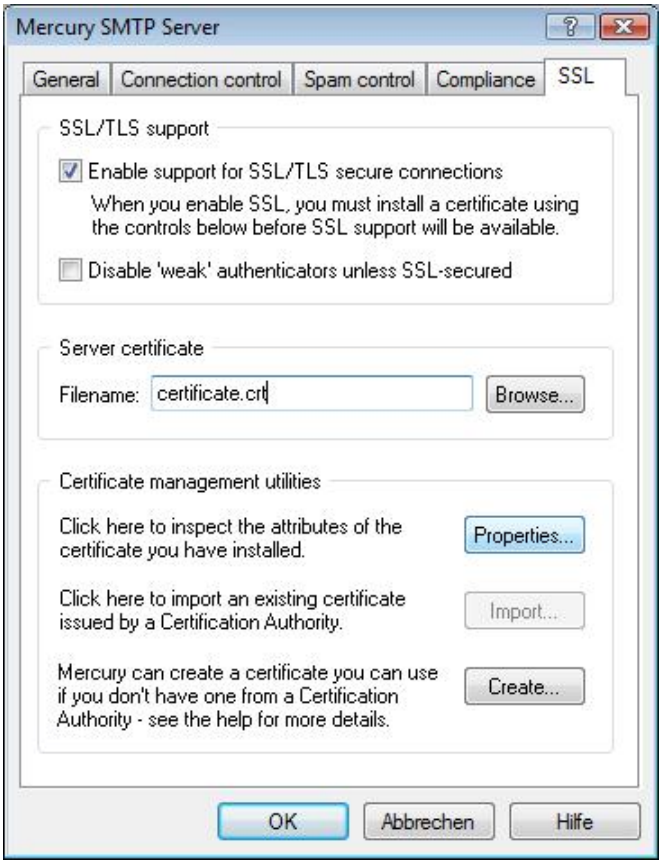
Sie vom Service-Anbieter. Unter folgender URL finden Sie eine Übersicht verfügbarer Services: *http://spamlinks.net/filter-dnsbl-lists.htm*.



Sicher nichts für Neulinge: Die *Compliance*-Einstellungen.

Auf der Registerkarte *Compliance* können Sie verschiedene Checks aktivieren, die E-Mails bestehen müssen, damit Sie von dem Server entgegengenommen werden. Sie können beispielsweise erzwingen, dass der Client das SMTP-Kommando *ESMTP SIZE* verwendet oder dass die Anzahl an Relay-Versuchen einen Wert x nicht überschreitet. Sie können auch verschiedene Einschränkungen hinsichtlich des Nachrichteninhalts vornehmen. Sie können beispielsweise verhindern, dass der SMTP-Server reine HTML-E-Mails verschickt oder Nachrichten weiterleitet, die

keinen Betreff besitzen. Über die *Exception list* können Sie außerdem Ausnahmen von diesen strikten Regeln definieren.

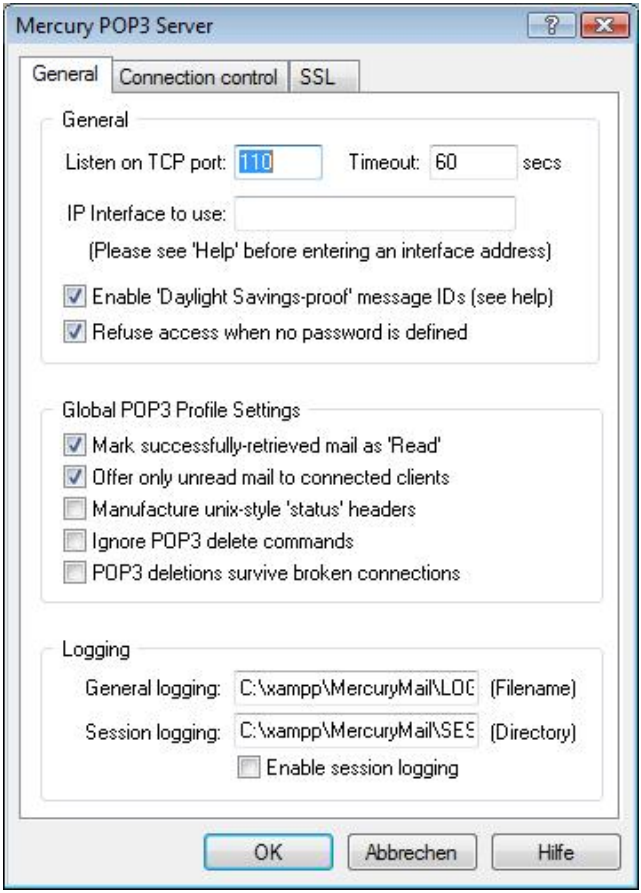


SSL-Unterstützung gefällig?

Die letzte Registerkarte der SMTP-Server-Konfiguration erlaubt Ihnen die Aktivierung und Anpassung der SSL-spezifischen Einstellungen. Um die Verbindung zwischen dem E-Mail-Client und dem SMTP-Server per SSL/TLS abzusichern, aktivieren Sie die Option *Enable support for SSL/TLS secure connections*. Dazu müssen Sie auch das Server-Zertifikat auswählen. Die Registerkarte stellt Ihnen außerdem verschiedene Hilfsmittel zur Seite, mit denen Sie beispielsweise ein Zertifikat anlegen können, um die SSL-Funktionalität prüfen zu können.

7.1.6 POP3-Konfiguration im Detail

Die Konfiguration von POP3- und IMAP4-Servern fällt weniger umfangreich aus, auch weil wir bei diesen Servertypen wieder den beiden Registerkarten *Connection control* und *SSL* begegnen.



Die Konfiguration des POP3-Servers ist überschaubar.

Die Konfiguration des POP3-Servers ist weit weniger aufwendig als die des SMTP-Servers. Auf der Registerkarte *General* können Sie verschiedene allgemei-

ne und globale Profileinstellungen vornehmen. Im Bereich *General* stehen Ihnen folgende Optionen zur Verfügung:

- **Listen on TCP/IP port**: Geben Sie hier den Port an, an dem der POP3-Server zu erreichen ist. In der Regel müssen Sie an der Standardeinstellung 110 keine Änderung vornehmen.
- **Timeout**: Geben Sie hier die Dauer an, die der POP3-Server auf eine Reaktion des Clients wartet, bevor er die Verbindung als beendet bewertet.
- **IP Interface to use**: Besitzt Ihr Server-System mehrere IP-Adressen, so können Sie hier spezifizieren, welche Adresse der POP3-Server verwenden soll.
- **Enable Daylight Savings-proof message IDs**: Das POP3-Protokoll sieht vor, dass jeder Nachricht eine ID zugewiesen wird. Diese soll sich solange nicht ändern, wie die Nachricht im Postfach liegt. Windows weist allen Dateien die Daylight Savings Time (DST) zu. Wenn Sie diese ID verwenden wollen, aktivieren Sie diese Option.
- **Refuse access when no password is defined**: Wenn Sie dieses Kontrollkästchen aktivieren, verweigert der POP3-Server allen Benutzern den Zugriff, die kein Passwort angeben, selbst dann, wenn keines in der Benutzerverwaltung hinterlegt worden sein sollte.

Im Bereich *Global POP3 Profile Settings* bestimmen Sie verschiedene POP3-serverweite Einstellungen:

- **Mark successfully-retrieved mail as Read**: Hat ein POP3-Client eine Nachricht erfolgreich heruntergeladen, wird sie vom Server als gelesen markiert.
- **Offer only unread mail to connected clients**: Ist dieses Kontrollkästchen aktiviert, werden dem Client lediglich die E-Mails angeboten, die noch nicht als gelesen markiert wurden. So ist sichergestellt, dass lediglich neue E-Mails an den Client übermittelt werden.
- **Manufacture unix-style status headers**: Verschiedene Clients, wie Eudora, verlangen einen Nicht-Standard-Header in Nachrichten, die heruntergeladen werden sollen.

- **Ignore POP3 delete commands**: Der Client löscht normalerweise heruntergeladene E-Mails auf dem POP3-Server. Durch Aktivieren dieser Option können Sie dieses Löschen verhindern – und zwar serverweit. Sollten Sie auf das Löschen verzichten wollen, so sollten Sie dieses besser in den jeweiligen POP3-Profilen vornehmen.
- **POP3 deletions survive broken connections**: POP3 stellt normalerweise eine gelöschte Nachricht wieder her, wenn die Verbindung zum Client abgerissen ist und der Server nicht sicher sein kann, dass die Nachricht vollständig beim Client angekommen ist. Wenn Sie dieses Kontrollkästchen aktivieren, wird der Löschvorgang unabhängig von anderen Problemen immer durchgeführt.

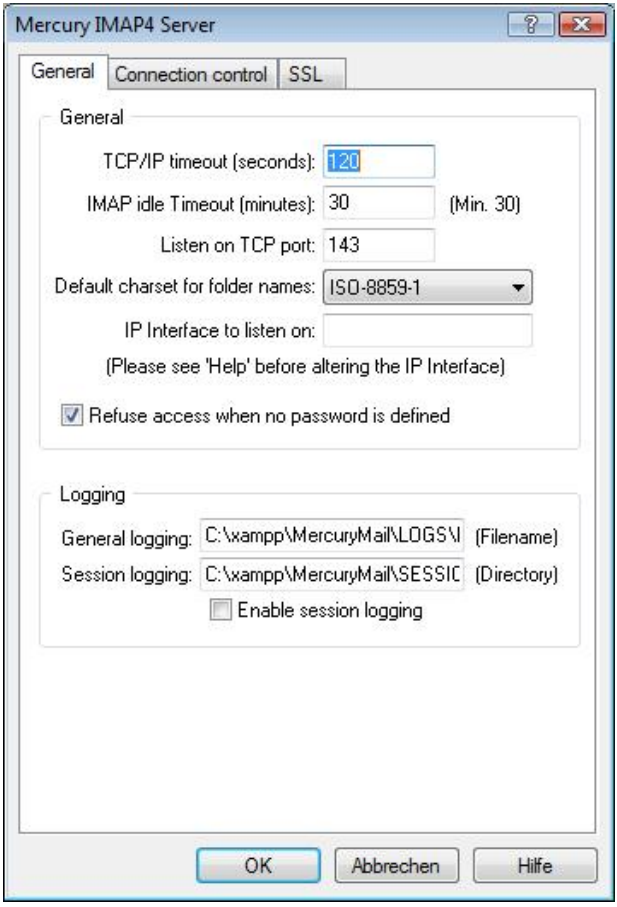
Im Bereich *Logging* können Sie wieder die Pfade zu den Protokolldateien einsehen bzw. ändern.

7.1.7 IMAP4-Konfiguration im Detail

Das POP3-Protokoll ist für den Zugriff auf das eigene Postfach nach wie vor das wichtigste Protokoll, doch es unterliegt einer Vielzahl von Einschränkungen, die IMAP beseitigt. IMAP wurde entwickelt, um Nachrichten nach Bedarf übermitteln zu können und um dem Anwender die Entscheidungsfreiheit zu geben, welche Daten tatsächlich übertragen werden sollen. Der Anwender muss also nicht mehr alle Daten auf den lokalen Rechner übertragen. Vielmehr kann er bestimmen, welche gebraucht werden. IMAP4 bietet eine Vielzahl interessanter Merkmale:

- Hierarchische Mailboxen können auf dem Server eingerichtet werden.
- Mehrere Mailboxen können auf einmal abgefragt werden.
- IMAP bietet die Möglichkeit, Mails zwischen Mailserver und verschiedenen Clients zu synchronisieren. So stehen auf jedem Rechner die gleichen Informationen zur Verfügung.
- Nachrichtenstatus, Header und Struktur können abgerufen werden.
- Der Nachrichtentext oder Teile von mehrteiligen Attachments können heruntergezogen werden.
- Nachrichtenstatus kann auf dem Server verändert werden.
- Speichern, Kopieren und Löschen ist auf Server-Seite möglich.
- Nachrichten auf dem Server können durchsucht werden.

Auch die IMAP4-Server-Konfiguration ist über das *Configuration*-Menü verfügbar. Auf dem zugehörigen Dialog finden Sie neben den allgemeinen Einstellungen auch die Ihnen bereits bekannte Registerkarte *Connection Control* wieder.

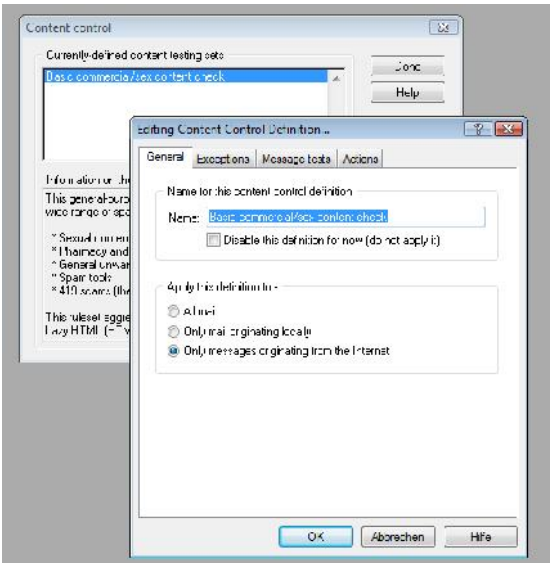


Die Konfiguration des IMAP-Servers ist ebenfalls sehr überschaubar.

Auf der Registerkarte *General* können Sie folgende Einstellungen des IMAP-Servers bearbeiten:

- **TCP/IP timeout**: Bestimmen Sie hier die Dauer in Sekunden, nach der der Server eine Verbindung im Leerlauf als beendet ansieht.

- **IMAP idle Timeout**: Hier geben Sie die Dauer in Minuten an, die vergehen, nachdem der IMAP-Server eine Verbindung im Leerlauf beendet hat.
- **Listen on TCP port**: Geben Sie hier den Port an, den der Server verwenden soll.
- **Default charset for folder names**: Dieses Auswahlmenü erlaubt die Auswahl eines Zeichensatzes, der für die Ordnerbezeichnung verwendet werden kann.
- **IP Interface to listen on**: Sollte das Server-System mehrere IP-Schnittstellen besitzen, so geben Sie die gewünschte hier an, die der IMAP-Server verwendet.
- **Refuse access when no password is defined**: Auch beim IMAP-Server können Sie die Verbindungsaufnahme verweigern, wenn der Benutzer kein Passwort verwendet.



Das Anlegen eines neuen Content-Filters.

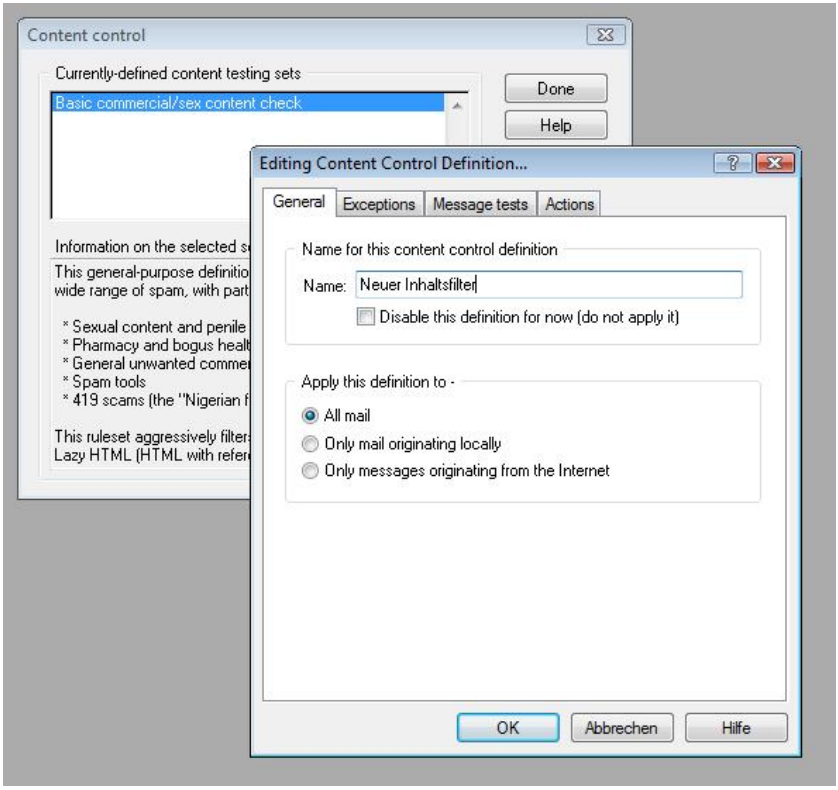
7.1.8 Filterfunktionen

Die elektronische Post hat unseren Alltag und die Kommmunikation revolutioniert. Dank des Mediums E-Mail lassen sich heute eine Vielzahl von Aufgaben, Ab-

stimmungen etc. vereinfachen. Doch die Technik hat auch eine Kehrseite, mit der wir uns alle täglich herumärgern müssen: Spam.

Den unerwünschten Werbe-Mails kann man sich kaum entziehen. Irgendwann landet jeder einmal in einer Spam-Liste und darf sich dann über fragwürdige Angebote freuen.

Einen Schutzmechanismus gegen Spam, den Mercury zu bietet hat, haben Sie bereits kennengelernt: Die Einbindung von Black- und Whitelists. Aber Mercuy hat noch mehr zu bieten: den Content-Filter.

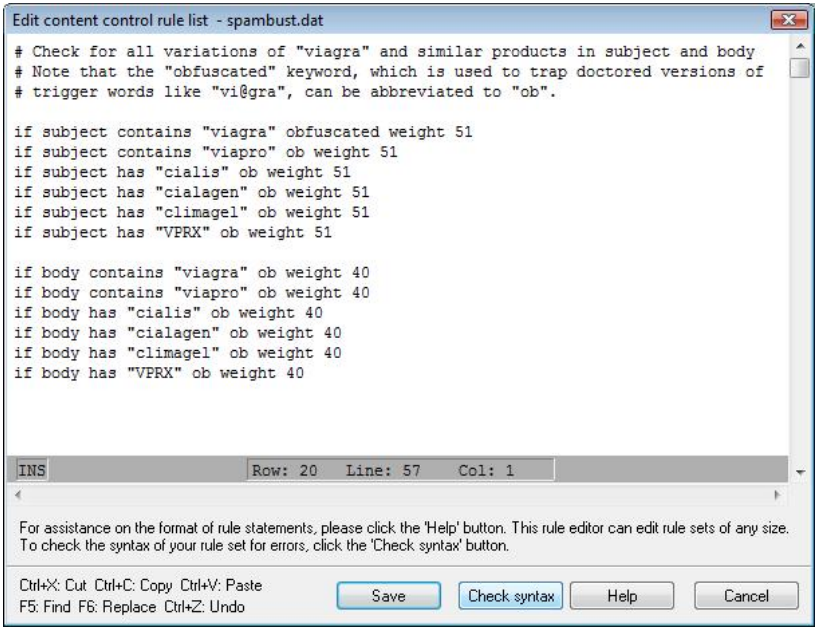


Das Anlegen einer neuen Content-Filterdefinition.

Über das Menü *Configuration* > *Content Control* steht Ihnen eine leistungsfähige Filterfunktion zur Verfügung, mit deren Hilfe Sie E-Mails auf unerwünschte Inhalte überprüfen und dann verschiedene Aktionen auf eine E-Mail anwenden können.

Im *Content Control*-Dialog können Sie quasi beliebig viele Filter einstellen und so auf die unterschiedlichsten Inhalte reagieren. Durch die Reihenfolge der Einträge, die Sie über die *Move up*- und *Move down*-Schaltfläche ändern können, wird die Verarbeitungsreihenfolge bestimmt.

In der Filterverwaltung finden Sie bereits einen vordefinierten Eintrag, der einen sehr ordentlichen Grundschutz bietet.



Die Spambust-Datei sorgt bereits für einen soliden Grundschutz gegen typische Spam-Inhalte.

Wenn Sie die ersten Erfahrungen mit den Filterfunktionen von Mercury sammeln, so bietet es sich an, zunächst mit dem vordefinierten Eintrag zu arbeiten. Die Funktionalität beim Editieren des Eintrags ist mit der beim Anlegen eines neuen Eintrags identisch. Um den Eintrag *Basic commercial/sex content check* zu bearbeiten, markieren Sie diesen und klicken auf die *Edit*-Schaltfläche.

Die Filterfunktion präsentiert Ihnen vier Registerkarten. Auf der Registerkarte *General* finden Sie die Bezeichnung des Content-Filters. Im darunterliegenden Bereich finden Sie eine weitere wichtige Einstellung: *Apply this definition to*. Damit bestimmen Sie, auf welche E-Mails der Filter angewendet wird. Sie haben die Wahl zwischen drei Einstellungen:

- **All mail**: Bei dieser Option wird der Filter auf ein- und ausgehende E-Mails angewendet.
- **Only mail originating locally**: Hier nur auf E-Mails, die vom lokalen System stammen.
- **Only messages originating from the Internet**: Bei der dritten Option wird der Filter lediglich auf E-Mails angewendet, die aus dem Internet stammen.

In der Regel können Sie die Standardeinstellung beibehalten, dass nur die E-Mails geprüft werden, die aus dem Internet kommen.

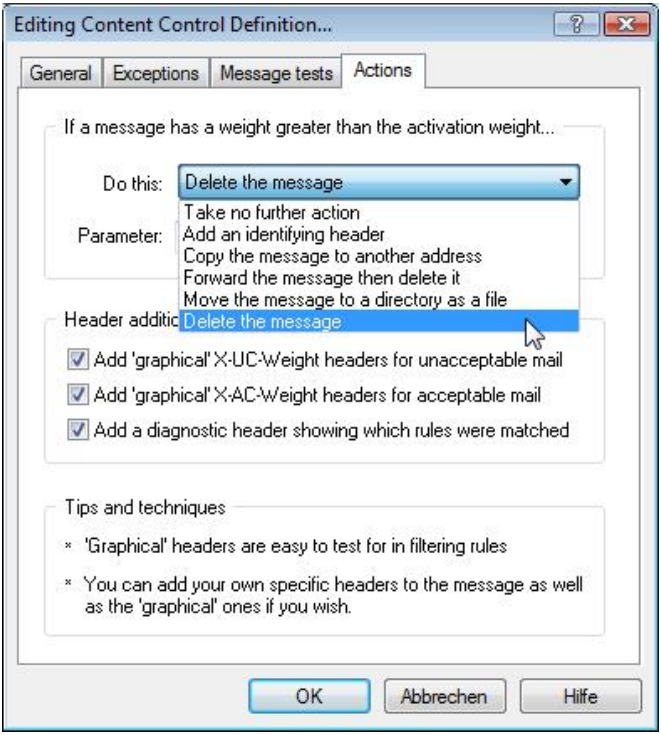
Auf der Registerkarte *Exceptions* legen Sie die Whitelist und die Blacklist an. Sie können beispielsweise aus Ihrem Standard-E-Mail-Programm oder aus einer bestehenden Benutzerdatenbank E-Mail-Adressen in ein Textformat exportieren und diese Daten dann einfach ins Eingabefeld *Whitelist* kopieren.

Die dritte Registerkarte trägt die Bezeichnung *Message Tests*. Ihre Bezeichnung scheint ein wenig unglücklich gewählt, weil es hier nicht um das Testen von Einstellungen, sondern um etwas anderes geht: Sie können einen Regelsatz anlegen – und zwar wieder in Form einer Textdatei –, der dann verwendet wird, wenn die beiden Sätze der Registerkarte *Exceptions* nicht greifen.

Hat der Content-Filter nun eine Nachricht gefunden, in der eine unerwünschte Phrase zu finden ist, so muss die Filterfunktion natürlich noch wissen, was mit dieser Nachricht passieren soll. Genau dazu verwenden Sie die Funktionen der Registerkarte *Actions*. Sie können folgende Aktionen ausführen:

- **Take no further action**: Wenn Sie sich für diese Option entscheiden, werden keine weiteren Aktionen mit der Mail ausgeführt.
- **Add an identifying header**: Hier wird lediglich ein zusätzlicher Header-Eintrag angelegt, der darauf hinweist, dass die Nachricht von der Filterfunktion identifiziert wurde.
- **Copy the message to another address**: Bei dieser Option kopiert die Content-Prüfung die E-Mail an eine andere E-Mail-Adresse. Geben Sie in dem Eingabefeld *Parameter* die gewünschte Adresse an.

- **Forward the message then delete it**: Leitet die Datei an die gewünschte Adresse weiter und löscht Sie dann.
- **Move the message to a directory as a file**: Verschiebt die E-Mail in das unter *Parameter* angegebene Verzeichnis und speichert sie dort als Datei.
- **Delete the message**: Löscht die Nachricht endgültig. Sie kann also nicht wiederhergestellt werden. Verwenden Sie diese Option mit Bedacht, da Sie immer damit rechnen müssen, dass durch unsaubere Filterkonfigurationen auch einmal versehentlich wichtige Inhalte gelöscht werden könnten.



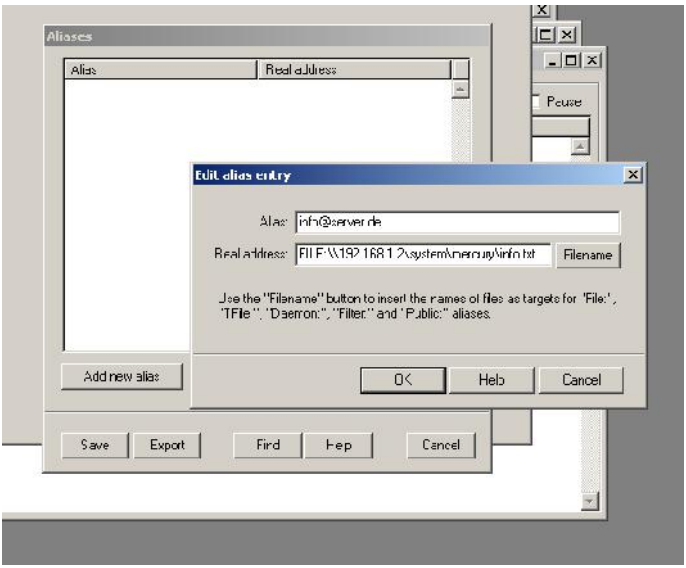
Die Auswahl der Aktionen, die auf die E-Mails mit den gefundenen Inhalten angewendet werden.

7.1.9 Autoresponder

Die Abwesenheitsnotizen, die man erhält, wenn man jemanden anmailt, dieser aber temporär (z. B. wegen Urlaub oder einer Geschäftsreise) nicht per E-Mail erreichbar ist, dürften Ihnen sicherlich auch schon des Öfteren begegnet sein. Auch derlei Meldungen lassen sich mit dem Mercury-MTS-System realisieren.

Der Mercury-Mailserver unterstützt drei Typen solcher automatisch zu versendender Nachrichten:

1. **Einfache Replies**: Das ist der einfachste Weg, um eine Nachricht bei Nichterreichbarkeit zu versenden. Sie erzeugen eine Datei *areply.pm* und legen diese in Ihrem Mail-Unterverzeichnis ab. In der Textdatei hinterlegen Sie Ihre Mitteilung an den Absender.
2. **Programmierte Replies**: Bei dieser Variante erzeugen Sie ein Regelwerk, das beim Eintreten einer spezifischen Bedingung eine Mail zurücksendet. Diese Variante bedeutet etwas mehr Arbeit als die Erste, ist dafür aber auch deutlich flexibler.
3. **Autoresponder**: Schließlich gibt es noch die Autoresponder-Funktion, die in Mercury als eine Variante der Alias-Funktion implementiert ist.



Das Erzeugen eines Alias-Eintrags für den Autoresponder.

Das Einrichten eines Autoresponders ist an sich recht einfach – wie so vieles beim Mercury-Mailserver. Zunächst müssen Sie einen Alias über *Configuration > Aliases* erzeugen.

Klicken Sie auf die Schaltfläche *Add new alias*. In den zugehörigen Dialog geben Sie eine Bezeichnung des Alias ein, die beispielsweise *info@server.de* lauten könnte. Wichtig ist, dass Sie hier die Adresse angeben, die beim Erhalt einer Mail einen spezifischen Nachrichteninhalt versendet.

In das Eingabefeld *Real address* geben Sie dann das Ziel des Alias ein. Meist ist es eine Datei, von der der Pfad spezifiziert werden muss. Soll der Inhalt einer Datei *info.txt* bei einer Nachricht an die angegebene Adresse *info@server.de* versendet werden, so sieht die entsprechende Konfiguration wie folgt aus:

```
FILE:\\192.168.1.2\pfad_zur_Datei\info.txt
```

Sie können auch einen absoluten Pfad angeben:

```
FILE:C:\pfad_zur_Datei\info.txt
```

In diesem Beispiel ist die Datei auf Festplatte C abgelegt.

Die Alias-Funktion unterstützt drei weitere Ziele, die unterschiedliche Aufgaben abdecken können:

- TFile: Dies ist eine Template-Datei.
- Filter: Bestimmt einen Verarbeitungsfilter.
- Daemon: Gibt einen auszuführenden Daemon an.

Mit einer Template-Datei sind so interessante Dinge wie das Einfügen des Absendernamens, des Datums und vieles mehr möglich. Dabei kommen Tilden zum Einsatz. Hier ein einfaches Beispiel für eine solche Template-Datei:

```
From: postmaster@~N (Mail System Administrator)
To: ~T
Subject: Confirmation of delivery
Date: ~D
```

Die beiden anderen Alias-Ziele sind bislang leider auch nicht in der Hilfe dokumentiert.

Eine weitere Besonderheit ist die Exportfunktion des Alias-Dialogs. So können Sie bestehende Autoresponder-Einstellungen einfach auf andere Mercury-Installationen übertragen oder mit anderen austauschen.

7.1.10 Beispielkonfiguration

Zum Abschluss dieses recht umfangreichen Abschnitts möchte ich Ihnen anhand einer typischen Umgebung zeigen, wie die Konfiguration in der Praxis aussehen kann, wenn Sie ein lokales Netzwerk mit E-Mails inklusive Außenanbindung versorgen wollen.

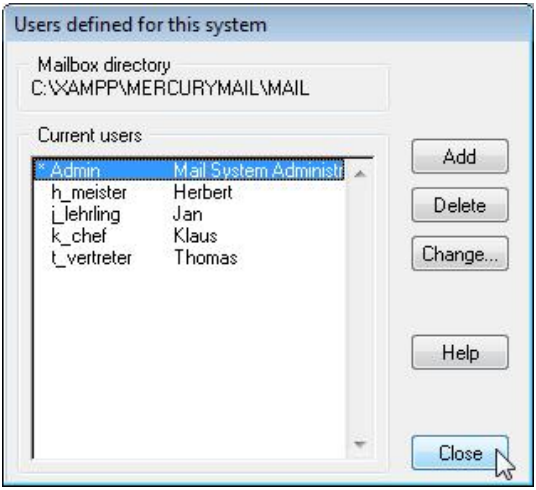
Dazu verwenden wir die Beispiel-Domain *beispiel.de* eines kleinen Beispielunternehmens. Das Unternehmen verwendet bislang die POP3-Postfächer bei einem der vielen Hosting-Services. In dem Unternehmen nutzen vier Leute E-Mail:

- Klaus – Chef
- Herbert – Meister
- Jan – Lehrling
- Thomas – Vertreter

Die Benutzerdaten fasst nachstehende Tabelle zusammen:

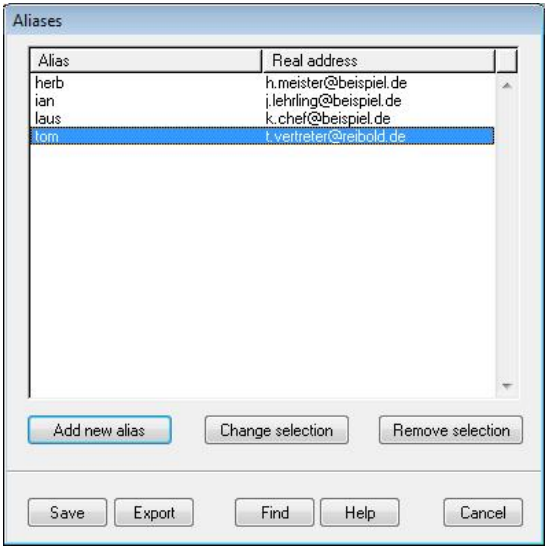
Benutzer	Username	Passwort	E-Mail-Adresse	Alias
Klaus	k_chef	geheim	k.chef@beispiel.de	laus
Herbert	h_meister	geheim	h.meister@beispiel.de	herb
Jan	j_lehrling	geheim	j.lehrling@beispiel.de	ian
Thomas	t_vertreter	geheim	t.vertreter@beispiel.de	tom

Zunächst gilt es, die Benutzer in der Benutzerverwaltung anzulegen. Dazu führen Sie den Befehl *Configuration> Manage local users* aus und legen die Benutzer an.



Die Benutzer sind angelegt. Sie können den Dialog mit *Close* schließen.

Im nächsten Schritt weisen Sie Alias-Namen den realen Namen zu. Dazu führen Sie den Befehl *Configuration> Aliases* aus und legen die Alias-Einträge an.

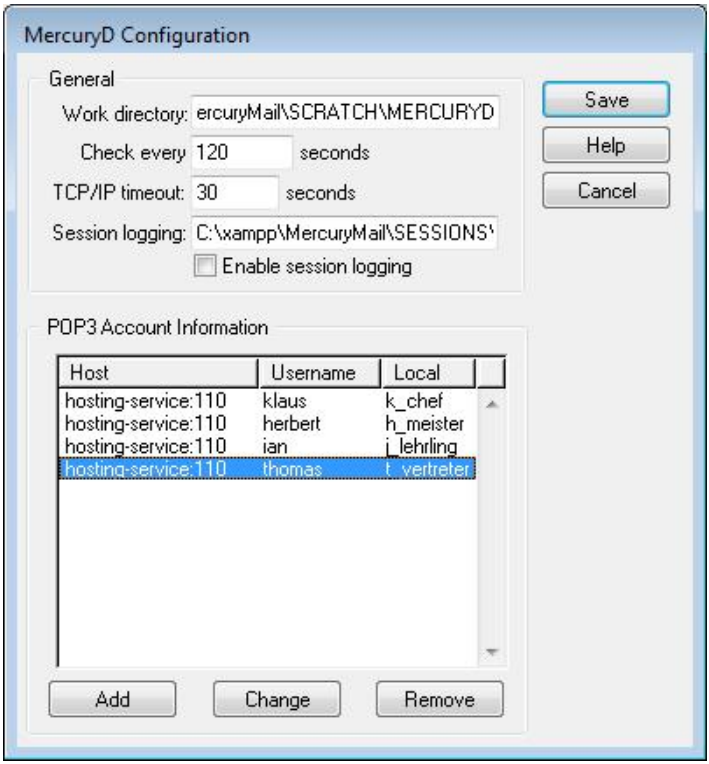


Die Alias-Konfiguration ist abgeschlossen.

Es Ihrer Aufmerksamkeit sicherlich nicht entgangen, dass Mercury über einen eigenen POP3-Client verfügt. Dieses Modul dient dazu, vom lokalen System aus die verschiedensten POP3-Postfächer abzufragen und die E-Mails auf das lokale System zu übertragen. Sie können mithilfe des POP3-Clients beliebige Postfächer abräumen und deren E-Mails lokal verfügbar machen.

In unserem Beispiel legen Sie also für die vier Benutzer die POP3-Accounts an, die die Postfächer bei dem Hosting-Service abfragen.

Es versteht sich von selbst, dass die Mercury-Benutzernamen nicht mit denen bei einem Hosting-Service identisch sein müssen. Meist sind sie sogar unterschiedlich. Wie Sie nachstehender Abbildung entnehmen können, sind die Benutzernamen beim Hosting-Service mit dem „normalen“ Vornamen des Benutzers identisch.



Der in Mercury integrierte POP3-Client übernimmt die Rolle des Sammeldienstes und lädt die E-Mail der Benutzer aus verschiedenen bestehenden Postfächern herunter.

Damit haben Sie eine voll funktionstüchtige Umgebung und die genannten Benutzer können mit Ihren Clients die Mails direkt beim Mercury-Mailserver abrufen.

Womöglich ist es sinnvoll, auch den SMTP-Client zu konfigurieren. Das ist beispielsweise dann sinnvoll, wenn Sie Ihr Netzwerk durch eine Firewall schützen und Drittsysteme Ihren Server nicht direkt kontaktieren können.

7.2 Fake sendmail

Mit Fake sendmail (*http://www.glob.com.au/sendmail/*) steht Ihnen ein zweites Werkzeug für den E-Mail-Versand zur Verfügung. Im Vergleich zum Mercury-Mailserver stellt es allerdings nur eine sehr eingeschränkte Funktionalität zur Verfügung. Um genau zu sein, taugt es lediglich als einfache Schnittstelle für den E-Mail-Versand. Es simuliert die -t-Option des Sendmail-Servers. Das Tool kann beispielsweise von PHP-Anwendungen für den Mail-Versand, genauer die Mail-Weiterleitung an einen echten SMTP-Server verwendet werden.

Die Funktionalität ist also sehr eingeschränkt. Auf der Website des Entwicklers steht auch eine Variante zum Download bereit, die SSL/TLS unterstützt.

Die Konfiguration von Fake sendmail erfolgt in der *sendmail.ini*. In der Konfigurationsdatei müssen in der Regel folgende Einstellungen definiert bzw. angepasst werden:

- SMTP-Server, der den weiteren Transport übernimmt.
- Eventuell Benutzername.
- Eventuell ein Passwort.
- Die E-Mail-Adresse.

All diese Einstellungen finden Sie im sendmail-Abschnitt der Fake-sendmail-Konfiguration. Hier ein Beispiel für die Fake-sendmail-Konfiguration:

```
; Beispielkonfiguration für Fake sendmail. Existiert die Datei nicht, prüft das Tool die Registry-Einstellungen in folgendem Schlüssel: HKLM\Software\Sendmail

[sendmail]


; Hier geben Sie den SMTP-Server Ihrer Domain an, der für die eigentliche Weiterleitung sorgt.
```

```
smtp_server=mail.server.de

; Hier geben Sie den SMTP-Port an.
smtp_port=25

; Hier die Standard-Domain.
default_domain=server.de

; Hier geben Sie den Pfad zur Protokolldatei an.
error_logfile=error.log

; Hier die Datei und den Pfad zu den Debug-Logs.
debug_logfile=debug.log

; Sollte Ihr SMTP-Server die Authentifizierung erfordern,
geben Sie hier den Benutzernamen und das Passwort an.
auth_username=
auth_password=

; Wenn der SMTP-Server vor der Authentifizierung POP3 verwen-
det, müssen Sie hier ebenfalls die POP3-Kennung angeben.
pop3_server=
pop3_username=
pop3_password=

; Um eine spezifische Absender-E-Mail zu erzwingen, geben Sie
diese hier an.
force_sender=

; Hier können Sie den Hostnamen angeben.
hostname=
```

Wenn Sie Probleme mit dem Tool haben sollten, finden Sie auf der Website des Entwicklers einige typische Problemlösungen.

Insgesamt bietet XAMPP für Windows – insbesondere dank des Mercury-Mailservers – eine beachtliche E-Mail-Funktionalität. In der Regel ist das weit mehr, als die meisten Anwender benötigen.

8 Mehr PHP-Power dank eAccelerator und PEAR

Wenn Sie auf einer XAMPP-Installation aufwendige Applikationen ausführen, so kommt irgendwann der Punkt, an dem Sie sich auf die Suche nach Optimierungsmöglichkeiten machen. Gerade PHP-Anwendungen sind heute sehr komplex, man denke nur an PHP-basierte Anwendungen wie Joomla! oder Magento. XAMPP verfügt über zwei Tools, die PHP optimieren und ausbauen helfen: Mit dem eAccelerator sorgen Sie für eine beschleunigte Ausführung des PHP-Codes, mit dem PEAR-Modul erweitern Sie die Funktionalität Ihrer PHP-Installation.

8.1 eAccelerator

Im XAMPP-Paket ist ein Tool enthalten, das – richtig eingesetzt – die Performance von PHP-Anwendungen spürbar verbessert. Die Rede ist von eAccelerator, einer Open-Source-Lösung zum Einsatz auf Webservern, die als Beschleuniger, Optimierer und Cache für PHP-Seiten dient. Es handelt sich dabei um einen Fork von TurckMMCache, der ursprünglich von Dmitry Stogov entwickelt wurde.

Was leistet der Beschleuniger aber eigentlich genau? Nun, die Beschleunigung des PHP-Codes wird erreicht, indem der PHP-Code in kompiliertem Zustand gespeichert wird und somit das wiederholte Kompilieren des PHP-Codes bei jedem Aufruf nahezu vollständig entfällt. Der eAccelerator speichert den kompilierten PHP-Code im Shared Memory und führt bei einem erneuten Aufruf direkt den kompilierten PHP-Code aus dem Hauptspeicher aus.

Außerdem kommen verschiedene Optimierungen zur Laufzeit zum Einsatz, die der Ausführung des PHP-Codes zusätzlichen Schwung geben. Welche das im Detail sind, sind dem Autor leider nicht bekannt.

Eine der spannendsten Fragen ist sicherlich, welche Performance-Steigerungen man mit einem Tool wie eAccelerator erreichen kann. Sie dürfen davon ausgehen, dass die Serverlast deutlich reduziert wird. Laut unterschiedlicher Quellen erhöht sich die Geschwindigkeit bei der Ausführung des PHP-Codes um das Ein- bis Zehnfache.

Sie können den eAccelerator in Verbindung mit PHP 4.x und PHP 5.0.x verwenden. Außerdem unterstützt das Tool folgende Plattformen:

- Linux
- FreeBSD
- Mac OS X
- Solaris
- Windows

Sie müssen den eAccelerator nicht unbedingt in Verbindung mit XAMPP und dem Apache einsetzen. Sie können den Beschleuniger auch mit dem Apache HTTP Server 1.3, 2.0, 2.2, 2.4, lighttpd (über FastCGI) und dem Internet Information Server einsetzen.

Die Konfiguration des Beschleunigers und der gesamten Beschleunigungsumgebung erfolgt über verschiedene Dateien. Die wichtigsten sind die folgenden:

- cache.php
- eaccelerator_cache_output.php
- eaccelerator_cache_page.php
- eaccelerator_cache_result.php
- eaccelerator_lock.php
- encoder.php
- info.php
- loader.php
- session.php.
- shared_memory.php.

Bevor Sie sich allerdings an die Anpassung der Konfiguration machen, müssen Sie den eAccelerator über die *php.ini* aktivieren. Dazu editieren Sie die ini-Datei und suchen folgenden Abschnitt:

```
[eAccelerator]
;extension=eaccelerator.dll
;eaccelerator.shm_size = "0"
;eaccelerator.cache_dir = "/opt/lampp/temp/eaccelerator"
```

```
;eaccelerator.enable = "1"
;eaccelerator.optimizer = "0"
;eaccelerator.debug = "0"
;eaccelerator.check_mtime = "1"
;eaccelerator.filter = ""
;eaccelerator.shm_max = "0"
;eaccelerator.shm_ttl = "0"
;eaccelerator.shm_prune_period = "0"
;eaccelerator.shm_only = "0"
;eaccelerator.compress = "1"
;eaccelerator.compress_level = "9"
;eaccelerator.keys = "shm_and_disk"
;eaccelerator.sessions = "shm_and_disk"
;eaccelerator.content = "shm_and_disk"
;eaccelerator.admin.name =
;eaccelerator.admin.password =
```

Sie finden den relevanten Abschnitt am Ende der *php.ini*. Entfernen Sie die Semikolons in jeder Zeile, speichern Sie die Datei und führen Sie anschließend einen Neustart des Apache-Webservers durch.

Wie Sie voranstehendem Abschnitt der *php.ini*-Datei entnehmen können, erlaubt diese neben dem Aktivieren auch die Anpassung verschiedener weiterer Einstellungen, beispielsweise auch die Aktivierung des Optimizers und der Datenkomprimierung.

Da Apache-PHP-Umgebungen bisweilen sehr unterschiedlichen Anforderungen genügen sollen, spielen Sie einfach ein wenig mit den Einstellungen, falls die Aktivierung noch keine spürbare Beschleunigung bringt.

8.2 PHP-Erweiterung PEAR

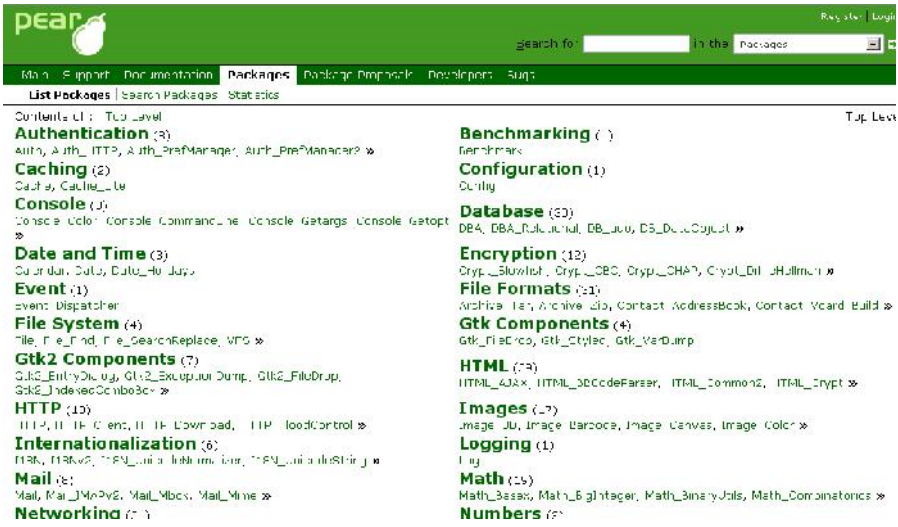
Wenn Sie die PHP-Funktionalität erweitern wollen oder eine Applikation einsetzen wollen, die eine Erweiterung verwendet, so gibt es hierfür prinzipiell zwei Techniken:

- PEAR (PHP Extension and Application Repository)
- PECL (PHP Extension Community Library)

Bei PECL handelt es sich um einen ehemaligen Teil von PEAR, der nur C-Erweiterungen anbietet. In der Regel genügt es, wenn Sie sich mit den PEAR-Fähigkeiten ein wenig vertraut machen.

PEAR ist eine Sammlung von Modulen und Erweiterungen für die Skriptsprache PHP, so wie man es auch vom CPAN-Projekt für Perl kennt.

Über die PEAR-Website können Sie sich ein Bild davon machen, wie breit die Palette der verfügbaren Erweiterungen inzwischen ist. Sie reicht von Funktionen für das Caching bis hin zu XML-relevanten Aufgaben.



Auf der PEAR-Website finden Sie fast 480 Erweiterungen für Ihre PHP-Umgebung.

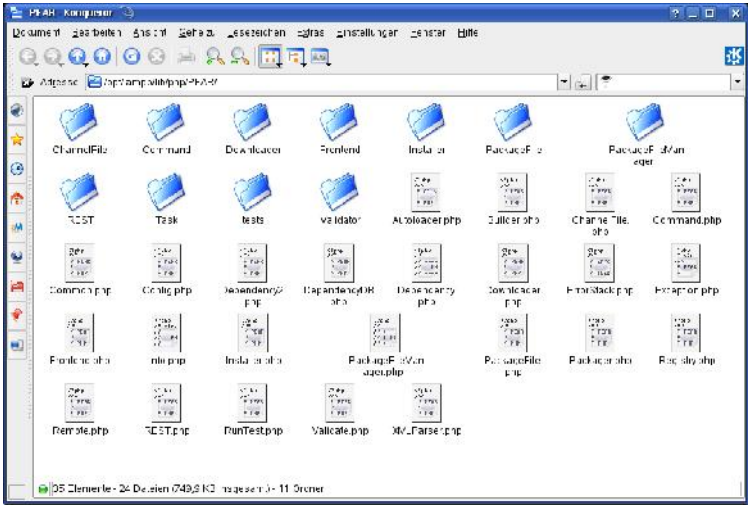
Genau genommen ist PEAR eine Bibliothek mit Skripten und Referenzimplementierungen, die Standardlösungen für Anwendungsgebiete in der Entwicklung von PHP-Applikationen bereitstellen. Sie sind gerade für Entwickler so interessant, weil sie hier eine zentrale Anlaufstelle mit freien Implementierungen finden, die sie einfach in ihre Anwendungen integrieren können.

Der Einsatz von Programmmodulen und Erweiterungen verkürzt somit den Entwicklungsprozess von PHP-Anwendungen erheblich, da sie dem Programmierer gängige Standardaufgaben abnehmen. Damit einher geht auch ein höheres Maß an Sicherheit bei der Anwendungsentwicklung, da der Entwickler auf qualitätsgesicherte Standardkomponenten zurückgreift, denn die Komponenten sind ausreichend getestet und geprüft.

Die einzelnen in PEAR enthaltenen Projekte (sie werden auch als Pakete bezeichnet) sind nach einheitlichen Standards entwickelt, werden ständig weiterentwickelt und getestet, um ein hohes Maß an Qualität sicherzustellen.

Wie bereits erwähnt, ist die Palette sehr breit gefächert. Sie reicht von Modulen zur Authentifizierung von Benutzern, für Caching, Datenbankzugriffe, Verschlüsselung, Konfiguration, HTML, Web Services, XML-RPC und XML.

Alle Projekte stehen als Open Source zur Verfügung und können mit dem PEAR-Installer (der ab PHP 4.3.0 Bestandteil einer PHP-Installation ist) sehr einfach auf dem eigenen Webserver installiert werden. PEAR stellt die Installationsmechanismen, die per Kommandozeile Pakete verwalten können (hinzufügen, erneuern, entfernen). Es lassen sich auch Abhängigkeiten in den genutzten Paketen kontrollieren. Wenn Sie selbst in die Entwicklung von PEAR-Erweiterungen einsteigen wollen, finden Sie auf der PEAR-Website eine Fülle an Informationen, wie diese zu entwickeln sind.



Ein Blick ins PEAR-Verzeichnis zeigt, dass bereits einige Erweiterungen auf Ihrem System verfügbar sind.

Sie finden alle PEAR-relevanten Dateien im Verzeichnis */opt/lampp/bin/pear*. In dieses Verzeichnis werden auch zukünftige PEAR-Module installiert. Für die Installation und den weiteren Umgang mit den Erweiterungen verwenden Sie am einfachsten die Funktionen auf der Kommandozeile.

Die Installation über die Kommandozeile ist der schnellste Weg, PEAR-Packages auf Ihrem System zu installieren. Dabei verbindet sich der PEAR-Paket-Manager mit dem PEAR-Package-Server über HTTP, lädt sich das gewünschte Paket herunter und installiert es entsprechend Ihren Einstellungen.

Die Ausführung der PEAR-Kommandos erfolgt nach folgendem Schema:

```
pear pear-Kommando
```

Um die vollautomatische Installation eines Pakets durchzuführen, verwenden Sie folgenden Befehl:

```
pear install <package>
```

Ersetzen Sie *package* durch den Namen des Pakets, das Sie installieren wollen, beispielsweise das Package *HTTP_Upload*.

Ist ein Paket als noch nicht stabil deklariert, können Sie die Installation mit der entsprechenden Status-Angabe erzwingen. Dazu ergänzen Sie den Namen des Pakets einfach mit dem Zusatz *-alpha* oder *-beta*:

```
pear install <package>-beta
```

Wenn Sie sich für die Liste aller verfügbaren Packages interessieren, führen Sie einfach folgenden Befehl aus:

```
pear remote-list
```

Dieser Befehl holt sich die Liste aller Packages, die aktuell im PEAR-Archiv verfügbar sind.

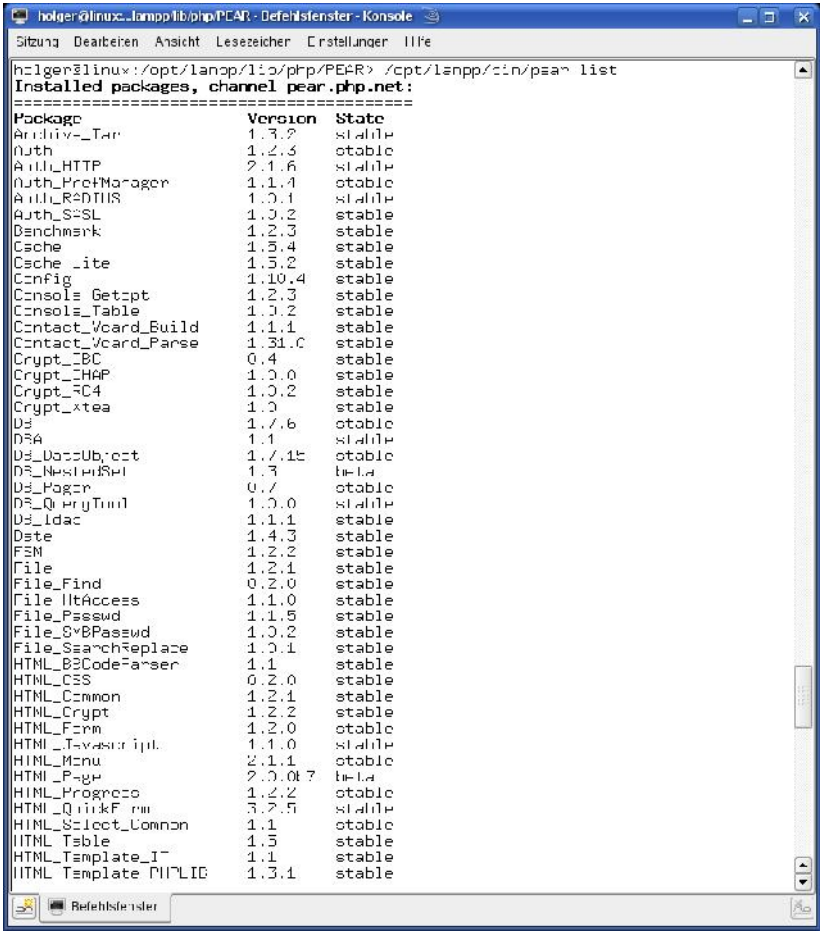
Sie können auch die halb automatische Installationsvariante verwenden. Die kommt dann zum Zuge, wenn Sie ein Paket von der PEAR-Website heruntergeladen haben und es von dem lokal gezippten Tar-Archiv installieren wollen. In diesem Fall führen Sie folgenden Befehl aus:

```
pear install <file>.tgz
```

Dieses Kommando installiert das lokale Package, ohne dass eine Online-Verbindung notwendig ist. Ersetzen Sie *<file>.tgz* durch den Namen der heruntergeladenen Datei.

Der PEAR-Paketmanager unterstützt eine Vielzahl an weiteren Befehlen. Beachten Sie, dass einige Root-Zugriff auf dem Server erfordern. Weitere wichtige Kommandos sind die folgenden:

- **build**: Erzeugt eine Erweiterung aus dessen Quellcode.
- **bundle**: Lädt und entpackt eine PECL-Erweiterung.
- **channel-add**: Fügt einen Channel der internen Channel-Liste hinzu.
- **channel-alias**: Definiert einen Aliasnamen für einen Channel.
- **channel-delete**: Entfernt einen Channel von der internen Channel-Liste.
- **channel-discover**: Initialisiert einen Channel auf Basis des Servers.
- **channel-info**: Zeigt Informationen über einen Channel an.
- **channel-update**: Erneuertt die Informationen über einen Channel in der internen Channel-Liste.
- **clear-cache**: Löscht den XML-RPC-Cache.
- **config-create**: Erzeugt eine PEAR-Konfigurationsdatei.
- **config-get**: Zeigt eine bestimmte Konfigurationseinstellung an.
- **config-help**: Zeigt Informationen zur Konfiguration an.
- **config-set**: Setzt eine bestimmte Konfigurationseinstellung.
- **config-show**: Zeigt alle Konfigurationseinstellungen an.
- **convert**: Konvertiert eine package.xml-Datei der Version 1.0 in das Format für Version 2.0. Wichtig für Paket-Entwickler.
- **cvsdiff**: Führt ein *cvs diff -u* über alle Dateien eines Packages aus und zeigt das Resultat an.
- **cvstag**: Setzt ein CVS-Release-Tag.
- **download**: Lädt ein Package herunter, installiert es aber nicht.
- **download-all**: Lädt alle verfügbaren Packages vom Package-Server.
- **info**: Zeigt Informationen über das angegebene Paket an.



Ein Beispiel für die Auflistung der Pakete mit dem Kommando */opt/lampp/bin/pear list.*

Hier ein Beispiel für das Abrufen von weiteren Informationen zur Erweiterung XML_RPC. Diese rufen Sie mit folgendem Kommando ab: *opt/lampp/bin/pear info XML_RPC*.

Die Ausgabe sieht dann wie folgt aus:

```
About XML_RPC-1.4.4
====================
Provides            Classes:
Package             XML_RPC
Summary             PHP implementation of the XML-RPC proto-
col
Description         A PEAR-ified version of Useful Inc's XML-
RPC for
PHP.
It has support for HTTP/HTTPS transport,
proxies and authentication.
Maintainers         Stig Bakken <stig@php.net> (lead)
Daniel Convissor <danielc@php.net> (lead)
Version             1.4.4
Release Date        2005-10-15
Release License     PHP License
Release State       stable
Release Notes       * Properly deal with empty values in
struct's.
Package.xml Version 1.0
Previous Installed  1.4.0
Version
Last Modified       2005-11-25
```

Die weiteren Befehle:

- **install**: Installiert ein Package und liefert eine entsprechende Erfolgsmeldung.
- **list**: Zeigt die installierten Packages an.
- **list-all**: Zeigt alle verfügbaren Packages an.
- **list-channels**: Listet die verfügbaren Channels auf.

- **list-files**: Listet die Dateien eines installierten Pakets auf.
- **list-upgrades**: Zeigt alle installierten Pakete an, für die Upgrades verfügbar sind.
- **login**: Stellt eine Verbindung mit einem PEAR-Package-Server her und authentifiziert den Nutzer am Server.
- **logout**: Loggt einen angemeldeten Nutzer an einem PEAR-Package-Server aus.
- **makerpm**: Erzeugt eine RPM-Specification-Datei von einem PEAR-Package.
- **package**: Erzeugt ein Package-Archiv.
- **package-dependencies**: Zeigt Abhängigkeiten eines Pakets an.
- **package-validate**: Prüft, ob ein Archiv konsistent und korrekt ist.
- **remote-info**: Zeigt Informationen über ein installiertes Paket einer entfernten Installation an.
- **remote-list**: Zeigt alle installierten Pakete auf einer entfernten Installation an.
- **run-scripts**: Startet die Post-Installationsskripte eines Packages.
- **run-tests**: Startet die Testskripte in einem Verzeichnis.
- **search**: Durchsucht die Package-Datenbank eines Packageservers.
- **shell-test**: Testet, ob ein Paket installiert ist.
- **sign**: Signiert ein Package-Archiv.
- **uninstall**: Deinstalliert das angegebene Paket und löscht alle installierten Dateien.
- **update-channels**: Erneuert die Informationen aller Channels in der internen Channel-Liste.
- **upgrade**: Installiert die aktuelle Version eines Packages.
- **upgrade-all**: Installiert die aktuelle Version, wenn verfügbar, für jedes installierte Package.

Wenn Sie tiefer in den Umgang mit PEAR einsteigen wollen und insbesondere wissen wollen, was die verschiedenen verfügbaren PEAR-Module leisten können, finden Sie auf der PEAR-Website entsprechende Informationen.

9 MySQL-Alternative SQLite

Wenn Sie mit XAMPP arbeiten wollen, so steht Ihnen out-of-the-box die MySQL-Datenbank zur Verfügung. Diese ist sicherlich sehr leistungsfähig, allerdings auch sehr komplex. Wenn Sie „nur“ einfache Datenbank-spezifische Aufgaben zu bewältigen haben oder einfach nur ein wenig in die Welt der Datenbank einsteigen wollen, so steht Ihnen mit SQLite eine einfache Alternative zur Verfügung.

Sie können XAMPP übrigens auch das Zusammenspiel mit anderen Datenbanken, wie dem MS SQL Server oder Oracle-Datenbanken, beibringen. Doch das ist sicherlich nur ambitionierten Anwendern vorbehalten.

SQLite bietet wichtige Datenbankfunktionen wie die folgenden:

- Nicht verschachtelte Transaktionen
- Unterabfragen (subselects)
- Sichten (views)
- Trigger
- Benutzerdefinierte Funktionen

Sie eignet sich insbesondere für den Embedded-Einsatz, da für alle wichtigen Programmiersprachen passende Datenbankschnittstellen existieren. Auch ein in der Konsole und in Shell-Skripten verwendbares, einfaches Front-end ist vorhanden. Durch die Entwicklung als Embedded lässt sich die Applikation direkt in entsprechende Anwendungen integrieren, sodass eine weitere Server-Software nicht benötigt wird. Gerade der letzte Punkt ist im Vergleich zu anderen Datenbanken von Vorteil, denn dank der Einbindung der Bibliothek wird die Applikation um Datenbankfunktionalitäten erweitert, ohne auf externe Softwarepakete angewiesen zu sein.

Ein häufig angeführtes Beispiel für den Einsatz von SQLite ist die Analyse von Logdateien. Die Datenbank liest eine Logdatei ein, zerlegt und speichert sie intern als Datensätze in einer Tabelle. Durch den SQL-Zugriff stehen Ihnen flexible Sortier- und Filtermöglichkeiten zur Auswahl.

Ein weiterer Vorteil: Die SQLite-Bibliothek ist schlank, mit nur wenigen Hundert Kilobyte sogar sehr schlank.

Doch sie unterliegt natürlich auch Einschränkungen. Werden beispielsweise Daten bearbeitet, so ist die komplette Datenbank für Schreiboperationen gesperrt. Eine weitere Einschränkung: Abgesehen von den Zugriffsberechtigungen auf das Dateisystem gibt es keine Benutzer- oder Zugriffsberechtigungen für die Datenbank.

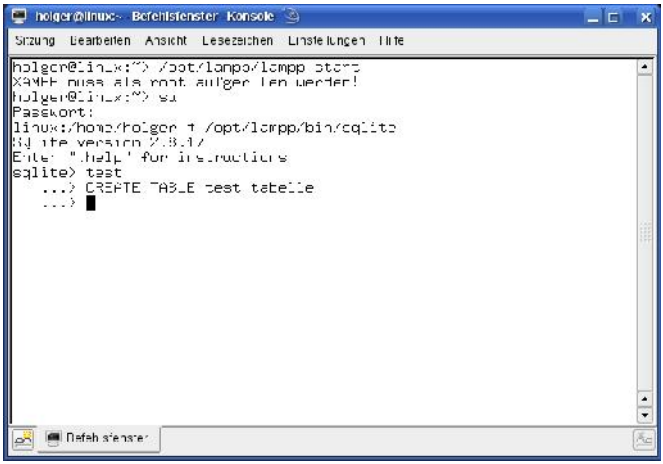
Die SQLite-Datenbank macht auch bei der Verwaltung von Websites eine gute Figur. Bei hoch frequentierten Sites und sehr umfangreichen Datensätzen sollten Sie aber doch zu MySQL greifen. SQLite kommt auch in verschiedenen Bereichen zum Einsatz, von denen man dies nicht direkt erwarten würde, so beispielsweise in Symbian OS, einem System, das auf vielen Mobiltelefonen Verwendung findet. Sie wird wohl auch in der nächsten Firefox-Version eingesetzt werden, beispielsweise zur Bookmark-Verwaltung.

9.1 SQLite in der Praxis

Schauen wir uns an, wie Sie mit der SQLite-Installation arbeiten. Um auf die Datenbank zuzugreifen, führen Sie folgenden Befehl aus:

```
/opt/lampp/bin/sqlite
```

Sie landen nach der Ausführung dieses Kommandos im SQLite-Dialog, der Ihnen die aktuelle SQLite-Version präsentiert und die Eingabe von weiteren Kommandos erlaubt.



Der Zugriff und erste Schritte mit der SQLite-Datenbank.

Um eine erste Datenbank zu erstellen, geben Sie als Nächstes einfach die gewünschte Datenbankbezeichnung ein, beispielsweise *test_db*:

```
sqlite> test_db
```

Ist die Datenbank erstellt, können Sie nun mit dem SQL-Kommando eine erste Tabelle erzeugen. Dazu verwenden Sie den Befehl *INSERT TABLE*. Ein Beispiel:

```
…> INSERT TABLE test_tabelle
```

Um die zuvor erzeugte Tabelle mit Daten zu füttern, verwenden Sie den INSERT-INTO-Befehl:

```
… > INSERT INTO test_tabelle VALUES (1, ‘Name1’, ‘Vorname1’, etc.)
… > INSERT INTO test_tabelle VALUES (2, ‘Name2’, ‘Vorname2’, etc.)
```

Nachdem Sie Ihre Tabelle mit den Daten gefüllt haben, können Sie das SQL-Kommando schließen und das Programm mit *.quit* beenden.

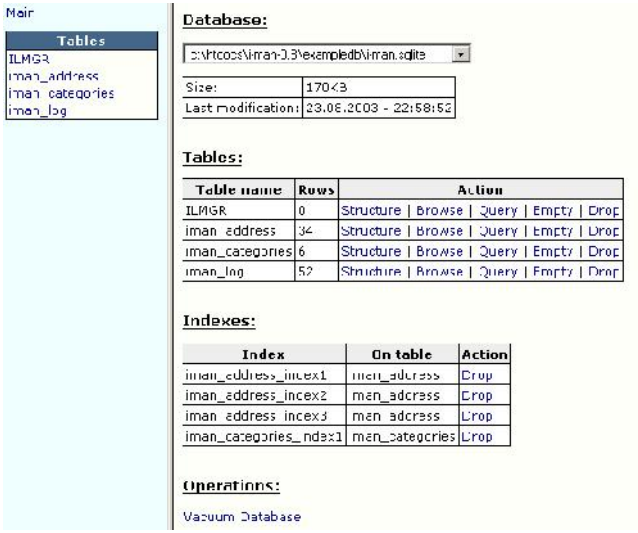
Die SQLite-Datenbank unterstützt einige weitere Kommandos. Diese sind nachfolgend zusammengefasst:

- **.databases**: Listet die Namen und Dateien der Datenbanken.
- **.dump ?TABLE?**: Zeigt die Datenbank im Textformat an.
- .**echo ON|OFF**: Schaltet Echo an bzw. aus.
- **.exit**: Beendet das Programm.
- **.explain ON|OFF**: Schaltet den Ausgabemodus passend für EXPLAIN an oder aus.
- **.header(s) ON|OFF**: Schaltet die Ansicht der Header ein oder aus.
- **.help**: Gibt die Hilfe aus.
- **.indices TABLE**: Zeigt die Namen aller Indizes einer Tabelle.
- **.mode MODE**: Bestimmt den Modus.
- **.mode insert TABLE**: Erzeugt ein Insert-Kommando für eine Tabelle.
- **.output DATEI**: Übergibt den Output an DATEI.

- **.output stdout**: Übergibt den Output an die Standardausgabe.
- **.quit**: Beendet das Programm.
- **.read DATEI**: Liest die angegebene Datei.
- **.schema ?TABLE?**: Zeigt die CREATE-Statements.
- **.show**: Zeigt die aktuellen Werte verschiedener Einstellungen.
- **.tables ?PATTERN?**: Listet die Tabellennamen, die zu dem angegebenen Muster passen.

9.2 phpSQLiteAdmin

Die Handhabung einer Datenbank auf der Konsolenebene ist sicherlich nicht jedermanns Sache. Wesentlich einfacher fallen typische Aufgaben, wenn Sie zu einem Datenbankmanager greifen. Mit phpSQLiteAdmin (*http://phpsqliteadmin.sourceforge.net*) gibt es ein mit phpMyAdmin vergleichbares Werkzeug, das die Nutzung der Datenbank vereinfacht. Unter XAMPP für Linux 1.6.x war es eine gewissen Zeit integriert. In der aktuellen Fassung ist es nicht mehr enthalten.



Mit phpSQLiteAdmin vereinfacht sich die Handhabung von SQLite deutlich.

Wenn Sie bereits ein wenig mit phpMyAdmin gespielt haben, so finden Sie sich schnell in phpSQLiteAdmin zurecht. Das Tool präsentiert Ihnen links die Navigationsleiste, rechts die dazugehörigen Funktionen und Einstellungen. Über das Auswahlmenü *Database alias* wählen Sie die gewünschte Datenbank aus, mit der Sie arbeiten wollen.

Nach der Datenbankauswahl präsentiert Ihnen das Tool eine Übersicht zur Datenbank. Sie erfahren, wie groß die Datenbank ist, wer der Besitzer und welches die Gruppe, und wann die letzten Änderungen vorgenommen wurden. Außerdem präsentiert Ihnen die Übersicht die in der Datenbank enthaltenen Tabellen. Über die *Action*-Spalte können Sie typische Aktionen wie die Ansicht aufrufen, Abfragen etc., durchführen.

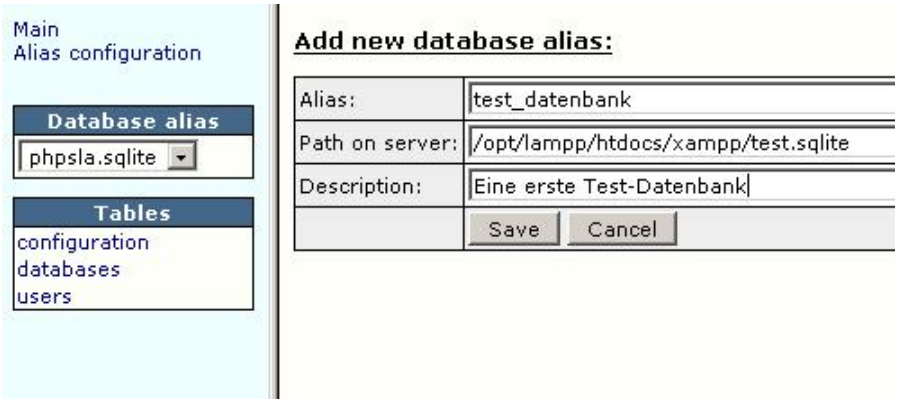
Für alle Datenbank-relevanten Aktionen ist der Bereich *Database Options* zuständig. Hier erzeugen Sie neue Tabellen und zeigen das Datenbankschema an.

Nicht auf den ersten Blick zu erkennen ist, dass Sie über den Datenbankmanager auch weitere Datenbanken erstellen können. Folgen Sie dazu dem Verweis *Alias Configuration*. Im rechten Fensterbereich werden die bereits existierenden Datenbanken samt Alias, Datenbankdatei und Beschreibung aufgeführt.

Die SQLite-Datenbanken.

Um eine neue Datenbank zu erstellen, folgen Sie dem Verweis *Add a new database alias*. Füllen Sie auf dem zugehörigen Dialog folgende Felder aus und sichern Sie die Datenbank anschließend mit einem Klick auf *Save*:

- Alias
- Path on server
- Description



Eine erste eigene SQLite-Datenbank entsteht.

Nach dem Speichern können Sie über das Auswahlmenü auf die neue Datenbank zugreifen, Tabellen erstellen etc.

9.3 Beispiel für den SQLite-Datenbankzugriff per PHP

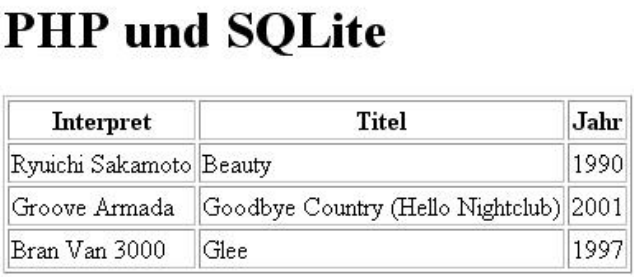
Ihre XAMPP-Installation verfügt auch über ein einfaches Beispiel, das verdeutlicht, wie Sie per PHP auf eine SQLite-Datenbank zugreifen. Sie finden die zugehörige Datei im Ordner */opt/lampp/htdocs/xampp/contrib*. Sie trägt die Bezeichnung *sqlite.php* und sieht wie folgt aus:

```
<html>
<head>
<title>PHP und SQLite</title>
</head>
<body>
<h1>PHP und SQLite</h1>
<table border="1">
<tr>
    <th>Interpret</th>
    <th>Titel</th>
```

```
    <th>Jahr</th>
</tr>
<?php
    $db = sqlite_open('../sqlite/cdcol', '0666');

    $query = "SELECT * FROM cds";
    $result = sqlite_query($db,$query);
    if ($result)
    {
        while ($row = sqlite_fetch_array($result))
        {
            echo "<tr>";
            echo "<td>".$row['interpret']."</td>";
            echo "<td>".$row['titel']."</td>";
            echo "<td>".$row['jahr']."</td>";
            echo "</tr>";
        }
    }
    else
    {
        echo sqlite_error_string(sqlite_last_error($db));
    }

?>
</table>
</body>
</html>
```

Was passiert hier nun genau? Eigentlich recht einfach. Mit der ersten Zeile des PHP-Codes erfolgt der Zugriff auf die angegebene Datenbank. Es folgt die Abfrage der Datenbank. Ist das Ergebnis positiv, wird durch die while-Schleife das Ergeb-

nis in Form einer HTML-Tabelle erzeugt. Auch die Fehlerbehandlung ist in diesem Beispiel realisiert.



PHP und SQLite

Interpret	Titel	Jahr
Ryuichi Sakamoto	Beauty	1990
Groove Armada	Goodbye Country (Hello Nightclub)	2001
Bran Van 3000	Glee	1997

Die Ausgabe des PHP-Dokuments.

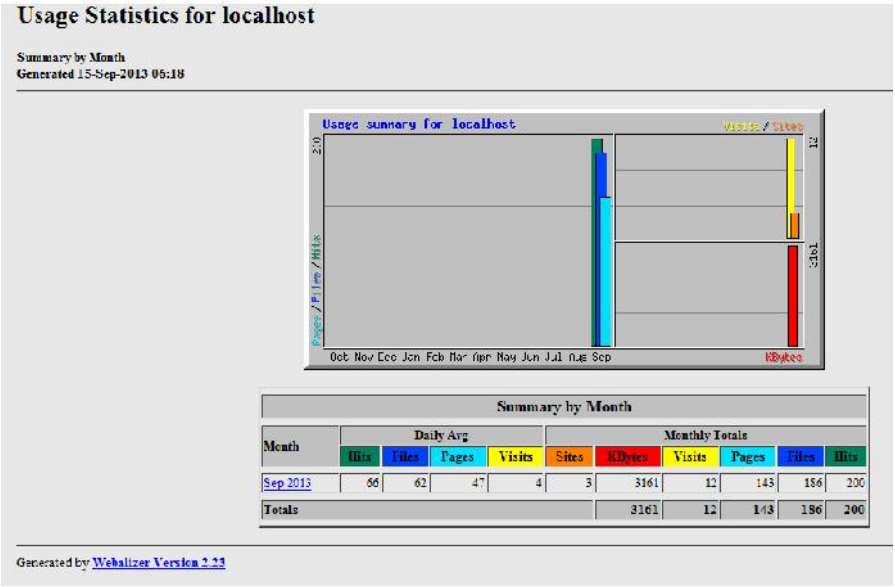
Das Ergebnis ist eine einfache Tabelle, wie sie voranstehende Abbildung zeigt. Wenn Sie weitere Erfahrungen mit SQLite und PHP sammeln wollen, bauen Sie doch dieses Beispiel einfach weiter aus. Integrieren Sie eine Suche oder ähnliche Funktionen.

10 Logfile-Analyse mit dem Webalizer

Wenn Sie XAMPP als Produktionsumgebung verwenden – sei es für interne und/oder externe Zugriffe – so sind sicherlich die Logfile-Auswertungen des Webalizers (*http://www.mrunix.net/webalizer/*) für Sie interessant. Sie verraten Ihnen, wer wann von wo auf Ihre Inhalte zugegriffen hat.

Der Logfile-Analyzer zählt, obwohl seine Weiterentwicklung längst eingestellt wurde, immer noch zu den beliebtesten Tools dieser Gattung. Die vom Webalizer generierten Statistiken enthalten üblicherweise folgende Informationen: Anfragen, Besuche, Verweise, Länder der Besucher und heruntergeladene Datenmenge. Diese Statistiken können sowohl grafisch als auch textuell betrachtet werden und sind auf unterschiedlichen Zeitskalen (Stunden, Tage, Monate, Jahre) dargestellt.

Sie greifen auf den Webalizer einfach über die XAMPP-Navigationsleiste zu. Sie finden das Werkzeug unter *Tools*.



Die Auswertung der Log-Dateien Ihrer XAMPP-für-Linux-Installation.

10.1 Webalizer-Basics

Beim ersten Zugriff auf das Analysewerkzeug können Sie am Bildschirm verfolgen, wie das Tool sich an die Auswertung der Protokolldatei macht und Ihnen anschließend die grafische Auswertung präsentiert.

Im Kopfbereich zeigt Ihnen der Webalizer an, welcher Zeitraum ausgewertet wurde und wann die letzte Auswertung erfolgt ist. Es folgt die eigentliche grafische Aufbereitung der Logfile-Informationen. Diese ist zweigeteilt:

- Oben die Zusammenfassung.
- Darunter die Zusammenfassung nach Monat.

Für die unterschiedlichen Informationen verwendet der Logfile-Analyzer auch unterschiedliche Farben, um die Daten deutlicher hervorzuheben.

Für die *Hits* verwendet das Tool standardmäßig ein dunkles Grün. Hinter dem Begriff Hit verbirgt sich schlicht und einfach eine Zeile in der Protokolldatei. Im Hintergrund passiert dabei etwa Folgendes: Wenn ein Benutzer mit seinem Browser auf Ihre XAMPP-basierte Site zugreift, schreibt der Server eine Zeile in die Protokolldatei. Der Browser stellt fest, dass er da noch ein paar Bilder, Style-Sheets etc. benötigt, damit die Seite vollständig ist. Er sendet weitere Requests an den Server, worauf dieser wieder weitere Zeilen in die Log-Datei schreibt.

Beim Aufruf einer Seite können also Dutzende Hits erzeugt werden, aber auch nur ein einziger, wenn es sich um eine simple HTML-Datei handelt.

Für die Auswertung der Files verwendet der Webalizer ein dunkles Blau. Hier erfahren Sie, wie viele Dateien vom Server an den Client übermittelt wurden. Hier wird die Gesamtanzahl der übermittelten Dateien aufgezeichnet. In der Regel liegt das Verhältnis von Hits zu Files 10 zu 9 − also etwas mehr Hits. Wie das Verhältnis im Einzelfall aussieht und wie viele Dateien übermittelt werden, ist letztlich vom Aufbau einer Seite abhängig.

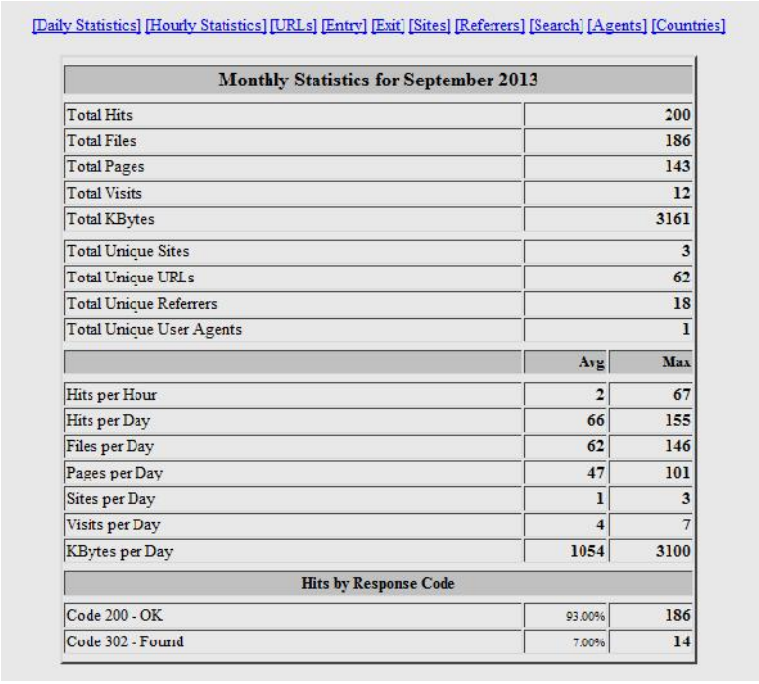
Für die Auswertung der Pages (Seiten) kommt ein helles Blau zum Einsatz. Im Unterschied zu Dateien ist eine Page etwas, was HTML enthält, also kein Bild, kein Stylesheet etc.

Besonders interessant ist das Verhältnis von Pages zu Visits. Es sollte zwischen 2 zu 1 und 5 zu 1 liegen – je mehr, desto besser. Beim Verhältnis 1:1 stolpern die Besucher mehr zufällig auf Ihre Site, schauen sich ein Dokument an und sind schon wieder weg. Wenn es Ihnen gelingt, die Besucher für ca. zehn Seiten pro Besuch zu interessieren, liegen Sie sehr gut im Rennen.

Wenn Sie auf Ihrer Site allerdings Frames verwenden, müssen Sie berücksichtigen, dass sowohl das Frameset als auch jeder einzelne Frame eine Seite ist. Wenn Sie eine Seite mit vier Frames haben, kommen Sie schon auf fünf Page-Impressions auf der Startseite.

In der Regel interessiert der Wert der Visits, also der Besuche Ihrer Site, am meisten. Besucht ein User mit seiner zugewiesenen IP-Adresse eine Seite, so wird die Zeit berechnet, die seit der letzten Anfrage vergangen ist. Ist die Zeitspanne größer als die konfigurierte visit-timeout-Zeit von standardmäßigen 30 Minuten oder wurde von diesem Besucher noch nie eine Anfrage gemacht, wird die Anfrage als neuer Visit vermerkt und die Zahl der Visits erhöht.

Zwar ist dieser Wert ein wenig trügerisch, weil natürlich kein Logfile-Analyzer wirklich wissen kann, wie viele Besucher man auf seiner Site begrüßen durfte, doch sind die erreichten „Schätzungen“ recht gut.



[Daily Statistics] [Hourly Statistics] [URLs] [Entry] [Exit] [Sites] [Referrers] [Search] [Agents] [Countries]

Monthly Statistics for September 2013		
Total Hits		200
Total Files		186
Total Pages		143
Total Visits		12
Total KBytes		3161
Total Unique Sites		3
Total Unique URLs		62
Total Unique Referrers		18
Total Unique User Agents		1
	Avg	Max
Hits per Hour	2	67
Hits per Day	66	155
Files per Day	62	146
Pages per Day	47	101
Sites per Day	1	3
Visits per Day	4	7
KBytes per Day	1054	3100
Hits by Response Code		
Code 200 - OK	93.00%	186
Code 302 - Found	7.00%	14

Die Details eines Monats.

Ein weiterer interessanter Wert: die Sites. Hier erfahren Sie, wie viele unterschiedliche IP-Adressen im Analysezeitraum auf Ihre Site zugegriffen haben. Schließlich präsentiert Ihnen der Webalizer in der KBytes-Spalte die Datenmenge, die der Server im Analysezeitraum gesendet hat. Diese Angaben sind allerdings recht ungenau. Weitaus interessanter ist meist der zeitliche Verlauf, gerade auch in Bezug zu den Pages.

Wenn Sie sich neben dem Überblick für weitere Details interessieren, so folgen Sie in der Tabelle *Summary by Month* dem jeweiligen Monats-Link. In der Detailansicht können Sie sich dann die täglichen und stündlichen Zugriffe sowie eine Vielzahl weiterer Details ansehen.

10.2 Webalizer-Konfiguration

Wenn Ihnen die Standardkonfiguration des Webalizers nicht zusagt, passen Sie einfach die Konfigurationsdatei *webalizer.conf* an. Sie finden die Datei unter Linux im Verzeichnis */opt/lampp/etc*. Die Konfigurationsdatei ist nach folgendem Schema aufgebaut:

```
Option Wert
```

Hier ein Beispiel für eine Webalizer-Konfigurationsdatei – inklusive der notwendigen Erläuterungen:

```
#
# Beispiel für eine Webalizer-Konfigurationsdatei.
#
# Bestimmt die Log-Datei.
LogFile        /opt/lampp/logs/access_log
#
# Bestimmt den Logfile-Typ.
LogType      clf
#
# Ausgabeverzeichnis:
OutputDir      /opt/lampp/htdocs/webalizer
#
# Hier geben Sie die Datei der historischen Daten an.
```

```
HistoryName  webalizer.hist
#
# Aktiviert die inkrementelle Analyse.
Incremental  no
#
# Legt die Datei fest, in der die inkrementellen Daten ge-
speichert werden.
IncrementalName    webalizer.current
#
# Bestimmt den Titel des Berichts.
ReportTitle    Usage Statistics for
#
# Bestimmt den Hostname.
HostName       localhost
#
# Bestimmt die Dateierweiterung des Berichts.
HTMLExtension  html
#
# Legt fest, welche Dateien als Seiten eingestuft werden.
PageType     htm*
PageType     cgi
PageType     phtml
PageType     php3
PageType     pl
#
# Aktiviert die HTTPS-Unterstützung
UseHTTPS       no
#
# Bestimmt die DNS-Cache-Datei für Revers-DNS-Lookups.
#DNSCache    dns_cache.db
#
```

```
# Akiviert DNS-Kindprozesse.

DNSChildren  0

#

# Bestimmt den vordefinierten HTML-Code für die Berichte.

HTMLPre <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transi-
tional//EN">

#

# Bestimmt den HTML-Code, der zwischen das HEAD-Tag nach der
Title-Zeile eingefügt wird.

HTMLHead <META NAME="author" CONTENT="The Webalizer">

#

# Bestimmt die Eigenschaften des HTML-Bodys:

HTMLBody <BODY BGCOLOR="#E8E8E8" TEXT="#000000"
LINK="#0000FF" VLINK="#FF0000">

#

# Bestimmt den HTML-Code, der vor der ersten horizontalen
Linie eingeführt wird.

HTMLPost     <BR CLEAR="all">

#

# Bestimmt den HTML-Code am Fuße des Berichts.

HTMLTail <IMG SRC="msfree.png" ALT="100% Micro$oft free!">

#

# Bestimmt den HTML-Code, der am Ende jeder erzeugten Datei
eingefügt wird.

HTMLEnd </BODY></HTML>

#

# Unterdrückt mit der Option yes (störende) Ausgabemeldungen.

Quiet        no

#

# Unterdrückt mit der Option yes Fehlermeldungen und Warnun-
gen.

ReallyQuiet  no

#
```

```
# Erlaubt die Einblendung von Timing-Informationen.
TimeMe       no
#
# Zeigt die GMT-Zeit an.
GMTTime            no
#
# Zeigt Debug-Meldungen.
Debug        no
#
# Ignoriert Verarbeitungsfehler.
FoldSeqErr   no
#
# Bestimmt die Dauer einer Session (30 Minuten).
VisitTimeout 1800
#
# Zeigt die Herkunftsländer in der grafischen Auswertung an.
CountryGraph yes
#
# Aktiviert die täglichen Grafiken und Auswertungen.
DailyGraph   yes
DailyStats   yes
#
# Aktiviert die stündlichen Grafiken und Statistiken:
HourlyGraph  yes
HourlyStats  yes
#
#  Aktiviert die Legende der grafischen Auswertungen:
GraphLegend  yes
#
# Über die Top-Optionen lässt sich steuern, wie viele Einträ-
ge der Webalizer in den jeweiligen Statistiken listet. Die
```

```
Angabe ist nur optional und primär dann sinnvoll, wenn die
Anzahl der Einträge in der Standardeinstellung zu gering ist
(Beispiel: TopSearch 30).

TopSites        30

TopKSites       10

TopURLs         30

TopKURLs        10

TopReferrers    30

TopAgents       15

TopCountries    30

TopEntry        10

TopExit         10

TopSearch       20

TopUsers        20

#

# Zeigt alle Informationen zu den Sites, URLs etc. an:

AllSites     no

AllURLs      no

AllReferrers no

AllAgents    no

AllSearchStr no

AllUsers       no

#

#Bestimmt den Index-Alias.

IndexAlias     home.htm

IndexAlias   homepage.htm

#

# Mit den Hide-Optionen verstecken Sie spezifische Informa-
tionen, damit sie nicht ausgewertet werden und im Bericht
auftauchen. Mit der Option Hide Agent können Sie gezielt An-
wenderprogramme aus der Liste der häufigsten Anwendungsprog-
ramme ausschließen, z. B. HideAgent RealPlayer.
```

```
# Mit der Option HideReferrer lassen sich aus der Liste der
externen Verweise Seiten ausblenden. Dies ist beispielsweise
dann praktisch, wenn mehrere Domains auf eine Seite weisen
und eigentlich interne Verweise zwischen den Domains als Ver-
weise gezählt werden.

# Die Option HideSite erlaubt es Ihnen, Hostnamen bzw. IP-
Adressen von der Liste der Top-Rechner auszuschließen.

# Mit der Option HideURL können Dateitypen von der Liste der
Top-URLs ausgeschlossen werden. Dies kann beispielsweise ge-
nutzt werden, um zu verhindern, dass Bilder, CSS-Dateien und
ähnliche Dateien in der Liste der Top-URLs auftauchen.

# Über die Option HideUser lassen sich gezielt Benutzer von
passwortgeschützten Bereichen aus der Liste der Benutzer aus-
blenden. Ein Beispiel: HideUser admin.

HideSite     localhost

HideReferrer interest.de

HideReferrer Direct Request

HideURL             *.gif

HideURL             *.GIF

HideURL             *.jpg

HideURL             *.JPG

HideURL             *.png

HideURL             *.PNG

HideURL             *.ra

HideAgent    RealPlayer

HideUser     root

HideUser     admin

#

# Verschiedene Gruppierungsoptionen:

GroupURL     /cgi-bin/*   CGI Scripts

GroupURL     /images/*    Images

GroupSite    *.aol.com

GroupSite    *.compuserve.com

GroupReferreryahoo.com/   Yahoo!
```

```
GroupReferrerexcite.com/     Excite
GroupReferrerinfoseek.com/   InfoSeek
GroupReferrerwebcrawler.com/ WebCrawler
GroupUser      root            Admin users
GroupUser      admin           Admin users
GroupUser      wheel           Admin users
#
# Liefert einen Überblick über die verwendeten Browser:
GroupAgent   MSIE
HideAgent    MSIE
GroupAgent   Mozilla
HideAgent    Mozilla
GroupAgent   Lynx*
HideAgent    Lynx*
#
# Erlaubt das Verstecken einzelner Sites im Bericht:
HideAllSites no
#
# Erlaubt das Gruppieren von einzelnen Hosts zu einer zugehö-
rigen Gruppe:
#GroupDomains0
#
# Hebt den Gruppennamen fett hervor:
GroupHighlight      yes
#
# Ignoriert folgende Informationen in der Logdatei:
IgnoreSite   bad.site.net
IgnoreURL    /test*
IgnoreReferrer      file:/*
IgnoreAgent  RealPlayer
IgnoreUser     root
```

```
#
# Schließt bestimmte User explizit ein:
#IncludeUser    someuser
#
# Über Option SearchEngine bestimmen Sie die Seiten, die als
Suchmaschine gewertet werden und in die Analyse der Suchbe-
griffe eingehen. In der Standardkonfiguration sind lediglich
amerikanische Suchmaschinen definiert, sodass es für eine
deutsche Seite immer Sinn macht, die Definitionen für diese
Option zu erweitern. Neben dem Domainnamen der Suchmaschine
muss außerdem angegeben werden, über welchen Parameter die
Suchmaschine die Suchbegriffe entgegennimmt.
#
SearchEngine yahoo.com    p=
SearchEngine altavista.comq=
SearchEngine google.com   q=
SearchEngine eureka.com   q=
SearchEngine lycos.com    query=
SearchEngine hotbot.com   MT=
SearchEngine msn.com            MT=
SearchEngine infoseek.com qt=
SearchEngine webcrawler   searchText=
SearchEngine excite       search=
SearchEngine netscape.com search=
SearchEngine mamma.com    query=
SearchEngine alltheweb.comquery=
SearchEngine northernlight.com  qr=
#
# Verschiedene Dump-Optionen erlauben das Anzeigen von Site,
URLs, Referrer etc.
DumpPath     /var/lib/httpd/logs
DumpHeader   no
DumpExtensiontab
```

```
DumpSites    no
DumpURLs     no
DumpReferrersno
DumpAgents   no
DumpUsers    no
DumpSearchStr  no
#
# Ende der Konfiguration.
```

In der Regel will man die Berichtausgabe anpassen. Daher beschränken sich die meisten Anpassungen auch auf diesen Bereich.

11 Mehr Sicherheit für Ihre XAMPP-Installation

XAMPP ist ein komplexes Gebilde, das immer häufiger die Grundlage für den Betrieb unternehmenskritischer Applikationen bildet. Gerade bei kritischen Systemen stellt sich immer auch die Frage, wie sicher ist die Umgebung, welche Sicherheitsrisiken lauern und wie man sich schützt? Die zentralen Fragen beim Einsatz eines solchen Systems sind:

- Gibt es vordefinierte Gruppen innerhalb eines Rollenkonzepts?
- Kann der Zugriff mittels Benutzer- und Gruppenverwaltung entsprechend den Anforderungen gesteuert werden?
- Gibt es Schutzmechanismen?
- Kann die Kommunikation zwischen dem System und den Clients verschlüsselt werden?
- Und wie wird das System technisch vor Fremdzugriffen geschützt?

Bei einem System, das so komplex ist wie XAMPP, muss man das sicherheitstechnische Augenmerk weit fassen. Zu berücksichtigen sind Fragen der Apache-, Datenbank- und PHP-Sicherheit. Natürlich spielen auch hier die Datensicherheit und die Sicherung eine wichtige Rolle.

Im Hinterkopf sollte man immer behalten, dass eine Vielzahl an Risiken den Betrieb eines XAMPP-Systems gefährden kann. Neben den „Standardrisiken“ sollte man sich beispielsweise auch mit Cross-Site-Scripting und SQL-Injektion auseinandersetzen. Beim Entwurf einer Sicherheitsstrategie ist auch zu berücksichtigen, ob es sich um eine Intranet- oder Extranet-Site handelt – oder beides.

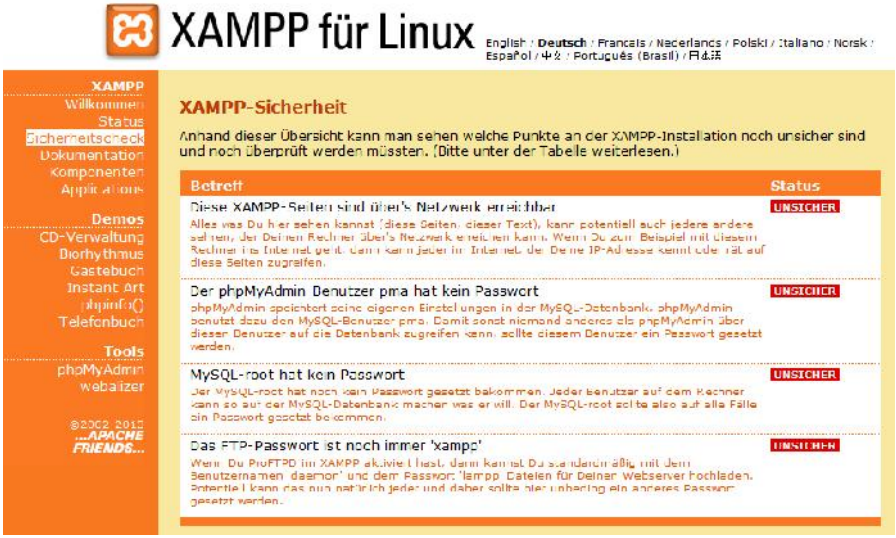
11.1 Standardsicherheit

XAMPP – und zwar sowohl die Windows- als auch die Linux-Variante – verfügt über Sicherheitsskripts, die helfen, die Grundkonfiguration der Umgebung sicherer zu machen. Diese sollten Sie immer dann ausführen, wenn Ihre XAMPP-Installation mehr als Spielwiese für das Testen von XAMPP und darauf aufsetzenden Applikationen dient.

11.1.1 Mehr Sicherheit für XAMPP für Linux

Wenn Sie mit XAMPP für Linux arbeiten, so sollten Sie sich nach der Inbetriebnahme des Systems als Nächstes um die Sicherheit der XAMPP-Installation kümmern. Von Haus aus ist XAMPP nicht für den Produktionseinsatz gedacht, sondern in erster Linie als Entwicklungsumgebung. Daher sind die Sicherheitseinstellungen längst nicht so restriktiv, wie sie es bei einem Produktionseinsatz sein sollten. Die Grundkonfiguration weist folgende Sicherheitsschwachstellen auf, die es im nächsten Schritt zu schließen sind:

- Die XAMPP-Seiten snd über das Netzwerk erreichbar.
- Der phpMyAdmin-Benutzer pma hat kein Passwort.
- Der MySQL-root besitzt kein Passwort.
- Der ProFTPD-Daemon benutzt das Passwort *xampp*.



Der Sicherheitscheck offenbart es: Ihre XAMPP-Installation ist extrem unsicher. Höchste Zeit, das zu ändern.

Über die XAMPP-Startseite können Sie den Sicherheitscheck starten, der Ihnen bei einer Neuinstallation genau diese Schwachstellen aufführt.

Ihre XAMPP-Installation verfügt über ein kleines Skript, mit dem Sie diese Einstellungen ändern können. Sie rufen es mit folgendem Befehl auf:

```
/opt/lampp/lampp security
```

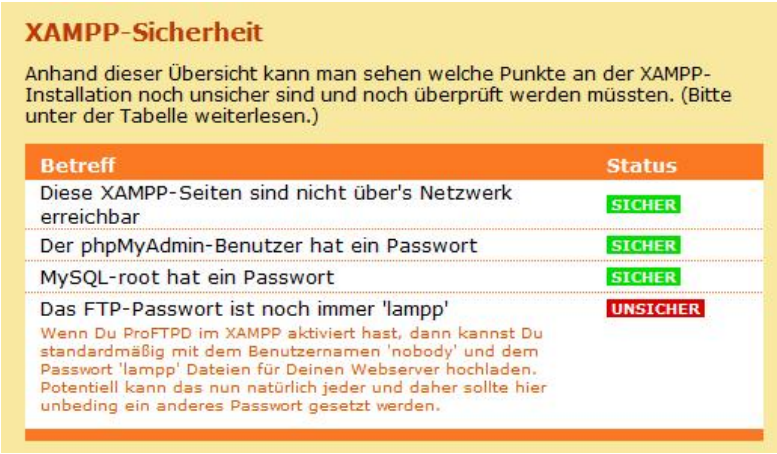
Wenn Sie XAMPP auf einem Windows-System ausführen, können Sie die Einstellungen auch über die Web-Schnittstelle ändern. Dazu im nächsten Abschnitt mehr.

Das Skript führt Sie interaktiv durch die verschiedenen Schritte, die für die Änderungen der Passwörter erforderlich sind. Der typische Ablauf sieht wie folgt aus:

```
XAMPP: Schneller Sicherheits-Check...

XAMPP: Die LAMPP-Seiten sind NICHT mit einem Paßwort geschützt.

XAMPP: Möchtest Du ein Passwort setzen? [ja] ja (1)

XAMPP: Paßwort: ******

XAMPP: Paßwort (Wiederholung): ******

XAMPP: MySQL ist über's Netzwerk erreichbar.

XAMPP: Normalerw. wird dies nicht benötigt. Soll ichs abschalten? [ja] ja

XAMPP: Abgeschaltet!

XAMPP: Der MySQL/phpMyAdmin-Benutzer pma hat kein Passwort gesetzt!!!

XAMPP: Möchtest Du ein Paßwort setzten? [ja] ja

XAMPP: Paßwort: ******

XAMPP: Paßwort (Wiederholung): ******

XAMPP: MySQL pma-Paßwort wird gändert.

XAMPP: Passe pma-Paßwort-Einstellungen im phpMyAdmin an.

XAMPP: MySQL hat kein root-Paßwort gesetzt!!!

XAMPP: Möchtest Du ein Paßwort setzen? [ja] ja

XAMPP: Schreib Dir das Paßwort unbedingt auf!!!

XAMPP: Paßwort: ******

XAMPP: Paßwort (Wiederholung): ******

XAMPP: MySQL root-Paßwort wird gändert.

XAMPP: Passe root-Paßwort-Einstellungen im phpMyAdmin an.
```

```
XAMPP: Das FTP-Passwort ist noch auf 'lampp' gestellt.
XAMPP: Möchtest Du das Paßwort ändern? [ja] ja
XAMPP: Paßwort: ******
XAMPP: Paßwort (Wiederholung): ******
XAMPP: Fertig.
```

Mit der Ausführung des Skripts haben Sie Ihre XAMPP-Installation gegen die wichtigsten Angriffsoptionen abgesichert. Führen Sie anschließend einen erneuten Sicherheitscheck durch, um sicherzustellen, dass nun auch alle Einstellungen abgesichert sind.

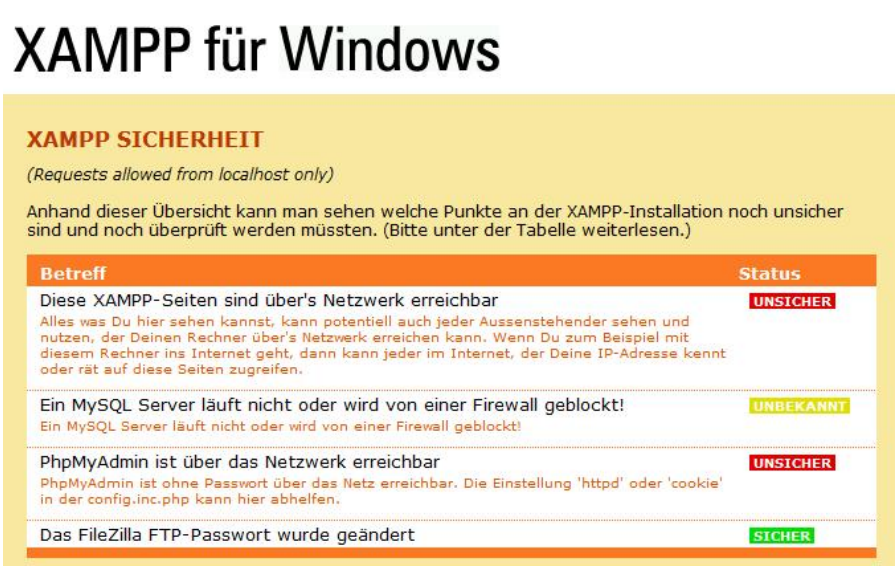


Nach der Ausführung des Sicherheitsskripts und einem erneuten Sicherheitscheck sind einige Schwachstellen geschlossen, aber längst noch nicht alle.

Es versteht sich von selbst, dass Sie beim Produktivitätstest alle Sicherheitslücken schließen sollten, die der Test ausgibt.

11.1.2 Mehr Sicherheit für XAMPP für Windows

Auch die Windows-Variante verfügt inzwischen über einen Sicherheitscheck und ein PHP-Formular, über das man die Einstellungen prüfen bzw. ändern kann. Folgen Sie in der Navigationsleiste dem Verweis *Sicherheitscheck*.



Auch der XAMPP-für-Windows-Sicherheitscheck zeigt, dass das System löchrig wie ein Schweizer Käse ist.

Je nach Umgebung weist die Prüfung Sie auf folgende Schwachstellen hin:

- Diese XAMPP-Seiten sind über das Netzwerk erreichbar.
- MySQL Admin User *root* hat kein Passwort.
- PhpMyAdmin ist über das Netzwerk erreichbar.
- Das FileZilla FTP-Passwort ist noch immer *wampp*.
- PHP läuft NICHT im *Safe Mode.*
- Ein POP3 Server wie Mercury Mail läuft nicht oder wird von einer Firewall geblockt!

Auch bei diesem Check kommen die drei farbigen Markierungen rot, gelb und grün zur Kennzeichnung des Sicherheitsstatus zum Einsatz.

Unterhalb der Ergebnisse finden Sie den Verweis zum Sicherheitsskript, mit dem Sie einige dieser Schwachstellen beheben können. Folgen Sie dem Link

http://localhost/security/xamppsecurity.php. Das funktioniert allerdings nur beim Zugriff über *localhost*. Ein Zugriff von Drittsystemen ist nicht möglich.

Wenn Sie dem Link folgen, landen Sie auf einem einfachen Formular, auf dem Sie MySQL ein neues Passwort für den Root-User verpassen und den XAMPP-Verzeichnisschutz aktivieren können.

Hier optimieren Sie die XAMPP-für-Windows-Sicherheit.

Geben Sie unter *MySQL SEKTION: ROOT PASSWORT* das neue Passwort ein, wiederholen Sie die Eingabe und übernehmen Sie die Änderung mit einem Klick auf *Passwort ändern*. Im unteren Bereich sollten Sie außerdem über die *.htaccess* den Verzeichnisschutz aktivieren.

Beachten Sie außerdem, dass Sie die beiden Server FileZilla und Mercury nicht über diese Funktion sicherer machen können. Hier helfen nur die Funktionen des jeweiligen Servers.

11.2 Sicherheitsrisiken

Neben den unsicheren Grundeinstellungen ist ein XAMPP-System durch vielerlei Techniken angreifbar. Dazu gehören beispielsweise die Ausnutzung von unsicheren Webserver-, PHP- oder Datenbankkonfigurationen. Natürlich lassen sich auch unsichere Verbindungen nutzen. Aber auch Techniken wie Cross-Site-Scripting oder SQL-Injektion bereiten Probleme.

11.2.1 Cross-Site-Scripting

Beim sogenannten Cross-Site-Scripting werden Sicherheitslücken im Browser ausgenutzt, um Benutzereingaben zu manipulieren, die an eine Web-Anwendung übergeben werden. Ein Angreifer kann dadurch dann unter anderem schädlichen Programmcode in eine für den Benutzer normalerweise korrekte Umgebung einbetten. Der Angreifer kann auch versuchen, eine gewisse Kontrolle über die Ausführung der Web-Anwendung zu erlangen. Ziel dieser Attacke sind meist das Ausspähen und die Manipulation von Benutzerdaten, wie beispielsweise Passwörtern, oder einfach das Ausführen von beliebigem Programmcode.

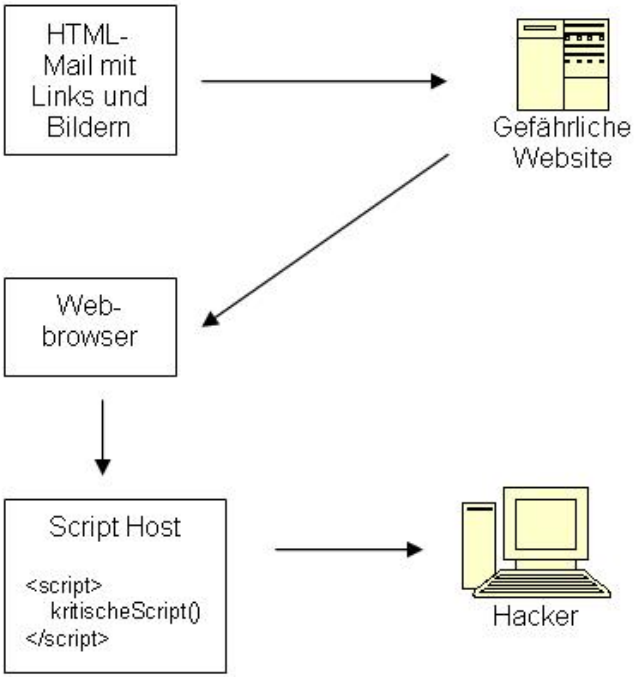
Bislang gibt es leider keine einheitliche Definition für diese Angriffstechnik. Dennoch ist den unterschiedlichen Definitionen das Angriffsszenario gemein, wonach versucht wird, schädlichen Programmcode in eine Web-Anwendung einzubetten, der dann auf der Client-Seite ausgeführt wird.

Verwandte Szenarien versuchen, den Programmablauf auf der Server-Seite zu beeinflussen. Sicherheitslücken können beispielsweise genutzt werden, um den Server zu veranlassen, fremden Programmcode zu laden und auszuführen. Benutzt die Web-Anwendung eine Datenbank, wie es bei Joomla! der Fall ist, so kann durch Manipulation der SQL-Befehle versucht werden, Einträge in der Datenbank zu verändern oder Abfrageergebnisse zu fälschen.

Was passiert nun bei solchen Vorgängen genau? Web-Anwendungen, die beispielsweise PHP nutzen, dienen in der Regel dazu, Inhalte dynamisch zu publizieren. Dabei werden die Benutzereingaben oft in den GET-Parametern der URL codiert. Werden diese Parameter nun ohne eine vorherige Prüfung im Programm weiterverarbeitet, so kann man in diesen Parametern einen Programmcode unterbringen, der dann in der erzeugten Webseite auftaucht. Meist kommt hierfür JavaScript zum Einsatz, da dieses in den meisten Browsern aktiviert ist. Theoretisch könnte man auch den Programmcode in anderen Programmiersprachen einschleusen.

Wird nun der Inhalt einer Variablen, die über einen GET-Parameter an das Skript übergeben wurde, ungefiltert ausgegeben, so landet der darin eingebettete Java-

Script-Code in der Webseite und wird vom Browser ausgeführt. Da das lokal ausgeführte JavaScript Zugriff auf die vom Browser verwalteten Cookies hat, kann der Inhalt der Cookies ausgelesen und beispielsweise an eine andere Webseite geschickt werden.



Cross-Site-Scripting stellt ein erhebliches Problem für User dar.

Häufig verwenden Web-Anwendungen zum Speichern der Authentifikationsdaten solche Cookies, sodass ein Angreifer sich damit Zugang zu einer fremden Identität erschleichen kann. Er muss sein Opfer nur dazu bringen, auf die speziell präparierte URL zu klicken. Diese URLs können aber auch in Image-Tags untergebracht werden, wo sie dann automatisch beim Laden der Webseite ausgeführt werden. Beliebte Cross-Site-Scripting-Ziele sind Foren, Gästebücher, Suchformulare, Webmailer und sogar dynamisch generierte Fehler-404-Seiten.

Schützen kann man sich indes recht einfach. Eine wichtige Schutzmaßnahme ist die Überprüfung sämtlicher Benutzereingaben. Das schließt neben den HTTP-GET- und -POST-Variablen auch die Cookies ein, die ja auch vom Client an den Server übermittelt werden. Bei der Überprüfung sollten alle nicht akzeptablen Werte, die nicht innerhalb eines fest definierten Wertebereichs liegen, herausgefiltert werden. Sonderzeichen, die vom Browser besonders interpretiert werden (wie etwa die spitzen Klammern < und >), müssen vor der Ausgabe in ihre HTML-Entities konvertiert werden. Diese Schutzmaßnahmen sind einfach zu implementieren, allerdings auch mit einem gewissen zeitlichen Aufwand verbunden.

Obige Abbildung zeigt ein typisches Szenario beim Cross-Site-Scripting. Im ersten Schritt erhält ein Benutzer eine HTML-Mail, die beispielsweise Links und/oder Grafiken enthält. Der ahnungslose User klickt auf einen Verweis und wird zu einer gefährlichen Website geführt. Diese sendet bösartigen Code an den Anwender zurück. Nun führt das Skript auf dem Host-Rechner die gewünschten Aktionen aus und sendet beispielsweise ausgespähte Daten an den Hacker.

11.2.2 SQL-Injektion

Ein weiteres Problem sind die sogenannten SQL-Injektionen. Bei dieser Technik versucht der Angreifer, SQL-Abfragen zu manipulieren. Hierzu wird über die Applikation, die den Zugriff auf die Datenbank bereitstellt, versucht, SQL-Statements einzufügen.

Man findet SQL-Injektionen oft bei CGI-Scripts. Aber auch Programme, die andere Daten, etwa Webseiteninhalte oder E-Mails, in SQL-Datenbanken eintragen, sind anfällig für diese Technik. Konkret wird versucht, weitere SQL-Anforderungen einzuschleusen oder die Abfragen so zu manipulieren, dass man zusätzliche Daten erhält. Manche Datenbanksysteme bieten auch die Möglichkeit, Zugriff auf eine Shell zu erhalten, womit der ganze Server kompromittierbar wird.

11.2.3 Angriff auf CGI

Auch die CGI-Funktionen sind mögliche Angriffsziele. Man kann PHP als CGI nutzen, wenn kein Modul in die Serversoftware eingebunden werden soll. Sinn macht es auch bei Systemen, bei denen verschiedene CGI-Wrapper genutzt werden sollen, um sichere chroot- und setuid-Umgebungen für Skripts zu schaffen.

In solchen Konfigurationen wird das ausführbare PHP-Binary meist im Cgi-bin-Verzeichnis des Webservers installiert. Problematisch ist dabei die Platzierung von

Interpretern im CGI-BIN-Verzeichnis. Obwohl das PHP-Binary als eigenständiger Interpreter verwendet werden kann, wurde PHP so entwickelt, um dem durch diese Konfiguration möglich werdenden Angriff vorzubeugen:

- **Zugriff auf Systemdateien (*http://www.server.de/cgi-bin/php?/etc/passwd*):** Bei Requests, bei denen auf ein Fragezeichen eine Abfrageinformation erfolgt, wird durch das CGI-Interface als Kommandozeilenargument an den Interpreter übergeben. In der Kommandozeile wird üblicherweise die im ersten Argument angegebene Datei von Interpretern geöffnet und ausgeführt. Beim Aufruf als CGI-Binary verweigert PHP die Interpretation der Kommandozeilenargumente.

- **Zugriff auf beliebige Web-Dokumente auf dem Server (*http://www.server.de/cgi-bin/php/gemein/doc.html*):** Der Teil der URLs nach der Angabe der PHP-Binärdatei wird meist dazu genutzt, um den Namen der Datei zu übergeben, die durch das CGI-Programm geöffnet und interpretiert werden soll. Normalerweise werden einige Einträge in der Konfigurationsdatei des Webservers benutzt (Apache: Action), um Aufrufe von Dokumenten an den PHP-Interpreter umzuleiten. Unglücklicherweise wird, wenn der Aufruf bereits in dieser Form geschieht, vom Webserver keine Zugriffsüberprüfung der Datei */secret/script.php*, sondern lediglich der Datei */cgi-bin/php* vorgenommen. So ist jeder Benutzer, der auf */cgi-bin/php* zugreifen darf, in der Lage, sich zu jedem geschützten Dokument auf dem Webserver Zugriff zu verschaffen.

- Bei PHP können die Konfigurationsoption *--enable-force-cgi-redirect* und zur Laufzeit die Konfigurationsdirektiven *doc_root* und *user_dir* verwendet werden, um diesen Angriff zu verhindern.

11.2.4 Apache-Einstellungen

Auch die Konfiguration des Apache-Webservers hat großen Einfluss auf die Sicherheit der Umgebung. Dabei wird häufig der Fehler gemacht, dem Apache Root-Rechte zu erteilen. Problematisch ist außerdem das Ausweiten der Möglichkeiten von Apache. Insbesondere die Ausweitung der Benutzerrechte für Apache auf Root ist äußerst problematisch, denn das gesamte System kann in Mitleidenschaft gezogen werden. Doch auch hierfür gibt es recht einfache Lösungen.

Mit *open_basedir()* kann man beispielsweise kontrollieren, welche Verzeichnisse PHP verwenden dürfen und welche nicht. Man kann auch Bereiche nur für Apache einrichten, um alle webbasierten Aktivitäten auf Nicht-Benutzer- bzw. Nicht-System-Dateien einzuschränken. Dazu sollte man alle .htaccess-Dateien um folgenden Code erweitern:

```
<Files .htaccess>
Order allow,deny
Deny from all
<Files>
```

Natürlich sollte auch die Datei *.htaccess* geschützt werden. Diesen Schutz können Sie wie folgt implementieren:

```
chmod 655 .htaccess
```

11.2.5 Dateisystem-Sicherheit

Bei Umgebungen wie Joomla!, die insbesondere auf PHP basieren, sind die implementierten Sicherheitseinstellungen hinsichtlich der Berechtigungen auf Datei- und Verzeichnisebene abhängig. Daraus folgt, dass man mit entsprechenden Dateisystem-spezifischen Sicherheitseinstellungen steuern kann, welche Dateien in dem Dateisystem gelesen werden dürfen. Vorsicht ist bei lesbaren Dateien geboten, um sicherzustellen, dass diese sicher von allen Usern mit Zugriff auf dieses Dateisystem (nur) gelesen werden können.

Eine Eigenschaft von PHP ist es, Zugriffe auf das Dateisystem auf Benutzerebene zu erlauben. Damit ist es natürlich auch möglich, ein PHP-Skript zu schreiben, das beispielsweise Systemdateien wie */etc/passwd* lesen, Ethernet-Verbindungen modifizieren oder auch Druckaufträge senden kann. Der Administrator muss sich also auch um diese Einstellungen kümmern und dafür sorgen, dass die zu lesenden bzw. zu schreibenden Dateien auch die Richtigen sind.

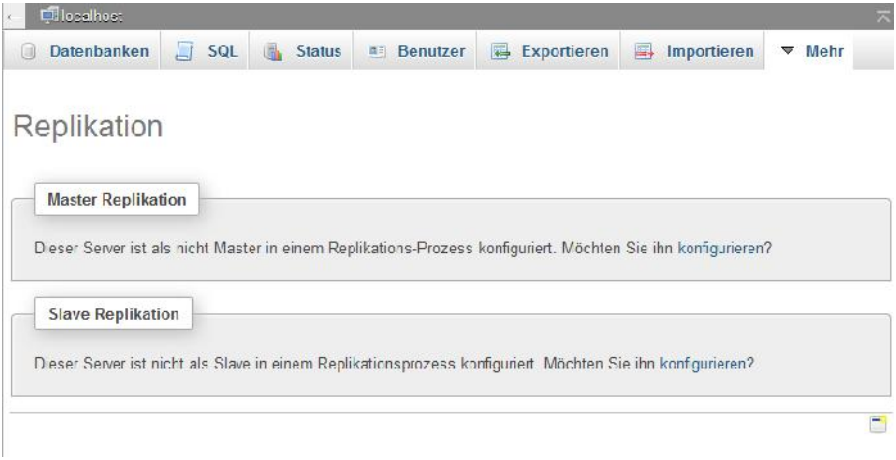
11.3 Datensicherung mit phpMyAdmin

Wie Sie Ihr System schützen und welche Sicherheitsmaßnahmen Sie ergreifen, ist meist davon abhängig, in welchem Kontext ein System eingesetzt wird. Wenn es sich um ein unternehmenskritisches System mit einer permanenten Internet-Anbindung handelt, ist es natürlich anders zu schützen als ein lokales Testsystem, das nur in einer Abteilung erreichbar ist.

Wenn Sie auf Ihrem System wichtige Daten hosten, ist es natürlich auch wichtig, dass Sie diese – am besten regelmäßig – sichern. Sie müssen dazu nicht unbedingt gleich zu einer aufwendigen Back-up-Lösung greifen, sondern können sich auch die Sicherungsfunktionen von phpMyAdmin zunutze machen. Zumindest können

Sie damit die Daten eines Content-Managementsystems, eines Online-Shops oder einer anderen MySQL-basierten Anwendung sichern.

Der MySQL-Datenbankmanager phpMyAdmin stellt Ihnen eine sehr flexible Import- und Exportfunktion zur Verfügung. Um bestehende Daten zu sichern, folgen Sie auf der phpMyAdmin-Übersicht dem Verweis *Exportieren*.



phpMyAdmin stellt Ihnen Export- und Replikationsfunktionen zur Datensicherung zur Verfügung.-

Wählen Sie zunächst aus, welche Daten Sie exportieren wollen. Dann bestimmen Sie das Zielformat. Außerdem können Sie eine Fülle an Exportoptionen verwenden, die beispielsweise Fragen der Datenstruktur bestimmen. Im unteren Bereich des Exportdialogs bestimmen Sie das Ziel, auf das die Sicherung kopiert wird. Sie können auch eine Komprimierung verwenden. Die gesicherten Daten lassen sich über die Importfunktion von phpMyAdmin ebenfalls sehr einfach wiederherstellen.

Ein absolutes Highlight unter den phpMyAdmin-Funktionen ist das Replikationsmodul, das bereits mit phpMyAdmin 3.3.0 eingeführt wurde. Es dient – wie sein Name schon besagt – der Synchronisation von Datenbeständen. Es ist insbesondere für alle jene Unternehmen von Bedeutung, die mit mehreren Servern arbeiten. Aber Replikation ist auch aus Gründen der Performance und Datensicherung von Bedeutung, weil replizierte Systeme Daten schneller ausliefern bzw. als (zusätzliche) Datensicherung dienen. Beide Anforderungen deckt die Replikationsfunktion von phpMyAdmin 4.0 ab.

11.4 Nach dem Angriff ist vor dem Angriff

Insbesondere kommerzielle Sites sind immer wieder beliebte Hacker-Ziele. Wenn auch Ihre Site womöglich Ziel eines Hackerangriffs war, so müssen Sie zunächst sicherstellen, ob Ihr System kompromittiert wurde. Im nächsten Schritt geht es darum festzustellen, ob Änderungen der Umgebung vorgenommen wurden und wenn ja, welche.

Nach einer Hacker-Attacke sind eigentlich Computer-Forensiker dran, die sich auf die Spurensuche, deren Analyse und Auswertung machen. Nach einem Angriff beginnen Sie zunächst die Sicherstellung des bzw. der attackierten Geräte und Speichermedien. Sie müssen sich auch an die Ermittlung aller Datenbestände machen. Es empfiehlt sich dabei, ein Protokoll der Aktionen zu erstellen, die der Administrator oder User nach dem Angriff bei der Erkennung der Systemeingriffe des Angreifers durchgeführt hat.

Befindet sich das verdächtige System noch in Betrieb, so müssen auch hier zunächst die Daten gesichert werden, die sich in den flüchtigen Speichern befinden. Es handelt sich um die gleichen Speicher wie bei Geräten, bei denen die Attacke bereits gelaufen ist. Auch hier steht als Nächstes eine Analyse der Datenträger an.

Komplizierter wird die Sache, wenn ein Angriff noch läuft. In diesem Fall müssen Sie Nutzen und Schaden gegeneinander abwägen. In der Regel ist es sinnvoll, die Netzwerkverbindung zu kappen, um das Löschen sensibler Daten oder Log-in-Informationen zu verhindern. Erweist sich der Angreifer als relativ harmlos und führt er keine schädlichen Aktionen durch, so sollten Sie versuchen, die Verbindungsinformationen auszulesen, um den Hacker später eindeutig identifizieren zu können.

In der Praxis erweisen sich die Forensic Toolkits als ausgesprochen nützliche Helfer bei der Durchführung typischer forensischer Aktionen. Sie helfen insbesondere bei folgenden Aufgaben:

- Automatisierte Analysen
- Rekonstruktion von Daten
- Speichermedien manipulationssicher duplizieren
- Auswerten von Datenformaten
- Sicherung der flüchtigen Daten
- Analyse der Zugriffs- und Metadaten

WinAudit erlaubt den kostenlosen Einstieg in die Welt der digitalen Forensik.

Es liegt in der Natur der Sache, dass solche Toolkits eine Vielzahl an Codierung und Dateiformaten unterstützen müssen, die in den verschiedenen zum Einsatz kommenden Betriebssystemen zu finden sind. Wichtig ist auch, dass die Datenuntersuchungen im Idealfall auf verschiedenen Ebenen stattfinden können, da jede Speicherebene aufschlussreiche Informationen bieten könnte.

Wenn Sie mit Windows arbeiten, so kann ich Ihnen WinAudit (*http://www.pxserver.com/WinAudit.htm*) ans Herz legen. Es taugt für die professionelle Detektivarbeit. Wenn Sie mit Linux arbeiten, ist das freie The Sleuth Kit (*http://www.sleuthkit.org/sleuthkit/*) erste Wahl. Allerdings ist es weitaus komplizierter in der Handhabung.

Nach einem mutmaßlichen Hacker-Angriff sollten Sie außerdem folgende Aktionen durchführen:

- Kontrollieren Sie die Logdateien Ihres Systems auf verdächtige Anfragen und Zugriffe. Hierbei ist ein professioneller Logfile-Analyzer wie der bereits oben erwähnte AWStats sehr hilfreich.
- Stellen Sie sicher, dass Sie alle Dateien und Verzeichnisse gelöscht haben, auch alle Unterverzeichnisse und alle Dateien sowie die Datenbanktabellen.

- Erst nach diesen Aktionen sollten Sie Ihr System aus dem letzten Back-up wiederherstellen.

11.5 Umfassender Schutz dank ModSecurity

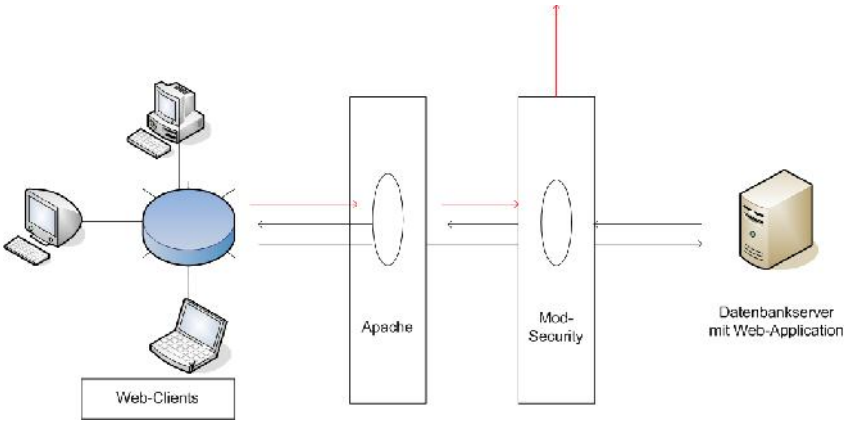
Typische datenbankbasierte Lösungen wie Magento (das gilt natürlich auch für Content-Managementsysteme, Blogs und dergleichen mehr) sind für potenzielle Angreifer beliebte Ziele. Viele Betreiber solcher Systeme übersehen, dass die schöne Fassade doch „nur“ ein Datenbank-Front-end und der Weg in ein System kürzer ist, als man denkt. Dank SQL-Injektion und anderer Attacken verschaffen sich Angreifer schnell weitreichende Zugriffsmöglichkeiten.

11.5.1 Schutz für Web-Anwendungen

Die klassischen Firewall-Technologien agieren auf Netzwerkebene und bieten auf der Ebene der Web-Anwendungen kaum bis keinen Schutz. Die Lösung für dieses Problem: Web-Application-Firewalls, die gelegentlich auch als WebShields bezeichnet werden. Solche Tools filtern den Datenstrom zwischen Browser und Web-Applikation. Wird ein unzulässiges Eingabemuster identifiziert, so wird – abhängig von der jeweiligen Konfiguration – der Transfer unterbrochen oder auf andere Weise reagiert. Eine Web-Application-Firewall ist also nichts anderes als ein Proxy.

Inzwischen gibt es eine beachtliche Palette an solchen Schutzlösungen – freie und kommerzielle. Neben der Filterung sind verschiedene Lösungen auch in der Lage, die vom Webserver an den Browser versandten Daten zu überwachen. Allerdings sind sie nicht in der Lage, auf alle Angriffsformen auf Web-Applikationen optimal zu reagieren. Es versteht sich von selbst, dass das Schließen von Sicherheitslücken der eingesetzten Lösung immer der bessere Schutz ist. Doch zeigt die Erfahrung, dass das nicht immer möglich ist, weil man etwa ein quelloffenes System betreibt, selbst aber nicht über das notwendige Know-how für das Schließen der Lücke verfügt.

Da die Angriffe auf Web-Anwendungen sehr unterschiedlich sein können, man denke nur an die gefürchteten SQL-Injektionen und Cross-Site-Scripting-Angriffe, müssen Sie davon ausgehen, dass der Aufwand für die Integration eines solchen Schutzes höher ist als bei einer Standard-Firewall. Auch mit deutlich höheren Lastanforderungen ist zu rechnen, wenngleich hier verhältnismäßig wenige Erkenntnisse vorliegen.



ModSecurity erweitert Ihre Apache-basierte Webanwendung um einen Traffic-Filter mit Reaktionsfunktionen.

Wenn Sie nicht sicher sind, welches für Ihre Infrastruktur die optimale Lösung ist, dürfte der Leitfaden zur Evaluierung von Web-Application-Firewalls des Web Application Security Consortiums (*http://www.webappsec.org/projects/wafec/*) für Sie von Interesse sein. Er wird Ihnen bei der Suche nach der passenden Lösung nützlich sein.

ModSecurity (*http://www.modsecurity.org*) stammt aus der amerikanische Software-Schmiede Breach Security (*http://www.breach.com*). Der Filter unterliegt der GPL und ist somit frei verfügbar. Die Entwickler bieten neben kommerziellem Support und Schulung auch eigene Hardware-Komponenten für den Schutz von Web-Applikationen an.

11.5.2 Nicht nur eine Apache-Lösung

Inzwischen gibt es verschiedene Web-Application-Firewalls. Da der überwiegende Teil der Web-Anwendungen auf dem Apache ausgeführt wird, ist es kaum verwunderlich, dass es für diesen eine spezielle Lösung gibt: ModSecurity. Dieser Filter nimmt eine besondere Stellung unter den freien Lösungen ein. Dank des DSO-Mechanismus kann er recht einfach nachträglich installiert werden. Sie sind aber keineswegs nur auf den Apache-Webserver beschränkt, sondern können ModSecurity auch als Reserve-Proxy einsetzen und so jeden beliebigen Webserver absichern.

ModSecurity ist ein typischer Input-Filter, den Sie mit Regeln versehen, um so beispielsweise XSS, SQL-Injection, Null-Byte oder Path Traversal zu erkennen und entsprechend zu reagieren. Das sogenannte Advanced Filtering ermöglicht es, selektiv auf bestimmte URLs oder auf bestimmte Werte im HTTP-Header zu reagieren. Es gibt weitere Besonderheiten, so können Sie beispielsweise mithilfe von LUA externe Programme integrieren und somit die Funktionalität des Filters nahezu beliebig erweitern.

11.5.3 Installation

ModSecurity ist speziell für das Zusammenspiel mit einem Apache-2.x-Webserver entwickelt worden. Bevor Sie sich an die Installation des Filters machen, sind neben einer aktuellen Apache-Installation verschiedene Voraussetzungen zu erfüllen. Stellen Sie zunächst sicher, dass das Modul *mod_unique_id* installiert ist. Außerdem ist die Installation der neuesten Version von libxml2 (*http://xmlsoft.org/downloads.html*) erforderlich. Optional ist die Installation der Skript-Sprache LUA 5.1.x (*http://www.lua.org*), wenn Sie ModSecurity funktional erweitern wollen.

Bevor Sie mit der Installation von ModSecurity beginnen, sollten Sie den Apache anhalten. Dann laden Sie sich das ModSecurity-Archiv von der Homepage und entpacken es. Die weitere Vorgehensweise hängt davon ab, ob Sie ModSecurity auf einem Linux- oder Windows-System ausführen.

Unter Linux führen Sie das *configure*-Skript aus. In der Regel sind keine weiteren Optionen erforderlich:

```
./configure
```

Starten Sie die Kompilierung mit *make* und führen Sie einen Test mit *make test* durch. Optional können Sie den ModSecurity Log Collector mit dem Kommando *make mlogc* kompilieren. Die eigentliche Installation erfolgt mit dem typischen Installationsbefehl:

```
make install
```

Wenn Sie ModSecurity mit einer Apache-für-Windows-Installation ausführen wollen, so editieren Sie die Datei *Makefile.win*, um den Apache-Basis- und Bibliothekenpfad anzupassen. Kompilieren Sie die Datei mit folgendem Kommando:

```
nmake -f Makefile.win
```

Installieren Sie dann das ModSecurity-Modul:

```
nmake -f Makefile.win install
```

Als Nächstes kopieren Sie die Dateien *libxml2.dll* und *lua5.1.dll* in das Apache-bin-Verzeichnis.

Damit sind die Betriebssystem-spezifischen Schritte abgearbeitet. Im nächsten Schritt editieren Sie die Apache-Konfigurationsdatei *httpd.conf*. Unter Linux müssen libxml2 und lua5.1 vor ModSecurity geladen werden:

```
LoadFile /usr/lib/libxml2.so
LoadFile /usr/lib/liblua5.1.so
```

Für das Laden des ModSecurity-Moduls verwenden Sie folgenden Befehl:

```
LoadModule security2_module modules/mod_security2.so
```

Zum Abschluss müssen Sie nur noch ModSecurity konfigurieren und den Apache neu starten.

11.5.4 ModSecurity im Überblick

Als Web-Application-Firewall bietet ModSecurity Schutz für Ihre Web-Applikationen vor allen gängigen Angriffsarten. Doch damit nicht genug. ModSecurity erlaubt Ihnen die Überwachung des HTTP-Traffics und stellt Ihnen eine Echtzeitanalyse zur Verfügung. Und all das, ohne dass größere Veränderungen an Ihrer Infrastruktur erforderlich wären.

Sie können mit ModSecurity den gesamten Traffic mit Ihrer Anwendung protokollieren. Dabei können Sie über die ModSecurity-Konfiguration bestimmen, welche Informationen für Sie von Interesse sind. Da in verschiedenen Requests bzw. Responses immer auch kritische Daten enthalten sind, kann ModSecurity diese Informationen vor der Protokollierung auch maskieren. Außerdem agiert der Sicherheitsspezialist als eine Art Web-Intrusion-Detection-Tool, das die Definition von Reaktionen auf verdächtige Ereignisse erlaubt.

Beim Schutz vor Attacken und dem Just-in-time-Patching unterstützt ModSecurity drei Ansätze:

- **Negatives Sicherheitsmodell**: Bei diesem Ansatz werden Requests auf Anomalien, unübliche Verhalten und Einträge untersucht und die Requests dann nach einem eigenen Punktesystem bewertet. Requests mit einer hohen Bewertung werden entweder aufgezeichnet oder abgewiesen.
- **Positives Sicherheitsmodell**: Bei diesem Ansatz läuft die Sache anders. Hier werden nur die Requests zugelassen, von denen bekannt ist, dass sie gültig sind. Dieser Ansatz setzt allerdings eine genaue Kenntnis der zu schützenden Anwendung voraus.
- **Bekannte Schwachstellen und Verwundbarkeiten**: Der letzte Ansatz ist das Standardmodell. Hier agiert ModSecurity als externes Patching-Tool, das die Möglichkeiten für Attacken erheblich einschränkt. Der Vorteil: Die Schwachstellen der zu schützenden Anwendung werden von außen geschlossen, ohne Eingriffe an der Anwendung selbst vornehmen zu müssen. Sie können also theoretisch beispielsweise eine bekannte SQL-Injektion-Schwachstelle weiter offen lassen, solange ModSecurity entsprechende Requests kennt und diese abfangen kann.

Das Herzstück von ModSecurity ist die sogenannte Rule-Engine. Sie implementiert die ModSecurity-Regelsprache, die speziell für die Bearbeitung von HTTP-Transaktionen entwickelt wurde. Sie ist einfach einzusetzen, erlaubt es, Standardaufgaben einfach zu realisieren, taugt aber auch für komplexe Verarbeitungsprozeduren.

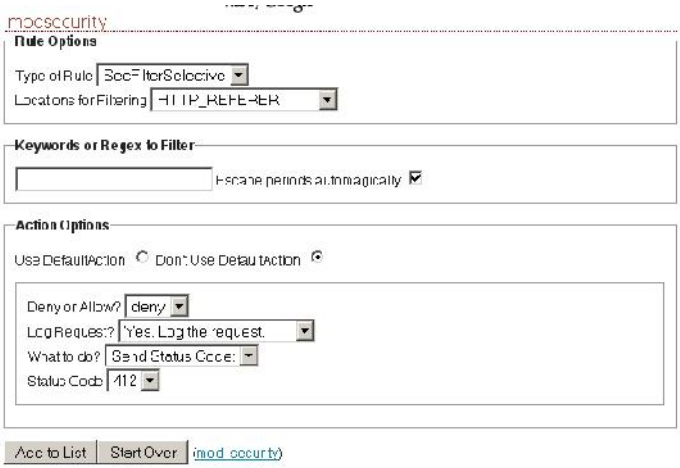
11.5.5 ModSecurity-Regeln erstellen

Für die Filterung und die Behandlung von Requests sind die ModSecurity-Regeln zuständig. Eine Standard-Installation kommt mit einem Basissatz an Regeln daher. Diese Regeln sind im Ordner *Rules* zu finden, tragen die Dateierweiterung *conf* und sind detailliert dokumentiert. Wenn Sie eigene Regeln schreiben wollen, sollten Sie sich daher zunächst intensiv mit den Core-Regeln befassen.

Um Ihre Web-Applikationen vor unerwünschten Attacken zu schützen, verwenden die Core-Regeln folgende Techniken:

- Sie erkennen Verletzungen des HTTP-Protokolls und definieren lokale Verarbeitungsregeln.
- Sie erkennen gängige Attacken.
- Sie erkennen Crawler, Bots, Scanner und andere möglicherweise schädliche Aktivitäten.

- Sie erkennen Trojaner und deren Aktivitäten.
- Sie unterdrücken Fehlermeldungen des Servers.



Der Regel-Editor von Noel Jackson eignet sich für erste Gehversuche beim Erstellen eigener Regeln.

Ein Angreifer kann beispielsweise versuchen, alle Einträge einer MySQL-Tabelle zu löschen. Dazu verwendet er folgende URL:

```
http://www.server.de/login.php?user=benutzer_name';DELETE%20FROM%20users
```

Verhindern lässt sich dies mit folgender Regel:

```
SecFilter "delete[[:space:]]+from"
```

Um mit ModSecurity eine SQL-Injection-Attacke zu verhindern, können Sie beispielsweise folgende Regeln verwenden:

```
SecFilter "insert[[:space:]]+into"
SecFilter "select.+from"
SecFilter "drop[[:space:]]table"
```

Das Erstellen von eigenen Regeln erfordert ein hohes Maß an Know-how bzgl. der zu schützenden Anwendung und der drohenden Gefahren. Da die Erstellung recht fehleranfällig ist, bietet es sich an, zu geeigneten Tools zu greifen. Für das Erstellen von eigenen Regeln gibt es inzwischen verschiedene Werkzeuge. Das Fortschrittlichste ist sicherlich REMO.

11.5.6 REMO – der Regel-Editor für ModSecurity

ModSecurity ist sicherlich kein einfach zu bedienendes Werkzeug. Die richtige Konfiguration zu realisieren, ist bisweilen schwierig und fehleranfällig. Da ist jede Hilfe willkommen, die die Arbeit mit dem Filter vereinfacht. REMO greift Ihnen beim Erstellen und Optimieren der Regeln unter die Arme.

ModSecurity verfolgt bei seiner Filterung standardmäßig den sogenannten Blacklist-Ansatz. Das bedeutet, dass nur bekannter gefährlicher Traffic gefiltert wird. Das Standardregelwerk sorgt für diese Filterung und verspricht so einen soliden Grundschutz, den man auch mittels des Update-Skripts auf dem neuesten Stand halten kann.

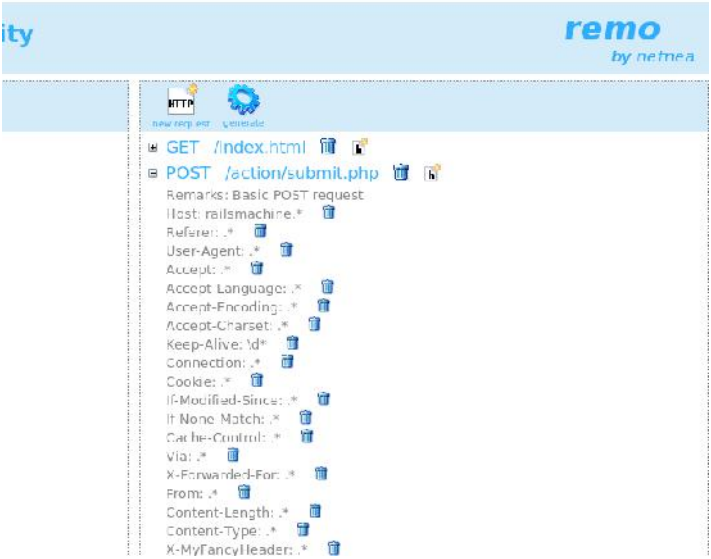
Mit dem Regel-Editor REMO (Rule Editor for ModSecurity, *http://remo.netnea.com*) steht Ihnen ein ausgesprochen nützliches Tool zur Verfügung, mit dem Sie ModSecurity um die Whitelist-Funktionalität ergänzen und gleichzeitig die Regeln über einen webbasierten Editor erweitern. Man spricht in diesem Zusammenhang auch von positiver Sicherheit.

REMO hilft Ihnen dabei, eine Whitelist mit gültigen Requests zu erstellen, zu pflegen und zu warten. Es handelt sich übrigens um eine Ruby-on-rails-basierte Applikation, die sich einfach installieren und ausführen lässt. Laden Sie das aktuelle Paket *remo-0.2.0.tar.gz* herunter, entpacken Sie es in einen Ordner Ihrer Wahl und starten Sie REMO im REMO-Ordner mit folgendem Befehl:

```
ruby script/server
```

Der Zugriff auf die Web-Schnittstelle erfolgt über folgende URL:

```
http://localhost:3000/main/index
```



Mit dem ModSecurity-Regel-Editor REMO vereinfacht sich das Erstellen und Bearbeiten von Regeln wesentlich.

Um eine erste eigene Regel zu erstellen, klicken Sie auf das New-request-Icon. REMO erzeugt im darunterliegenden Feld einen Standardeintrag mit der Bezeichnung *GET click-to-edit*. Mit einem Klick auf die Bezeichnung editieren Sie diesen und können beispielsweise aus der GET- eine POST-Methode machen. Weisen Sie dem Eintrag den Anwendungspfad und die gewünschten Parameter zu. Mit einem abschließenden Klick auf *Generate* erzeugen Sie die Regel. REMO erzeugt aus Ihren Angaben eine Regel-Datei, die Sie dann in das Apache-Verzeichnis kopieren.

Am besten schließen Sie die Regeldatei wie folgt in Ihre Apache-Konfiguration ein:

```
<IfModule mod_security2.c>
       Include /etc/apache2/rulefile.conf
</IfModule>
```

Nach einem Apache-Neustart ist die Regel aktiv. Dank REMO ist es einfach, die Möglichkeiten von ModSecurity besser auszunutzen. Einziges Manko: Die Weiterentwicklung scheint ins Stocken geraten zu sein. Womöglich kommt in Zukunft auch ein Editor der ModSecurity-Entwickler.

11.5.7 Konfigurationsdirektiven

Die meisten ModSecurity-Konfigurationsdirektiven können innerhalb der verschiedenen Apache-Konfigurationen wie, VirtualHost, Location oder Directory, verwendet werden.

Daneben gibt es andere, die nur in der ModSecurity-Hauptkonfigurationsdatei verwendet werden können. Die meisten dieser Konfigurationen sollen außerhalb der Apache-Konfigurationsdatei *httpd.conf* verwendet und über Include-Anweisungen eingebunden werden. Mit den ModSecurity-Konfigurationsdirektiven legen Sie fest, auf welche Bereiche ModSecurity angewendet wird.

Wenn Sie eigene Regeln erstellen wollen, so sollten Sie eine Datei mit der Bezeichnung *modsecurity_crs_15_customrules.conf* erstellen und diese Datei in dem Verzeichnis ablegen, in dem auch die Core-Regeln liegen. Mit dieser Dateibezeichnung ist sichergestellt, dass Ihre Regeln nach der Standard-ModSecurity-Konfiguration, aber noch vor den Core-Regeln geladen werden. So ist gewährleistet, dass Ihre Regeln eine höhere Priorität als die allgemeinen Regeln haben, was gerade bei spezifischen Allow-Regeln wichtig ist, um den Zugriff auf Ihre Anwendung zuzulassen.

Die Entwickler empfehlen ausdrücklich, die Core-Regeln nicht zu verändern. Sollten Sie spezifische Anforderungen haben, sollten sie über die Custom-Rules realisiert werden. In der ModSecurity-Referenz, die Sie im Dokumentationsverzeichnis der ModSecurity-Website finden, sind die vielen Direktiven detailliert mit Beispielen dokumentiert.

Interessant ist in diesem Zusammenhang auch, wo die Regeln und die damit verbundenen Aktionen platziert werden. ModSecurity 2.x erlaubt die Verwendung in den folgenden Kommunikationsphasen zwischen Web-Client- und -Server:

1. Request eines Headers (REQUEST_HEADERS)
2. Request eines Bodys (REQUEST_BODY)
3. Response eines Headers (RESPONSE_HEADERS)
4. Response des Bodys (RESPONSE_BODY)
5. Logging (LOGGING)

Nun muss ModSecurity nur noch wissen, in welcher Phase eine Regel ausgeführt werden soll. Dazu verwendet man die *SecDefaultAction*-Direktive. Hier ein Beispiel für die Verwendung:

```
SecDefaultAction "log,pass,phase:2"
```

```
SecRule REQUEST_HEADERS:Host "!^$" "deny,phase:1"
```

Ein Blick auf die webbasierte ModSecurity-Konsole.

11.5.8 Die ModSecurity-Konsole

Die ModSecurity-Entwickler haben eine weitere Besonderheit im Programm: Die ModSecurity-Konsole (*http://www.modsecurity.org/projects/console/*). Dabei handelt es sich um eine webbasierte Schnittstelle, der Sie die ModSecurity-Aktionen und -Warnungen in Echtzeit entnehmen können. Dieses Tool ist neben Linux auch für Windows-Plattformen verfügbar. Sie können mit dem Werkzeug bis zu drei ModSecurity-Sensoren kostenlos steuern und überwachen.

Eigentlich ist das Tool für jene Administratoren gedacht, die mehrere Server überwachen sollen. Aber auch dann, wenn Sie nur für einen Server zuständig sind, ist der Einsatz sinnvoll, denn die Warnungen, die ModSecurity ausgibt, werden Ihnen in aufbereiteter Form präsentiert. Das erleichtert es, insbesondere die sicherheitskritischen Aktionen detailliert zu analysieren.

Die Ereignisse werden in einer eigenen Datenbank gesammelt. Der Datenbestand kann über ein aufwendiges Suchformular nach den unterschiedlichsten Kriterien,

wie Transaktions-ID, Hostname, angefragte URL, Status-Code, Anwendung etc., durchforstet werden.

Eine weitere Besonderheit sind sicherlich die Report-Funktionen. Die ModSecurity-Konsole kann Berichte im PDF-Format erzeugen – und zwar per Zeitsteuerung oder bei Bedarf – und diese dann auch gleich noch per E-Mail versenden.

12 Einsatzszenarien – Magento, WordPress & Co.

XAMPP bildet, wo auch immer man sich umschaut, heute die Grundlage unterschiedlicher Unternehmensanwendungen, die auf dem Apache-MySQL-PHP-Gespann basieren. Aufzählen könnte man an dieser Stelle viele. Man denke nur an die unzähligen PHP-basierten Content-Managementsysteme, Foren- und Group-Ware-Lösungen. Exemplarisch wollen wir in diesem Kapitel am Beispiel von vier Anwendungen zeigen, wie unterschiedlich aufwendig die Installation von Anwendungen sein kann, die auf XAMPP basieren:

- Magento
- Joomla!
- WordPress
- Tine

Besonders einfach ist die Installation gängiger Applikationen mit dem BitNami-Installer, der über die Startseite Ihrer XAMPP-Installation verfügbar ist.

Mit BitNami wird die Installation von webbasierten Applikationen wie Joomla, Magento und WordPress zum Kinderspiel.

12.1 Magento

Wenn Sie die ersten Schritte mit Magento (*http://www.magentocommerce.com*) unternehmen, das System zum ersten Kennenlernen und Evaluieren (am besten auf einem Testsystem) einrichten, so werden Sie vermutlich aus dem Staunen nicht mehr herauskommen. Magento ist ein in PHP entwickeltes Shopping-System, das sich ausgesprochen flexibel zeigt – nicht nur bei der Produktkategorisierung, sondern auch in anderen Bereichen. Magento besitzt eine eigene Suchmaschinen-Optimierung, eine Ajax-unterstützte Anwendungsoberfläche für Front- und Back-end sowie mehr als beachtliche Analyse- und Reportingfunktionen. Magento hat sich längst im mittleren E-Commerce-Segment etabliert.

12.1.1 Was spricht für Magento?

Wenn Sie in naher Zukunft einen Online-Shop aufbauen oder von einem bestehenden System oder Dienstleister zu einer neuen Lösung umsteigen wollen, weil Sie mit der bestehenden Lösung unzufrieden sind, so haben Sie die Qual der Wahl. Es gibt Dutzende Lösungen und Anbieter, für die Sie sich entscheiden können. Bevor Sie sich nun auf Magento oder eine andere Lösung festlegen, sollten Sie sich vergegenwärtigen, dass ein Shop immer zwei Seiten hat: Die eine, das Front-end, bekommen die hoffentlich zahlreichen Kunden zu sehen, die andere, das Back-end, dient der Administration des Shops.

Die meisten Shop-Betreiber interessieren sich leider nur für die Back-end-Seite – zum Leidwesen ihrer Kunden. Dabei ist es für den Erfolg eines Shops wichtig, dass sich Ihre Kunden wohlfühlen und dann hoffentlich vielfach zuschlagen.

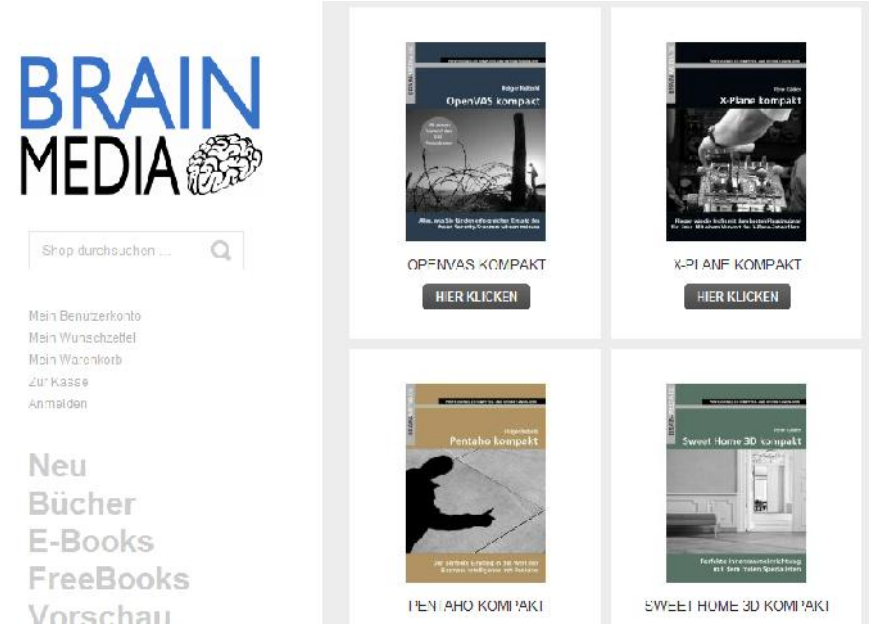
Vielen Betreibern ist es nach wie vor wichtiger, dass Ihnen ein multifunktionales Back-end mit allem Pipapo zur Verfügung steht, als dass die Kunden sich in einer angenehmen Umgebung bewegen. Bei Magento haben Sie beides: Eine exzellente Administrationszentrale für den Betreiber und eine vorzügliche Shopping-Umgebung für Ihre Kunden.

Wie komfortabel das Shoppen in einem Magento-basierten Shop ist, können Sie in einem von den Entwicklern angelegten Demo-Shop (*http://demo.magentocommerce.com*) prüfen. Nehmen Sie sich die Zeit und unternehmen Sie doch einfach einmal einen Einkaufsbummel.

In einem Shop wie dem Demo-Shop fühlt man sich als Kunde bestens über alle Eigenschaften des Produkts informiert. Verschiedene intelligente Funktionen unterstützen die Kaufentscheidung. Den Warenkorb hat man jederzeit verfügbar, und Sie haben auch an der Kasse volle Transparenz über den Inhalt Ihres Einkaufswa-

gens. Das gilt auch für Kostenbestandteile oder zusätzliche Kosten, wie Mehrwertsteuer oder Versand.

Hinter Magento steckt die Firma Varien (*http://www.varien.com*), die ihren Sitz im sonnigen Los Angeles hat. Sie wurde 2001 gegründet und schickt sich mit ihrem Hauptprodukt Magento an, den E-Commerce-Markt aufzumischen.



Auch der Brain-Media-Shop verwendet Magento mit AJAX-Funktionalität.

Woher die Bezeichnung Magento stammt, scheint nicht so klar. Der Schluss liegt nahe, dass diese von der Firmenfarbe stammt. Auch das Magento-Logo ist dem magentafarbenen Firmenlogo sehr ähnlich – auch wenn das Magento-Logo inzwischen mehr orange als pinkfarben ist.

Die Entwickler von Varien haben sich zum Ziel gesetzt, mit Magento die Marktführerschaft zu erobern. Wenn es in dem rasanten Tempo weitergeht, wie die bisherige Entwicklung verlaufen ist, so scheint das nur eine Frage der Zeit zu sein.

Wie bei anderen quelloffenen Projekten steht dem Varien-Team eine große Entwicklergemeinschaft zur Seite. Der Reiz, hier gleich von Anfang an dabei zu sein,

ist sicher sehr hoch – gerade auch für potenzielle Dienstleister, für die sich ein neuer Markt öffnet.

Besonders aktiv ist die deutsche Community, die innerhalb kürzester Zeit einen sehr beachtlichen Beitrag zur Weiterentwicklung des Systems geleistet hat. Wichtig für potenzielle Betreiber eines Magento-basierten Shops: Sie können mit Support sowohl von professioneller Seite als auch von der großen Entwicklergemeinschaft rechnen.

Wenn man das erste Mal mit Magento spielt, spürt man förmlich, dass sich die Entwickler bereits vor der Entstehung viele Gedanken gemacht und die notwendigen Schlussfolgerungen für die Implementierung eines Online-Shops zogen. Dank eines schlüssigen Konzepts ist Magento eine sehr flexible Lösung, die sich recht einfach an kundenspezifische Bedürfnisse anpassen lässt. Das Shopping-System bietet verschiedene Wege, den Kunden zum Produkt und schließlich zum Kauf zu bewegen.

Besonders wichtig für den Betreiber ist die Suchmaschinenfreundlichkeit. Magento unterstützt die wichtigsten Elemente der Suchmaschinenoptimierung automatisch. Aus den Produktdaten werden geeignete URLs, ein aussagekräftiger Titel und die passenden Meta-Tags generiert.

Aber auch für den Kunden hat der Magento-Shop viele nützliche Funktionen zu bieten. Sucht er einen bestimmten Artikel, kann er eine Tag-Wolke, umfangreiche Suchfunktionen oder Filter nach Preis, Marke oder Farbe nutzen.

In Magento können Sie auch Produktbewertungen anderer Kunden zulassen und dem Kunden weitere Produktvorschläge unterbreiten. Der Kunde kann mehrere Produkte miteinander vergleichen – ein tolles Feature, um ihm die Kaufentscheidung zu erleichtern. Auch eine Wunschzettelfunktion, wie man sie von Amazon & Co. kennt, hat Magento zu bieten.

Eine meiner Lieblingsfunktionen sind die Marketingfunktionen – ein Punkt, der mich an xt:commerce und anderen Lösungen schon immer gestört hat. Im Online-System sind alle notwendigen Informationen für Marketingkampagnen gebündelt. Daher ist es nur folgerichtig, diese auch für das Versenden eines Newsletters oder die Durchführung von Kampagnen zu nutzen.

Magento ist eine sehr flexible Lösung. Sie können beispielsweise folgende Dinge realisieren:

- Staffelpreise in Abhängigkeit von der Menge einführen.
- Verschiedene Steuersätze und Währungen definieren.
- Unterschiedliche Steuersätze oder Preisregeln für einzelne Kundengruppen anlegen.

- Einen mehrsprachigen Shop anlegen.
- Zusammenfassung mehrerer Shops auf einer oder mehreren Sites.

Wie der Demo-Shop zeigt, ist mit Magento auch für eine optisch ansprechende Gestaltung des Shops gesorgt. Ihnen stehen verschiedene Layout-Vorlagen und Optionen für Bilder zur Verfügung, die Sie natürlich auch anpassen können.

Sollten Sie weitere Informationen in Ihren Shop integrieren wollen, so ist auch das kein Problem, denn Magento verfügt über ein eigenes Content-Managementsystem, das ebenfalls über eine Suchmaschinen-Optimierung verfügt.

Je größer die Anwenderzahl wird und je mehr die Verbreitung zunimmt, umso mehr werden Sie auch von den kommenden Verbesserungen profitieren. Bereits heute gibt es bei Magento Connect (*http://connect.magentocommerce.com*) eine Vielzahl von Extensions, die beispielsweise die Migration von Drittsystemen oder die Anbindung an ein bestehendes Content-Managementsystem erlauben.

Und schließlich gibt es umfangreiche Möglichkeiten, die Verkäufe und das Vorgehen der Benutzer im Shop auszuwerten und die konkreten Erkenntnisse aus Wunschzetteln, Tags und Suchabfragen in konkrete Verbesserungen am Shop umzusetzen.

Bevor wir uns mit der Installation und Konfiguration von Magento befassen, sollten Sie einige Eigenschaften des Shoppingsystems und zentrale Begriffe kennenlernen, denen Sie immer wieder begegnen werden. Magento besteht aus verschiedenen Elementen, die in ihrer Gesamtheit die Funktionalität, das Design und die Geschäftslogik bestimmen.

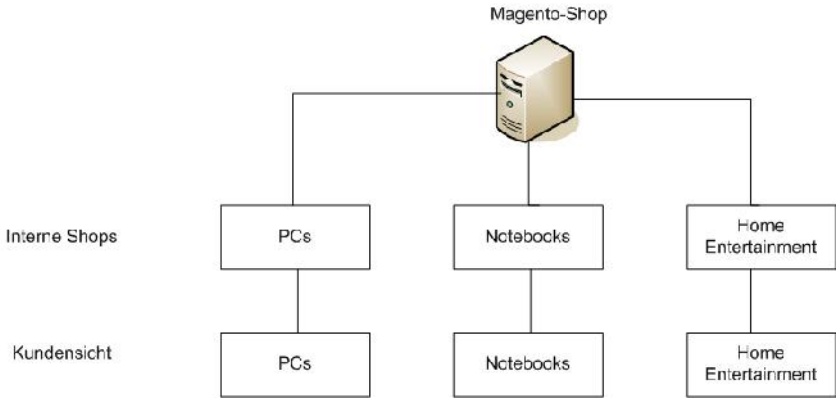
Neben den unzähligen Shop-spezifischen Funktionen, die Magento abzudecken versteht, ist die Unterstützung von mehreren Shops ein zentrales Highlight des Systems. Nicht einmal Content-Managementsyteme wie Joomla! beherrschen das auf ihrem Einsatzgebiet.

Sie können mit Magento verschiedene Shops verwalten, die unter unterschiedlichen URLs erreichbar sind. Ob in diesen Shops auch unterschiedliche Sprachenvarianten angeboten werden, bleibt Ihnen überlassen. Das ist sicherlich auch von Ihren Produkten und der Zielgruppe abhängig. Unterschiedliche Sprachvarianten können auch unter einer URL verfügbar sein. Sie müssen für Ihre deutschsprachigen Kunden also beispielsweise nicht zwingend eine de- und für die internationalen eine com-Domain verwenden.

Natürlich können Sie einen bestehenden Shop auch jederzeit lokalisieren, eben so, wie es in Ihre Planung passt bzw. mit Ihrem Budget zu leisten ist. Sie können mit

Magento auch eine Shop-in-Shop-Umgebung aufsetzen – ein bewährtes Konzept, das beispielsweise in der Kaufhauskette Kaufhof sehr erfolgreich angewendet wird.

Nachstehende Abbildung zeigt ein mögliches Szenario: Der zentrale Magento-Server vereint unter einer Schnittstelle drei Shops. Dem Kunden präsentieren sich in diesem Szenario drei eigenständige Online-Angebote. Jeder dieser Bereiche kann auch unterschiedliche Sprachversionen anbieten.



Ein typisches Szenario: Mit Magento legen Sie in Ihrem Shop verschiedene Bereiche bzw. Sub-Shops an, die auch eigenständig sein könnten.

Entsprechend ist denkbar, dass Sie mit Magento mehrere eigenständige Shops verwalten, die nicht nur unterschiedliche Produkte anbieten, sondern auch einen anderen Standort haben. Damit eignet sich Magento hervorragend für Dienstleister, die für ihr Kunden einen professionellen Online-Shop realisieren.

Die mit Abstand häufigste Variante ist allerdings viel einfacher: Sie ist durch ein Shopping-System mit einem Warenangebot gekennzeichnet. Auch hier bekommt der potenzielle Kunde „nur“ einen Online-Shop zu Gesicht.

Wir wollen an dieser Stelle nicht in die Tiefen des Magento-Systems einsteigen. Dennoch sollten Sie auch die wichtigsten Komponenten der Magento-Architektur kennenlernen. Später kommen wir auch noch auf die Programmstruktur zu sprechen.

Magento basiert auf dem sogenannten Zend Framework. Das ist ein Open-Source-Framework für die Entwicklung von Web-Anwendungen und Services mit PHP 5. Das Gerüst ist durch eine Objektorientierung gekennzeichnet, wobei jede Kompo-

nente mit wenig Abhängigkeiten zu anderen Komponenten daherkommt. Durch diese lose Koppelung ist es Entwicklern möglich, die Komponenten individuell einzusetzen. Die Zend-Entwickler bezeichnen das auch als Use-at-will-Design.

Dank des Zend-Frameworks basiert Magento auf drei Eckpfeilern:

- Flexibilität – das System ist an die jeweiligen Bedürfnisse anpassbar. Wie wir noch sehen werden, bietet Magento eine Unmenge an Konfigurations- und Anpassungsmöglichkeiten.
- Upgradebar – durch die Trennung des Funktionskerns von Anpassungen und Erweiterungen ist das System erweiterbar.
- Sicher und schnell – durch die Verwendung des Zend-Frameworks ist Magento schnell und vergleichsweise sicher. Auch auf die Sicherheit kommen wir in einem eigenen Kapitel noch zu sprechen.

Die Grundfunktionen – das klingt nach wenig, aber es sind eine ganze Menge – sind in dem Magento-Kern implementiert. Das ist das Paket, das Sie über die Magento-Commerce-Website herunterladen und dann installieren. Die Kernkomponenten des Systems sind eine Sammlung von Modulen, die die verschiedenen Grundfunktionen bereitstellen und vom Magento-Entwicklerteam stammen bzw. von diesem zertifiziert wurden.

Die Entwickler empfehlen ausdrücklich, diese Dateien nicht zu editieren und zu verändern. Die Kernfunktionen sind im Core-Ordner zu finden, einem Unterordner des app-Verzeichnisses. Im app-Verzeichnis finden Sie zwei weitere vordefinierte Ordner, die bei einer Neuinstallation leer sind: *community* und *local*. In diesen beiden Ordnern werden weitere Komponenten installiert. Auch darauf kommen wir später noch zu sprechen. Im Ordner *local* finden Sie Anpassungen. Sie werden vom Kern getrennt gespeichert und verwaltet, damit sie den Kernfunktionen nicht in die Quere kommen.

Bei dem Code im Ordner *community* handelt es sich meist um Erweiterungen des Magento-Shops. Auch sie werden in einem eigenen Ordner gespeichert, damit es keine Probleme mit dem Kern gibt.

Ein weiteres wichtiges Merkmal von Magento ist seine Erweiterbarkeit. Sie können – Programmierkenntnisse vorausgesetzt oder aber mithilfe von speziellen Erweiterungen – Magento funktional aufbohren. Diese Erweiterungen werden über das Magento-Kontrollzentrum installiert. Prinzipiell kennt das System verschiedene Erweiterungen:

- **Module**: Module dienen der Erweiterung der Funktionalität von Magento. Über solche Module lassen sich beispielsweise Zahlungs-Gateways reali-

sieren. Andere mögliche Erweiterungen sind Zusatzfunktionen für Ihr Marketing oder Migrations-Tools.

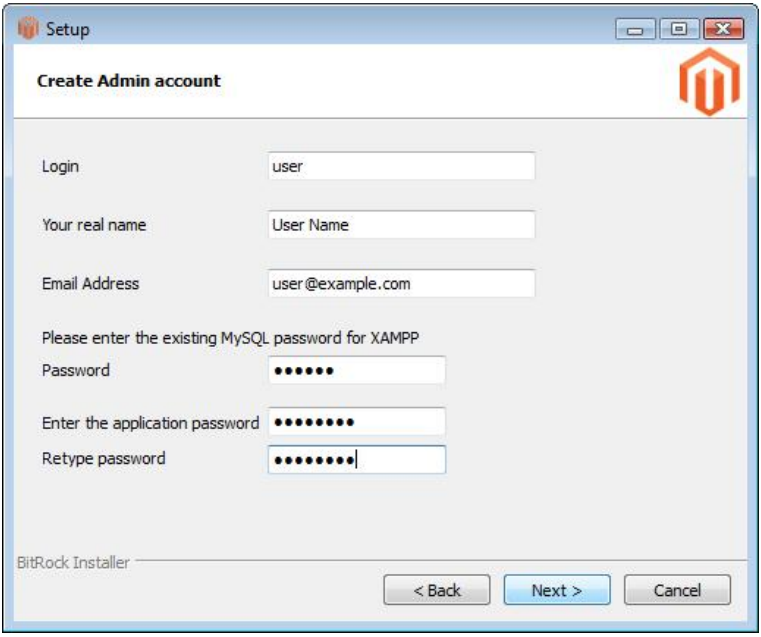
- **Schnittstelle**: Bei einer Magento-Schnittstelle handelt es sich um eine Sammlung von Themes, die das visuelle Bild der Magento-Schnittstelle bestimmen. Sie können eine Schnittstelle dem Shop, der Website oder auch beiden zuweisen.
- **Themes**: Bei einem Theme handelt es sich um eine Kombination aus Layout-Einstellungen, Templates und Skin-Dateien. Magento kommt mit einigen Standard-Themes daher, kann aber auch um Dritt-Themes erweitert werden, mit denen Sie dem Shop ein völlig anderes Aussehen verpassen. In diesem Zusammenhang ist vielleicht noch interessant, dass es sich bei den Layouts um XML-Dateien handelt, in denen die Blockstruktur definiert ist und die Site- sowie Meta-Informationen hinterlegt sind. Bei den Templates handelt es sich um PHTML-Dateien, die ihrerseits (X)HTML-Code enthalten. Die Skins sind JavaScript- und CSS-Code, die die (X)HTML-Dateien ergänzen.
- **Blöcke**: Dann gibt es noch die sogenannten Blöcke. Wenn Sie bereits mit einem Content-Managementsystem gearbeitet haben, so wissen Sie, was es mit diesen Blöcken auf sich hat. Dahinter stehen fertige Funktionsbereiche, wie der Header, die linke Spalte, die Fußzeile oder der Inhaltsbereich. Diese Blöcke können dann mit sogenannten Content-Blöcken bestückt werden. Der Block *Header* kann beispielsweise ein Navigationssystem aufnehmen und im *Footer* können Sie die Content-Blöcke Impressum und/oder Links einfügen.

Damit haben Sie einen ersten Eindruck von den wichtigsten Komponenten des Shopping-Systems. Als Nächstes können Sie sich der Installation widmen.

Die Inbetriebnahme von Magento ist dank des BitNami-Installers einfach. Laden Sie sich über die lokale XAMPP-Startseite das aktuelle Magento-Modul herunter. Das Installationsprogramm bietet Ihnen neben Magento die Einrichtung von Beetailer an, einem Service für die Facebook-Integration.

Nach der Wahl des Installationsverzeichnisses legen Sie den Magento-Administrator an. Sie müssen außerdem das MySQL-Passwort angeben, damit eine Datenbank für das Shoppingsystem angelegt werden kann.

Beachten Sie, dass das Magento-Passwort mindestens acht Zeichen lang sein muss.



Das Ablegen des Magento-Admin-Accounts.

Im nächsten Dialog bestimmen Sie die IP-Adresse des Shops und in einem weiteren die SMTP-Einstellungen. Der Installer kopiert die Shop-Daten in Ihre XAMPP-Umgebung. Ist die Installation von Magento abgeschlossen, greifen Sie über das Applications-Menü der XAMPP-Startseite auf das Shopping-System zu.

Alternativ können Sie auch direkt auf das Shopping-System und die zugehörige Administrationszentrale zugreifen. Der Shop ist über folgende URL verfügbar:

```
http://localhost/magento/
```

Die Admin-Zentrale über diese URL:

```
http://localhost/magento/admin
```

bzw.

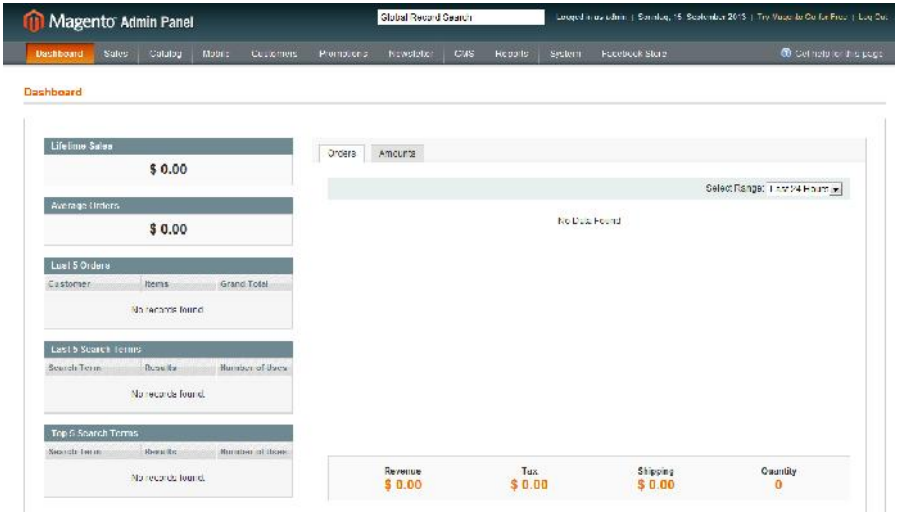
```
http://localhost/magento/index.php/admin
```

Die Installation aller weiteren Module verläuft im Wesentlichen genauso. Sollten bei der Ausführung eines BitNami-Moduls Probleme auftreten, konsultieren Sie das BitNami-Wiki (*http://wiki.bitnami.com*).

12.1.1 Die Administrationszentrale kennenlernen

Bevor wir uns als Nächstes anschauen, wie Sie auf schnellem Weg zu Ihrem ersten eigenen Shop kommen, werfen wir noch einen Blick auf die wesentlichen Elemente der Magento-Administrationszentrale. Die Admin-Konsole besteht aus folgenden Elementen:

- **Header**: Im Header steht Ihnen eine Suchfunktion zur Verfügung. Außerdem zeigt Magento an, als welcher Benutzer Sie angemeldet sind. Auch das Datum und der Ausloggen-Link sind Bestandteil des Headers.
- **Navigationsleiste**: Unterhalb des Headers finden Sie die Navigationsleiste, über die Sie auf die verschiedenen Funktionsbereiche zugreifen. Über den Übersicht-Link gelangen Sie von jeder beliebigen Seite schnell wieder zurück zur Magento-Startseite. Rechts finden Sie den Hilfe-Link, der Sie zur webbasierten Hilfe führt.



Ein erster Blick auf die eingedeutschte Magento-Administrationszentrale.

- **Nachrichtenleisten**: Magento verfügt auch über einen Posteingang. Der Posteingang und neue Nachrichten sind über die Nachrichtenleiste verfügbar, die Sie unterhalb der Navigationsleiste finden. Wenn Sie neue Nachrichten haben, so zeigt Ihnen das ein Hinweisschild an.
- **Arbeitsbereich**: Es folgt der Arbeitsbereich, in dem Sie die eigentlichen Funktionen des Systems finden. Beim Einloggen landen Sie beispielsweise standardmäßig in der Übersicht, die Ihnen die Gesamteinnahmen, den durchschnittlichen Bestellumsatz, die letzten fünf Bestellungen und die Suchbegriffe aufführt. Rechts werden die Details zu den Bestellungen aufgeführt. Über das Auswahlmenü *Bereich auswählen* passen Sie den Ansichtszeitraum an. Am Fuße der Bestellübersicht erfahren Sie außerdem, welche Einnahmen Sie generiert haben, wie der Steueranteil ist, wie hoch die Versandkosten sind und wie viele Produkte Sie verkauft haben.

  Der Arbeitsbereich präsentiert Ihnen weitere interessante Funktionen. So können Sie diesem im unteren Bereich Ihre Bestseller, die am häufigsten angesehenen Produkte, die Liste der Kunden und Neukunden entnehmen.
- **Footer**: Über die Fußzeile können Sie die Sprache der Benutzerschnittstelle ändern – vorausgesetzt, Sie haben mehrere Sprachen installiert. In der Mitte der Fußzeile zeigt Ihnen das System die installierte Version an. In unserem Fall ist es Magento 1.7.0.2. Rechts finden Sie den Link zur Magento-Community, die Sie zurate ziehen können, wenn Sie einmal nicht weiter kommen. Außerdem finden Sie dort die Copyright-Info.

Damit kennen Sie die wichtigsten Elemente der Magento-Schnittstelle. Welches Ihre nächsten Schritte sind, hängt stark davon ab, wie vertraut Sie mit Magento bereits sind bzw. davon, wie viel Erfahrung Sie schon im Umgang mit einer Shopping-Lösung haben. Der eine Anwender füttert das System am liebsten mit den ersten Produkten, ein anderer passt zunächst das Design an, wieder ein anderer widmet sich am liebsten erst den Systemeinstellungen, um weitere Benutzer einzuführen oder einen neuen Shop anzulegen.

12.1.2 Der kurze Weg zum eigenen Shop

Nachdem Sie Magento installiert und konfiguriert haben, wollen Sie natürlich direkt mit der Arbeit an dem System loslegen. Doch wie gehen Sie am besten vor? Hierfür bieten sich verschiedene Wege an – immer abhängig von Ihren Vorkenntnissen und Erfahrungen im Umgang mit einem System wie Magento.

Wenn Sie zu den eher unerfahrenen Anwendern gehören, so ist folgender Weg zu empfehlen: Laden Sie sich die Beispieldaten für den Magento-Shop über den Magento-Download-Bereich *http://www.magentocommerce.com/download/*) herunter. Das Paket ist ca. 10 MB groß. Achten Sie darauf, dass das Paket vor der eigentlichen Magento-Installation installiert werden muss. Mithilfe der Beispieldaten ist es einfach, mit den verschiedenen Funktionen zu spielen und Erfahrungen zu sammeln. Passen Sie die Beispieldaten so an bzw. ergänzen Sie diese so, bis der Shop Ihren Anforderungen entspricht. Dazu müssen Sie insbesondere folgende Anpassungen durchführen:

- Änderung und Erweiterung der Produktverwaltung und Produktbeschreibungen.
- Anpassungen der Steuersätze und Regeln.
- AGB anlegen.
- Kunden und Gruppen anlegen.
- Systemeinstellungen anpassen, insbesondere die Shop-Kontakte, Zahlungsmethoden und Versandmöglichkeiten. Ganz wichtig ist die Konfiguration des SMTP-Servers für den Versand von Transaktions-E-Mails. Außerdem müssen die E-Mail-Vorlagen angepasst werden.

Wenn Sie diese grundlegenden Anpassungen vorgenommen haben, können Sie sich im nächsten Schritt dann auch dem Content-Management und den verschiedenen Marketingfunktionen zuwenden. Design-Anpassungen sind nichts für Einsteiger – auch nichts für Fortgeschrittene.

Wenn Sie bereits Erfahrungen mit dem Aufsetzen eines Online-Shops gesammelt haben, so können Sie mit Magento einfach einen neuen Shop von Grund auf realisieren. Dabei profitieren Sie davon, dass Magento mehrere Shops verwalten kann. Die notwendigen Schritte sind prinzipiell die Gleichen wie bei den Anpassungen des Demo-Shops.

Das A und das O einer jeden Entwicklung: Testen, testen und testen. Bevor Sie Ihren Shop „auf die Allgemeinheit loslassen“, sollten Sie diesen ausgiebig auf seine Funktionalität testen, denn nichts ist ärgerlicher, als wenn Bestellbestätigungen nicht beim Kunden, sondern im Nirgendwo landen, angebotene Zahlungsmethoden nicht funktionieren etc. Am besten suchen Sie sich für das Testen externe Hilfe, da Dritte unbefangen an einen Shop und seine Funktionalität herangehen.

Auf der Brain-Media-Website steht ein FreeBook unter der URL *http://www.brain-media.de/index.php/freebooks.html* zum kostenlosen Download bereit, das Sie in die Verwendung des Shopping-Systems einführt.

12.2 Joomla!

Wer heute eine professionelle Website im Internet präsentieren will, der kommt kaum um den Betrieb eines Content-Managementsystems umhin. Diese helfen Ihnen bei der einheitlichen Präsentation, sind meist über Add-ons und/oder Plug-ins funktional erweiterbar und erleichtern Ihnen (und Ihren Mitarbeitern und Kollegen) die Pflege und Wartung einer Site.

Inzwischen gibt es eine Vielzahl von interessanten Content-Managementsystemen. Neben kommerziellen sind es insbesondere Open-Source-Projekte, die immer mehr Interesse finden. Gerade im deutschsprachigen Raum ist Joomla! sehr beliebt – trotz verschiedener Einschränkungen und Schwächen.

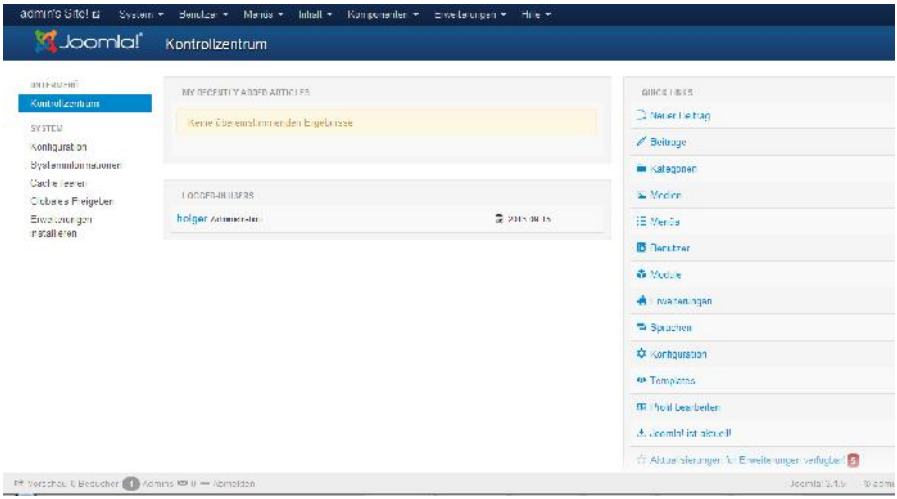
Dennoch gibt es viele gute Gründe für den Einsatz dieses Systems. Als modulare Umgebung kann Joomla! mit einer Vielzahl an Modulen funktional erweitert werden. So stehen Module für Dokumentenmanagement, Bildergalerien, Umfragen, Formular- und Templategenerator, Wettermodule und sogar Online-Shops zur Verfügung. Für Administratoren und Redakteure wichtig: Das System ist extrem einfach zu bedienen. Zum Erstellen von Inhalten verwendet man beispielsweise einen Fast-WYSIWYG-Editor.

Wie man es von einem professionellen System erwartet, trennt Joomla! durch den Einsatz von Templates den Inhalt vom CSS-basierten Layout. Mit dem Template-Konzept kann man seiner Website ein beliebiges Layout verpassen. Weitere Highlights sind die flexible Benutzerverwaltung, die Unterstützung von Content-Syndication, der XML-Export und, und, und. Last, but not least: Joomla! ist Open Source und unterliegt der weit verbreiteten GNU/GPL-Lizenz. Als Open-Source-Software ist das CMS daher kostenlos verfügbar und kann bei Bedarf nach Belieben erweitert werden. Natürlich soll an dieser Stelle nicht verschwiegen werden, dass Joomla! auch – zum Teil – erheblichen Einschränkungen unterliegt.

Joomla! (*http://www.joomla.org* bzw. *http://www.joomla.de*) zählt zu den interessantesten Content-Managementsystemen, die die Open-Source-Gemeinde vorzuweisen hat. Es ist erwiesenermaßen ein sehr leistungsfähiges und dabei einfach wartbares CMS. Es ist in der Lage, sehr große Websites zu realisieren. Die Inhalte werden wie bei anderen Systemen dynamisch aus MySQL-Datenbanken erzeugt.

Joomla! basiert auf PHP und nutzt das Datenbanksystem MySQL. Somit ist es für Administratoren und Entwickler recht einfach, eigene Module und Komponenten für das CMS zu erstellen. In der Regel ist das nicht erforderlich, denn für Joomla! gibt es inzwischen eine Unmenge an Modulen und Erweiterungen. Auch ein auf Joomla! abgestimmtes Shopping-System ist verfügbar. Sogar eine Dreamweaver-Erweiterung für das Erstellen von Templates ist verfügbar. Ein Blick in den Administrationsbereich macht schnell deutlich, warum Joomla! so beliebt ist: Das System besitzt eine klare und saubere Struktur.

Um das System nutzen zu können, genügt eine XAMPP-Installation. Da Sie mit der XAMPP-Installation die Voraussetzung für die Ausführung von Joomla! geschaffen haben, müssen Sie nur noch das Content-Managementsystem installieren. Dazu verwenden Sie am einfachsten ebenfalls das BitNami-Paket. Damit richtet man mit wenig Aufwand eine vollfunktionstüchtige CMS-Umgebung ein.



Das Joomla!-Kontrollzentrum.

Der Zugriff auf Joomla erfolgt nach der Installation über folgende URL:

```
http://localhost/joomla/
```

Die Admin-Zentrale über diese URL:

```
http://localhost/joomla/administrator
```

Über das Joomla!-Kontrollzentrum führen Sie alle administrativen Aufgaben aus. Sie konfigurieren die Umgebung, installieren Erweiterungen, legen Gruppen und Benutzer an und vieles mehr. Natürlich können Sie auch als Administrator Inhalte und Medien anlegen, doch empfiehlt es sich, für derlei Aufgaben spezielle Redakteur-Accounts anzulegen.

Wenn Sie erste Tests mit dem Content-Managementsystem unternehmen wollen, sei Ihnen das FreeBook „Joomla! Kompakt“ empfohlen, das Sie unter *http://www.brain-media.de/index.php/freebooks.html* herunterladen können.

12.3 Jedem seinen eigenen Blog: WordPress

Eigentlich stammen die Blogs ja aus dem privaten Bereich und erlauben es Internet-Nutzern, ihr Mitteilungsbedürfnis global zu befriedigen. Längst haben auch Firmen den Nutzen dieser Online-Tagebücher für sich erkannt. Gerade unter Marketing-Experten gelten die Blogs als wahre Wunderwaffe. Blogs sind – man kann es an nahezu jeder Ecke im Internet sehen – ein wichtiges Mittel, um Kunden für die eigenen Informationen, Produkte und Dienstleistungen zu interessieren und (im Idealfall) zu binden.

Der Begriff Blog, die Abkürzung für Weblog, entstammt der Wortkreuzung aus den englischen Begriffen World Wide Web und Log für Logbuch. Ein Blog ist nichts anderes als ein online geführtes und damit öffentlich zugängliches Tagebuch. Die Themen sind dabei so bunt und vielfältig wie das Web selbst. Was zunächst als eine einseitige Plattform begann, hat sich inzwischen häufig zu einem Medium für den intensiv geführten Meinungsaustausch entwickelt.

Warum ist dieses Medium nicht nur für Privatpersonen, sondern für Unternehmen und Werbende so interessant? Es sind mehrere Dinge, wobei der Reiz sicherlich im Mix liegt, den man mit keinem anderen Medium so hinbekommt. Ein Online-Tagebuch kann Ihnen beispielsweise helfen, schon vor einer Produkteinführung das Interesse Ihrer Zielgruppe zu wecken. Womöglich kommt sogar Feedback, das Sie in die Produktentwicklung einbringen können.

Sie können auch einen Weblog betreiben, der sich mit Entwicklungen, Einsatzmöglichkeiten und Branchentrends rund um Ihr Angebot beschäftigt. Wenn es Ihnen gelingt, hier brauchbare Informationen zu platzieren, ist es recht einfach, diesen als Standardquelle zu etablieren.

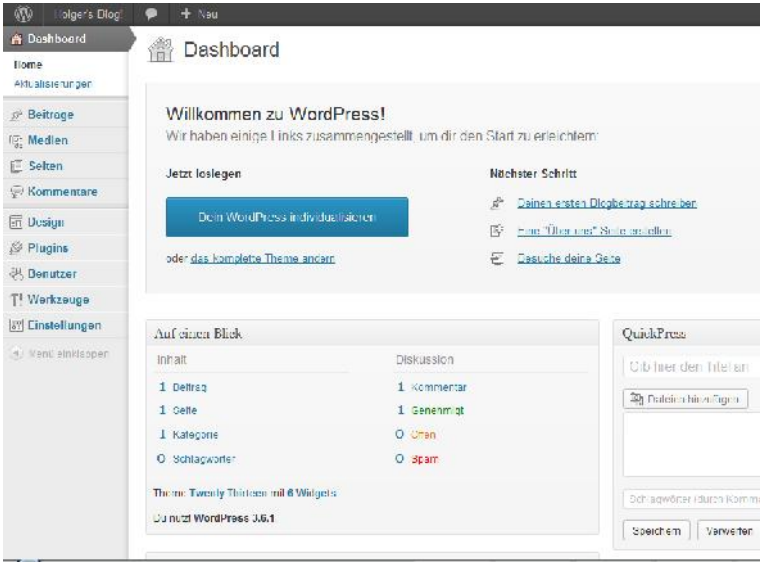
Ein weiterer Pluspunkt: Durch den Einsatz eines Weblogs können Sie sich als modernes Unternehmen positionieren, das auch mit neuesten Techniken umzugehen versteht. Ein Muss ist es ohnehin, wenn Sie eine junge Zielgruppe erreichen wollen, da deren Freizeit- und Konsumverhalten ein Anderes ist.

Als positive Nebeneffekte sind zusätzliche Verlinkungen und Nennungen im Internet immer wichtig, da sie (auch) für ein besseres Ranking in Suchmaschinen verantwortlich sind.

Die wichtigste Lösung für den Betrieb eines eigenen Blogs ist zweifelsohne WordPress. Wie viele andere Web-Lösungen basiert auch WordPress auf PHP und setzt

die MySQL-Datenbank voraus. Es handelt sich dabei letztlich um ein Datenbank-front-end, das die in der Datenbank gespeicherten Informationen verwaltet und für Dritte nutzbar und/oder lesbar macht. WordPress zeichnet sich durch ein hohes Maß an Benutzerfreundlichkeit aus, ist einfach zu installieren, zu konfigurieren und zu warten.

Wenn Sie eine XAMPP-Installation betreiben und darauf eine WordPress-Installation aufsetzen, so bringt das eine ganze Menge Vorteile. Sie sind Herr der Lösung und können alle Einstellungen und Anpassungen vornehmen, die das System zu bieten hat. Sie können nicht nur die Konfiguration Ihren Anforderungen entsprechend anpassen, sondern auch ein Design Ihrer Wahl erzeugen und verwenden. Wenn Sie beispielsweise das Blog-Design an das Ihrer Firmen-Site anpassen wollen, kommen Sie um den Betrieb einer eigenen WordPress-Lösung kaum umhin.



Die Administrationszentrale von WordPress nennt sich Dashboard.

Der Zugriff auf den Blog erfolgt nach der Installation mit dem BitNami-Installer über folgende URL:

```
http://localhost/wordpress/
```

Die Admin-Zentrale über diese URL:

```
http://localhost/wordpress/wp-admin
```

Auch für angehende WordPress-Blogger stellen wir ein FreeBook unter der URL *http://www.brain-media.de/index.php/freebooks.html* zum kostenlosen Download bereit.

12.4 Groupware für alle: Tine 2.0

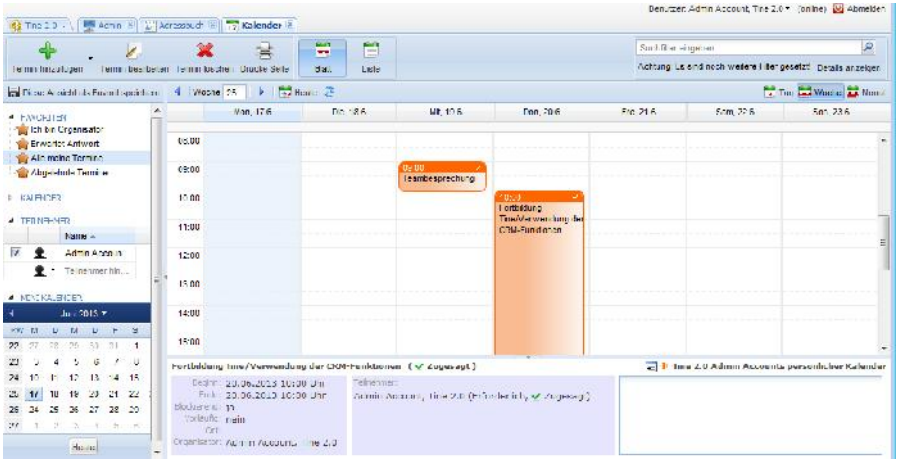
BitNami stellt eine Vielzahl von Web-Applikationen bereit, die heute im kommerziellen und privaten Bereich eine wichtige Rolle spielen, doch längst nicht alle. Eine Ausnahme, die Sie kennen sollten, ist Tine 2.0. Dabei handelt es sich um eine PHP-basierte Open Source-Groupware-Lösung, die die klassischen E-Mail- und Kalenderfunktionen mit bereichsspezifischen Anwendungen kombiniert. Die Umgebung dient der internen Kommunikation und erlaubt das Verwalten von Terminen, Aufgaben und Kontakten für eine Vielzahl von Nutzern. Ergänzt werden diese Grundfunktionen um CRM-, Dateimanager- und sogar Zeiterfassungsmodule.

Das kommt Unternehmen entgegen: Dank der modularen Architektur lässt sich Tine 2.0 an die Anforderungen von Unternehmen anpassen. Je nach Bedarf kann das Grundsystem um Zusatzmodule erweitert oder in bestehende Systeme integriert werden. Als webbasierte Umgebung kann der Zugriff von allen gängigen Geräten erfolgen. Für die Integration und das Zusammenspiel mit bestehenden Infrastrukturkomponenten ist die Verfügbarkeit von Schnittstellen wie WebDAV, CalDAV oder CardDAV von Bedeutung. Im Zeitalter von mobilen Geräten wichtig: Sogar die Synchronisation mit Smartphones gehören zum Standardfunktionsumfang.

12.4.1 Tine 2.0 im Überblick

Auf den ersten Blick ist nicht direkt erkennbar, dass Tine auf eine lange Entwicklungsphase zurückblicken kann. Tine 2.0 ist ein Abkömmling von eGroupWare, das selbst wiederum ein Fork von phpGroupWare ist. Die beiden Vorläufer existieren bereits seit rund 10 Jahren und mehr. So ist es nicht weiter verwunderlich, dass Tine einen beachtlichen Funktionsumfang zu bieten hat. Die Kernfunktionen von Tine 2.0 im Überblick:

- **E-Mail**: Die Grundfunktionalität wird über das E-Mail-Modul sichergestellt, das die direkte Verknüpfung mit dem Adressbuch und der Aufgabenverwaltung bietet.
- **Kalender**: Dank des flexiblen Kalenders vereinfacht sich die unternehmensweite Terminverwaltung und die Abstimmung gemeinsamer Termine.



Ein erster Blick auf die typischen Groupware-Funktionen von Tine 2.0.

- **Adressbuch**: Das Adressbuch kann über die Server-Grenzen hinaus auch externe Mitarbeiter und Kontakte verwalten.
- **Aufgabenverwaltung**: Hier verwalten Sie Aufgaben nach Status und Priorität und arbeiten effizienter mit gemeinsamen Aufgabenlisten.
- **Dateimanager**: Der Zugriff auf zentrale Dateien und Ordner kann über die Weboberfläche oder per WebDAV erfolgen.
- **Zeiterfassung**: Mit diesem Modul führen Mitarbeiter Zeitkonten, deren Daten Sie dann für das Controlling und Rechnungsstellung verwenden können.
- **Customer Relationship Management**: Tine erlaubt Ihnen das Verwalten von Projekten mit Mitarbeiter-, Partner- und Kundeninformationen.

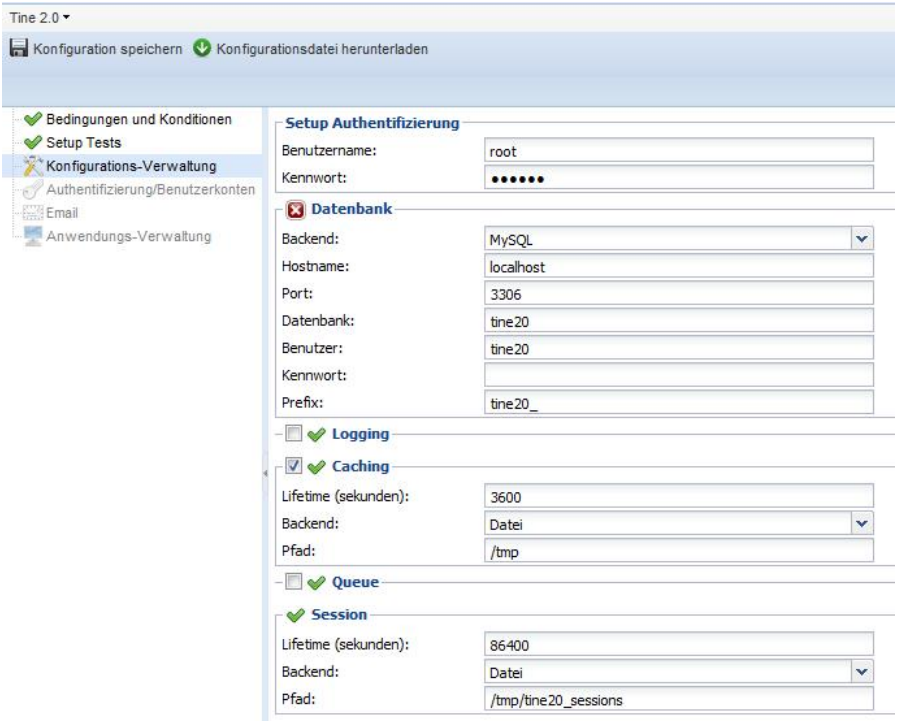
- **Telefonintegration**: Aus dem Adressbuch heraus können Sie Kontakte per Mausklick anrufen. Dabei wird auch eine Anruf-Historie generiert.
- **Suchfunktion**: Die Umgebung verfügt über eine erweiterte Filterfunktion, mit der Sie auch komplexe Suchanfragen durchführen können. Dabei sind die Suchanfragen speicherbar und können bei Bedarf wiederverwendet werden.
- **Dynamische Listenansicht**: In den dynamischen Listen könne Sie Datengruppen unterschiedlichster Größe abbilden. Dieses Modul unterstützt insbesondere den Vertrieb, das Controlling und die Buchhaltung.
- **Benutzerfreundlichkeit**: Die Benutzerfreundlichkeit von Tine 2.0 ist nach ISO 13407 zertifiziert.
- **Logbuch**: Tine 2.0 protokolliert alle Aktivitäten und Änderungen an einem Datensatz automatisch im Logbuch.
- **Rechtevergabe**: Außerdem verfügt die Umgebung über eine flexible Rechtevergabe, mit der Sie exakt steuern, wer Zugriff auf welche Funktionen besitzt.

Für Unternehmen, die über Ländergrenzen hinweg agieren, dürfte die Mehrsprachigkeit ein weiterer Pluspunkt darstellen. Neben den typischen Grundfunktionen wie man sie von klassischen Groupware-Umgebungen kennt, hat Tine 2.0 einige weitere Besonderheiten zu bieten. Sie können beispielsweise alle Daten in Tine verknüpfen, alle Kontakte aus einer bestimmten Stadt kombinieren und alle Leads im CRM-Modul durchsuchen.

Das neu integrierte Personal-Modul ermöglicht außerdem die Verwaltung der wichtigsten Mitarbeiterdaten wie Eintritts- und Austrittsdatum, Anschrift, Kontodaten, Urlaubsansprüche etc. und kann auch die innerbetrieblichen Strukturen abbilden. Damit entwickelt sich Tine von der klassischen Groupware hinzu zu einer flexiblen Groupware-Umgebung mit ERP- und CRM-Funktionen.

12.4.2 Installation und Einrichtung

Für eine derart multifunktionale Umgebung fallen die Systemvoraussetzungen erfreulicherweise sehr bescheiden aus. Alles, was Sie für die Inbetriebnahme und Ausführung der Groupware-Umgebung benötigen, ist eine Apache-MySQL-Installation samt PHP-Komponenten. Über die Projekt-Site stehen auch fertige Installationspakete für Debian-basierte Linux-Server zur Verfügung.



Das webbasierte Setup von Tine – so einfach kann die Einrichtung einer Groupware-Umgebung sein.

Steht bereits eine XAMPP-Installation zur Verfügung, genügt es, das Tine-Archiv in das Dokumentverzeichnis zu entpacken. Optional ist die Installation der VoIP-, Human Ressource- und Inventar-Komponenten.

Haben Sie die Tine 2.0-Komponenten in das Verzeichnis tine auf Ihrem Webserver abgelegt, rufen Sie das Setup über folgende URL auf:

```
http://IP-Adresse-des-Servers/tine/setup.php
```

Das Setup dient der Einrichtung der Tine-Umgebung und dem Zusammenspiel mit den Web- und Datenbankserver. Es umfasst sechs Schritte. In Schritt 1 stimmen Sie der Tine-Lizenz und der Datenschutzvereinbarung zu. Im zweiten Schritt erfolgt ein automatischer Setup-Test, der Ihre Umgebung auf die notwendigen Sys-

temvoraussetzungen hin überprüft. Hier begegnen Sie womöglich folgender Fehlermeldung:

```
Extension fileinfo not found
```

Diese Erweiterung wird optional in Zukunft zur Verwendung kommen. Da Sie das Setup nur mit erfolgreich bestandenem Setup-Test weiterführen können, deaktivieren Sie diesen Test einfach. Entfernen Sie dazu die Voraussetzung *fileinfo* aus der Datei */Setup/essentials.xml*.

Nach erfolgreich bestandenem Setup-Test können Sie sich der Konfigurationsverwaltung zuwenden. Im zugehörigen Formular geben sie den Benutzernamen und das Passwort sowie verschiedene datenbankspezifischen Daten an. Wichtig ist, dass Sie im Bereich Datenbank die korrekte Datenbankbezeichnung angegeben haben. Die Datenbank sollten Sie vor der Ausführung des Tine-Setup anlegen, beispielsweise mit phpMyAdmin. Klicken Sie anschließend auf Konfiguration speichern, um zum vierten Schritt zu gelangen. Hier legen Sie insbesondere den administrativen Tine-Benutzer an.

Im fünften Schritt definieren Sie das Zusammenspiel von Tine 2.0 mit dem E-Mail-Server. Sie können dabei IMAP-, SMTP- und SIEVE-Server einbinden. Der letzte Schritt dient der Aktivierung der verschiedenen Module. Hier aktivieren Sie beispielsweise das Kalender-, das Sales-, das CRM und das ActiveSync-Modul.

Haben Sie alle gewünschten Module im Anwendungsmanager aktiviert bzw. installiert, können Sie sich das erste Mal in Tine 2.0 einloggen. Folgen Sie dazu dem Link Zum Tine 2.0 Login. Melden Sie sich mit dem in Schritt 4 angelegten Admin-Benutzer ein.

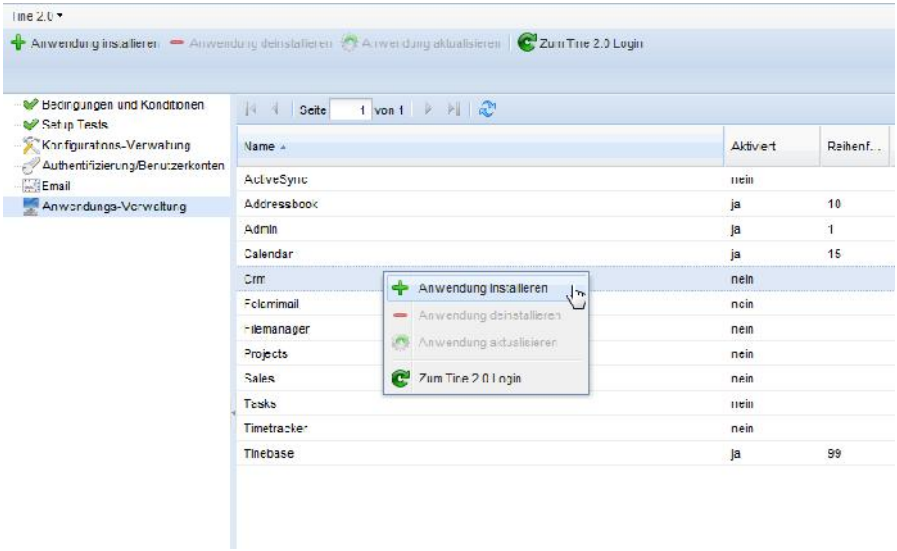
Tine schreibt die Basiskonfiguration in die Konfigurationsdatei *config.inc.php* vor. Bevor Sie sich allerdings ersten administrativen Aufgaben zuwenden, sollten Sie Ihre Tine 2.0-Installation absichern. Der Tine-Ordner muss lediglich für den Benutzer-Account lesbar sein, der den Webserver ausführt. Wenn Sie die config.inc.php über die Web-GUI aktualisieren wollen, dann muss diese Datei die einzige sein, auf die der Webserver-Account schreibenden Zugriff besitzt. Soll sie nur lesbar sein, können Sie die Konfigurationsdatei während des Setup herunterladen, später lokal bearbeiten und dann auf den Webserver überspielen.

12.4.3 Erste administrative Schritte

Nachdem Sie das Basissystem von Tine 2.0 installiert und eingerichtet haben, können Sie sich den ersten administrativen Aufgaben zuwenden. Dazu loggen Sie

sich mit dem administrativen Account ein, klicken auf die Tine 2.0-Registerkarte und wählen dort das Admin-Modul.

Tine öffnet für jeden Funktionsbereich, den Sie öffnen, eine eigene Registerkarte. So stehen für die administrativen Aufgaben ebenso eigene Register wie für das Adressbuch, das CRM- und andere Module zur Verfügung.

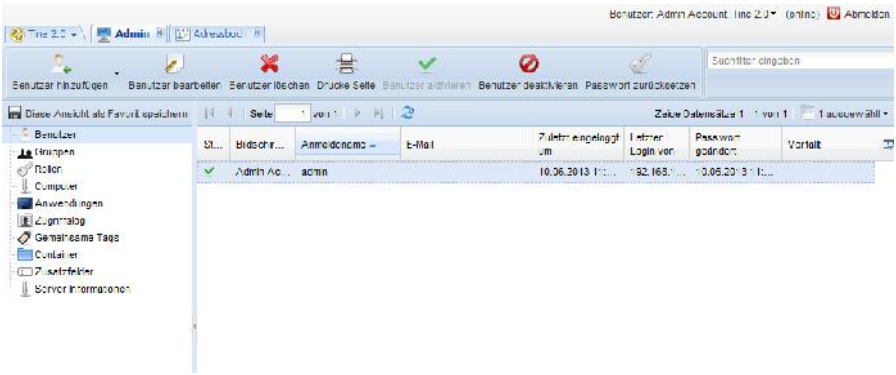


Verschiedene Funktionen wie das CRM-Modul müssen im Setup aktiviert werden.

Eine der zentralen Aufgaben des Tine-Administrators ist die Benutzer- und Gruppenverwaltung. Tine ergänzt diese klassischen Zugriffsmechanismen durch eine Rollen-Funktion. In der Benutzerverwaltung fügen Sie neue Benutzer hinzu, modifizieren, entfernen, aktivieren und deaktivieren Sie Benutzer. Dabei ist jeder User mindestens einer (primären) Gruppe zugeordnet. In der Gruppenverwaltung legen sie Gruppen an, entfernen und bearbeiten diese. Ein Benutzer kann verschiedenen Gruppen angehören.

Über Rollen steuern Sie die Privilegien in der Umgebung. Sie können Gruppen beispielsweise den Zugriff auf das CRM-Modul gewähren, deren Mitarbeiter Zugriff auf diese Informationen für die tägliche Arbeit benötigen. Im zweiten Schritt weisen Sie dieser Rolle dann die gewünschten Gruppen zu. Sie können Tine auch für die Verwaltung von Samba-Shares innerhalb der Umgebung verwenden. In der

Kategorie *Computer* legen Sie die Freigaben an und machen diese für die Tine-Benutzer zugänglich.



Der Zugriff auf die administrativen Funktionen von Tine 2.0.

In der Anwendungen-Kategorie können Sie installierte Module temporär aktivieren und deaktivieren sowie verschiedene Anpassungen vornehmen – sofern verfügbar. Markieren Sie dazu einen Anwendungseintrag mit der rechten Maustaste und passen Sie den Status an oder öffnen Sie Einstellungen mit einem Rechtsklick.

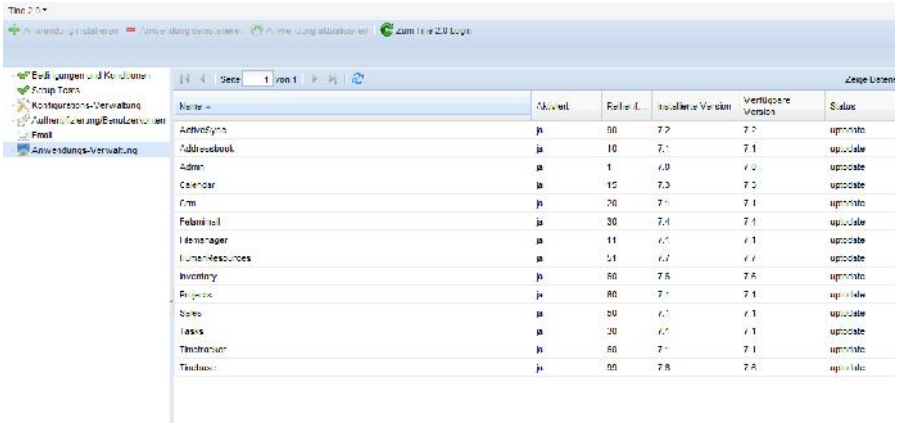
Im Admin-Modul finden Sie auch die Logfile. In der tabellarischen Übersicht können Sie den Account, die IP-Adresse des Clients, den Ein- und Auslogzeitpunkt, das Ergebnis und den Client-Typ entnehmen. Außerdem können Sie die Session-ID einblenden. Mit *Gemeinsame Tags* legen Sie Markierungen an, die Sie allen Benutzern in spezifischen oder allen Anwendungen zur Verfügung stellen können.

Das Admin-Modul hat drei weitere Funktionen zu bieten: Mit Container können Sie spezielle Ablagen anlegen, die beispielsweise nur dem internen Gebrauch dienen. Mit Zusatzfeldern können Sie Tine-Dialoge wie beispielsweise das Adressbuch um zusätzliche weitere Felder erweitern. Schließlich liefert Ihnen Server Informationen die *phpinfo()*-Ausgabe mit allen relevanten Informationen über die Server- und PHP-Umgebung.

12.4.4 Anpassung der Basisumgebung

Tine 2.0 kommt nach der Erstkonfiguration in einer sehr rudimentären Ausstattung daher, bei der lediglich drei Module installiert sind: Neben dem Admin sind das noch das Kalender- und das Tinebase-Modul. Diese sind notwendig für die Aus-

führung von Tine 2.0. In der Praxis sind es aber das E-Mail-, das CRM-, Adressbuch- und das Aufgabenmodul, die die Umgebung unternehmenstauglich machen.



Mithilfe des Setup wurden alle Tine-Module installiert und stehen nun über das Tine-Menü im Backend zur Verfügung.

Um die gewünschten Module nachzuinstallieren, öffnen Sie das Tine-Setup mit der URL *http://IP-Adresse/Tine-Pfad/setup.php* und loggen sich als Setup-User ein. In der Anwendungsverwaltung markieren Sie die Anwendungen mit der rechten Maustaste und führen aus dem Pop-up-Dialog den Befehl Anwendung installieren aus. Sie können auch mehrere Module auf einen Schlag installieren. Halten Sie die Strg-Taste gedrückt, markieren Sie die gewünschten Komponenten und führen Sie den Installieren-Befehl aus. In der Spalte *Hängt ab von* werden relevante Abhängigkeiten aufgeführt. So ist das CRM-Modul nur dann einsetzbar, wenn Sie das Admin-, Adressbuch-, Aufgaben und Sales-Modul eingerichtet haben.

Über die Tine-Projektsite stehen mit HumanResources und dem Inventar-Modul zwei weitere interessante Erweiterungen zur Verfügung. Die Integration dieser beiden Module ist einfach: Entpacken Sie die Archive und kopieren Sie dann die Ordner *Inventory* bzw. *HumanResources* in das Tine-Verzeichnis. Aktualisieren Sie im Anwendungsmanager des Tine-Setup die Ansicht und installieren Sie die Module. Fertig. Anschließend stehen die Module den Anwendern zur Verfügung. Hinter dem HumanResources-Modul verbirgt sich die optionale Zeiterfassung.

Der Zugriff auf die verschiedenen Module erfolgt für alle Benutzer über das Tine-Menü links der Benutzerschnittstelle. Neben den aktivierten bzw. für bestimmte Benutzer verfügbare Module kann jeder Benutzer über das Menü sein Profil bear-

beiten und verschiedene Anpassungen vornehmen. Unter Profil kann er insbesondere seine Kontaktinformationen auf den neuesten Stand bringen. Hinter Einstellungen verbergen sich die Konfigurationen für die Zeitzone, die Sprachversion, die Standardeinstellungen und der Fenstertyp. Für die verschiedenen Module stehen zusätzliche Anpassungsmöglichkeiten zur Verfügung. Sie können beispielsweise beim E-Mail-Modul das Standardkonto und das Abrufintervall anpassen.

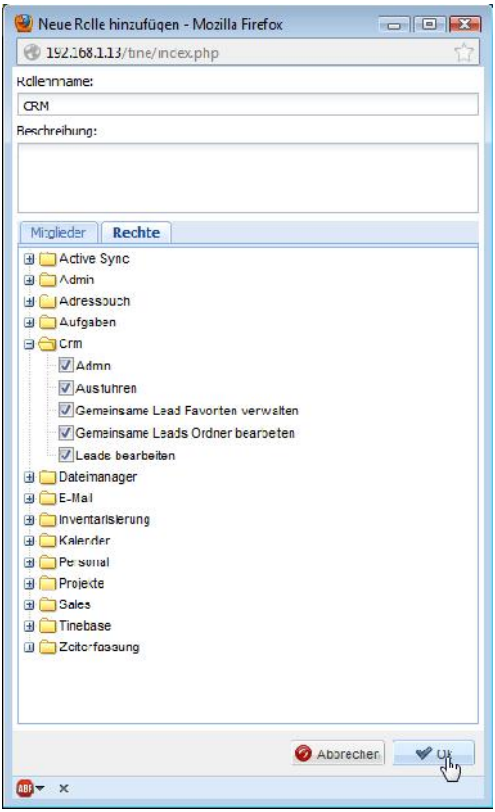
12.4.5 Benutzer, Gruppen und Rollen

Eine der zentralen Aufgaben eines Tine-Administrators ist das Anlegen und Verwalten von Benutzern, Gruppen und Rollen. Während des Setups haben Sie den Speicherort für Ihre Benutzerkonten definiert. Tine 2.0 unterstützt hierfür die Speicherung in der SQL-Datenbank oder per LDAP. Beachten Sie, dass bei einem Wechsel von SQL nach LDAP alle benutzerspezifischen Daten verlorengehen. Über einen MySQL-Datenbankmanager wie phpMyAdmin können Sie natürlich einfach bestehende Benutzerdaten importieren. Tine legt die Daten in den Tabellen *tine20_roles*, *tine20_accounts* und *tine20_groups* ab.

Tine 2.0 ist standardmäßig mit zwei Rollen ausgestattet: der Admin- und der User-Rolle. Während die Admin-Rolle alle verfügbaren Rechte besitzt, können die Benutzer nur aktivierte Anwendungen ausführen. Sie können diese beiden Rollen bearbeiten oder aber über den Admin-Bereich neue Rollen anlegen.

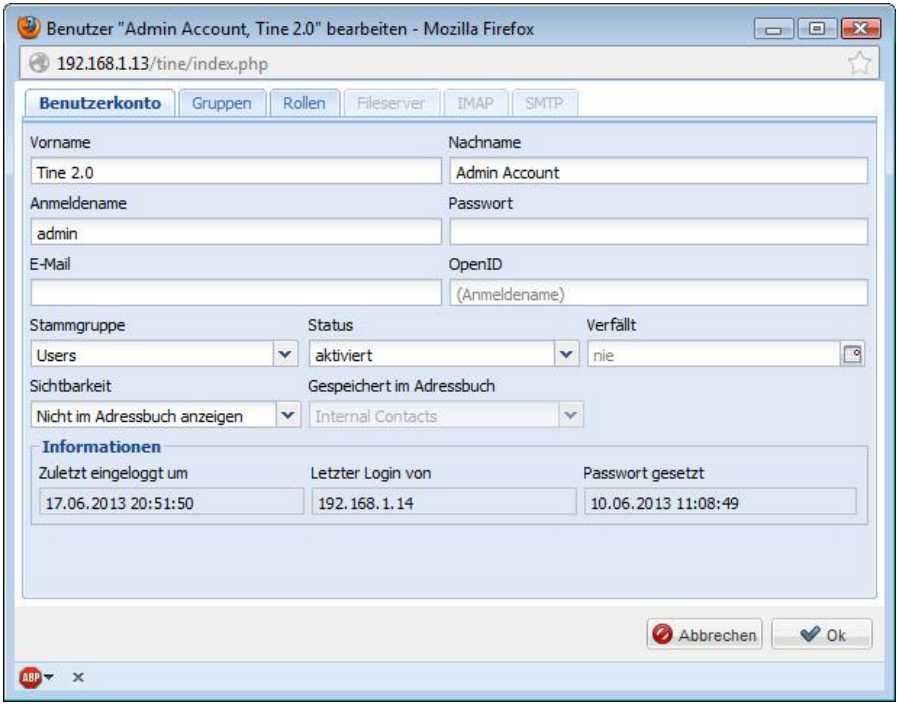
Um eine neue Rolle zu erzeugen, öffnen Sie die Kategorie *Rollen* und klicken auf Rolle hinzufügen. Weisen Sie der Rolle unter *Rollenname* eine Bezeichnung und gegebenenfalls eine Beschreibung zu. Über die Registerkarte *Mitglieder* wählen Sie die Gruppen aus, denen Sie die Rolle zuweisen wollen.

Auf der Registerkarte Rechte werden die verschiedenen Tine 2.0-Module und die jeweils verfügbaren Rechte ausgeführt. Sie können über die Rollenverteilung beispielsweise eine Rolle für die Administration des CRM-Moduls anlegen. Dazu öffnen Sie den CRM-Knoten und aktivieren die CRM-spezifischen Rechte. Entsprechend gehen Sie bei anderen Rollendefinitionen vor. Mithilfe des Rollensystems können Sie Aufgaben in der Umgebung wunderbar delegieren und so beispielsweise Administratoren für bestimmte Abteilungen oder Projekte einrichten.



Das Anlegen einer neuen Rolle: Über die Registerkarte *Rechte* weisen Sie der Rolle für alle aktivierten Module die gewünschten Berechtigungen zu.

Sind die gewünschten Rollen angelegt, können Sie sich im nächsten Schritt den Gruppen und Benutzern zuwenden. Auch das ist dank der Benutzerfreundlichkeit von Tine 2.0 einfach. Um eine neue Gruppe anzulegen, öffnen Sie die Gruppen-Kategorie und klicken auf Gruppe hinzufügen. Hinterlegen Sie den Gruppennamen, eine Beschreibung und bestimmen Sie die Sichtbarkeit innerhalb des Systems. Unter *Gruppenmitglieder* wählen Sie die Benutzer aus, die Sie der Gruppe zuweisen wollen.



Der editierte Benutzereintrag des Tine 2.0-Administrators.

Die Benutzereinstellungen fallen ein wenig umfangreicher aus. Um einen neuen Benutzer anzulegen, öffnen Sie die Benutzerverwaltung und klicken auf Benutzer hinzufügen. Der zugehörige Dialog umfasst mehrere Registerkarten. Auf der Karte Benutzer geben Sie die typischen Kontaktinformationen, den Status, die Stammgruppe und die Sichtbarkeit an. Die Gruppen- und Rollenzugehörigkeit bestimmen Sie auf den entsprechenden Registerkarten. Haben Sie den Datei- IMAP- und SMTP-Server eingerichtet, können Sie dem Benutzer auch den Zuriff auf diese Komponenten erlauben.

Administratoren können über die Benutzerverwaltung einzelne User-Konfigurationen bearbeiten, deren Passwörter zurücksetzen und Accounts deaktivieren.

12.4.6 LDAP- und Outlook-Integration

Outlook ist der Quasi-Standard in Unternehmen, insbesondere bei der Kommunikation innerhalb von Unternehmen. Wenn Sie nun die Evaluierung oder gar die Migration nach Tine 2.0 in Erwägung ziehen, spielt die Verwendung von bestehenden Daten eine wichtige Rolle. Gerade in kleineren Umgebungen verzichtet man gerne auf einen vollwertigen MS Exchange Server, indem man beispielsweise auf eine Lösung wie CodeTwo Public Folders (*http://www.codetwo.de*) setzt. Dann müssen insbesondere bestehende Outlook-Daten in das Tine 2.0-System migriert werden.

Da es keinen nativen Weg für die Migration von Kontakten, Kalendereinträge und Aufgaben gibt, müssen Sie sich eines Spezialisten bedienen: O'Tine (Outlook to Tine, *http://www.nohl.eu/tine-20/otine-outlook-zu-tine-20-migrieren/*). Das Programm liest die Outlook-Daten von der COM-Schnittstelle, übersetzt sie nach JSON-RPC und führt dann einen Upload in das Tine 2.0-System durch.

Die Verwendung erfolgt in drei Schritten. Im ersten Schritt stellen Sie die Verbindung zur Groupware her. Dazu müssen Sie die IP-Adresse, das Protokoll und den Benutzernamen spezifizieren. Im zweiten Schritt liest das Programm die Outlook-Daten ein. Sie können dabei bestimmen, welche Importquellen migriert werden. Abschließend werden die zu importierenden Daten an Tine 2.0 übermittelt. Es versteht sich von selbst, dass das eine gewisse Zeit dauern kann. Anhand der Fortschrittanzeige können Sie die Abarbeitung verfolgen.

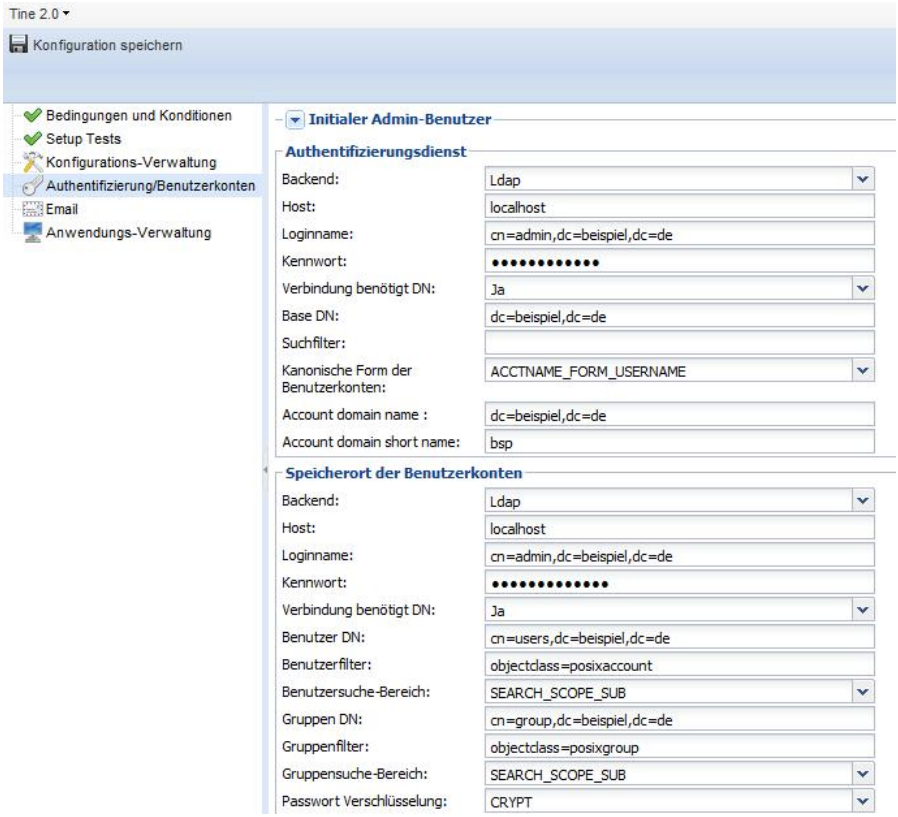
Anstelle der MySQL-basierten Benutzerverwaltung können Sie auch einen bestehenden LDAP-Server integrieren. Tine 2.0 nutzt dabei den Zend Framework LDAP-Adapter, der auch die Authentifizierung per Active Directory-Server unterstützt. Wichtig für das Zusammenspiel mit dem LDAP-Server: Sie müssen den intialen Tine 2.0-Administrator verwenden, nicht den Account des LDAP-Administrators.

Um LDAP als Account-Speicher verwenden zu können, müssen Sie auf Seiten von Tine 2.0 zwei neue Gruppen anlegen: *objectClass* und *posixGroup*. Die Konfiguration des LDAP-Servers erfolgt im Tine-Setup. Dort wählen Sie unter Authentifizierungsdienst und unter *Speicherort* der Benutzerkonten jeweils im Auswahlmenü Backup die Option LDAP. Die minimalen LDAP-Voraussetzungen sehen wie folgt aus:

- ou=user,dc=beispiel,dc=de
- uid=admin (posixAccount,InetOrgPerson)
- ou=groups,dc=beispiel,dc=de
- cn=administrators (posixGroup)

- memberuid=admin
- cn=users (posixGroup)

Beachten Sie dabei, dass die uid-Nummer und die Gruppennamen den LDAP-Einstellungen im Tine 2.0-Setup entsprechen müssen.



Einfach aufzusetzen: Tine 2.0 spielt dank des ZEND LDAP-Apapters zuverlässig mit einem LDAP-Server zusammen, bei Bedarf auch mit einem Active Directory-Server.

12.4.7 Ein starkes Team: Asterisk und Tine

Ein weiteres Highlight von Tine: Tine 2.0 erlaubt die Integration der VoIP-Lösung Asterisk. Sie können die relevanten Informationen von SIP Peers und Voice-Mailboxen in der Tine 2.0-Datenbank speichern. Asterisk wiederum kann auf diese Informationen über das MySQL- oder das CURL-Backend zugreifen. Nach der Asterisk-Integration können aus dem Telefonbuch heraus Anrufe initiiert werden.

Um Asterisk in die Groupware-Umgebung zu integrieren, müssen Sie die Asterisk-Einstellungen in der Tine-Konfigurationsdatei *config.inc.php* hinterlegen. Fügen Sie dazu folgende Konfiguration ein:

```
'asterisk' =>
    array (
        'managerbaseurl' =>
'http://asteriskmanagerhostname.domain:8088/asterisk',
        'managerusername' => 'managerusername',
        'managerpassword' => 'managerpassword',
    ),
```

Um eine Ansicht für Asterisk 1.6 in der Tine 2.0-Datenbank zu generieren, fügen Sie folgenden Code ein:

```
set names utf8;

create view `view_asterisk_sip_peers` AS select
`tine20_asterisk_sip_peers`.*,
`tine20_asterisk_context`.`name` AS `context` from
`tine20_asterisk_sip_peers` join `tine20_asterisk_context` on
`tine20_asterisk_sip_peers`.`context_id` =
`tine20_asterisk_context`.`id`;
```

Erzeugen Sie außerdem einen MySQL-Account für die Telefonie-Applikation, mit dem Sie auf die oben erzeugte Ansicht zugreifen können:

```
grant select,update on DATABASENAME.view_asterisk_sip_peers
to DATABASEUSERNAME@HOSTNAME_ASTERISK_SERVER identified by
'PASSWORT';
```

Als Nächstes muss Asterisk für die Verwendung der MySQL-Datenbank konfiguriert werden. Dazu fügen Sie folgende Zeile zur Asterisk-Konfigurationsdatei */etc/asterisk/res_mysql.conf* hinzu:

```
[general]
dbhost = MYSQL_HOSTNAME
dbname = DATABASENAME
dbuser = DATABASEUSERNAME
dbpass = THESECRETPASSWORD
dbport = 3306
```

Ergänzen Sie dann folgende Zeile zur Asterisk-Konfiguration *etc/asterisk/extconfig.conf*:

```
sippeers =>
MYSQL_HOSTNAME,DATABASENAME,view_asterisk_sip_peers
```

Führen Sie einen Neustart der Asterisk-Konfiguration durch und das Zusammenspiel sollte funktionieren.

Seit Asterisk 1.6 verfügt die Telefonie-Applikation über ein CURL-basiertes Realtime-Backend. Es erlaubt die direkte Kommunikation mit Tine 2.0 über HTTP. In diesem Fall benötigt Asterisk keinen direkten Zugriff auf die Datenbank.

Fügen Sie hierfür zum Abschnitt [*globals*] in der */etc/asterisk/extensions.conf* folgende Zeile hinzu:

```
[globals]
CURLOPT(userpwd)=TINE20USERNAME:TINE20PASSWORD
```

Wichtig ist dabei, dass der verwendete Benutzername und das Passwort vom einem bestehenden Tine 2.0-Account stammen, der Zugriff auf die VoIP-Anwendung besitzt. Ergänzen Sie die Asterisk-Konfiguration */etc/asterisk/extconfig.conf* um folgende Zeilen:

```
sippeers =>
curl,http://TINE20WEBSERVER/index.php?method=Voipmanager_SipP
eers.handleResConfig&action=
```

```
sipregs  =>
curl,http://TINE20WEBSERVER/index.php?method=Voipmanager_SipR
egs.handleResConfig&action=
```

Nach einem erneuten Reload der Asterisk-Konfiguration spielen die beiden Systeme zusammen.

12.4.8 Datenabgleich mit ActiveSync

Im Smartphone-Zeitalter ist der Datenabgleich zwischen einer Umgebung wie Tine 2.0 und den mobilen Endgeräten ein Muss. Dank der ActiveSync-Implementierung in Android kann man von diesen Geräten einfach und zuverlässig mit Exchange-Servern kommunizieren. Da Tine 2.0 ebenfalls ActiveSync-Unterstützung nach dem Aktivieren des entsprechenden Moduls bietet, steht einem Datenabgleich zwischen beiden nichts im Wege.

Nach der Aktivierung des Moduls benötigt Tine lediglich noch eine Weiterleitung der Clients, die in der .htaccess im Tine-Verzeichnis angelegt wird. Nehmen Sie dort folgende Anpassung vor:

```
RewriteEngine on

RewriteRule Microsoft-Server-ActiveSync(.*) index.php$1  \\

[E=ACTIVESYNC:true,E=REMOTE_USER:%{HTTP:Authorization}]
```

Erfolgt der Zugriff auf die Tine 2.0-Umgebung SSL-geschützt, konfigurieren Sie die Weiterleitung von HTTP auf HTTPS wie folgt:

```
RewriteCond %{SERVER_PORT}      !^443$

RewriteRule (.*)  https://%{SERVER_NAME}%{REQUEST_URI}
[R=301,L]
```

Testen Sie als Nächstes die Synchronisation. Um einen ersten Testdurchlauf durchführen zu können, benötigen Sie für die ActiveSync-Konfiguration auf Seiten des Smartphones folgende Daten: Benutzername (exakt wie in der Tine-Benutzerverwaltung hinterlegt), das Passwort, die Server-Adresse und eventuell die E-Mail-Adresse. Das Domain-Eingabefeld können Sie frei lassen.

Unter Android 4.x erfolgt die Aktivierung eines ActiveSync-Kontos in den Geräteeinstellungen mit *Einstellungen* > *Konten* > *Konto hinzufügen* > *Microsoft Ex-*

change ActiveSync. Alternativ können Sie auch eine App wie RoadSync verwenden. Die Groupware-Umgebung kommuniziert natürlich nicht nur mit Android, sondern spielt auch hervorragend mit iPhones und allen anderen ActiveSync-fähigen Endgeräten zusammen.

Tine 2.0 ist nicht nur ein würdiger Nachfolger von eGroupWare, sondern lässt seinen Vorläufer in nahezu allen Belangen alt aussehen. Funktional bietet die Groupware-Umgebung alles, was man in kleinen und mittleren Umgebungen benötigt. Dem Anspruch einer benutzerfreundlichen Umgebung wird die Umgebung hervorragend gerecht. Man darf sich schon jetzt auf den Ausbau der CRM- und ERP-Funktionen freuen.

13 Tipps&Tricks für die tägliche Arbeit

XAMPP ist ein komplexes, wenn auch recht einfach einzusetzendes System. Häufig treten erst in konkreten Einsatzszenarien Probleme auf oder es bieten sich Möglichkeiten, noch mehr aus dem System herauszuholen. In diesem Kapitel stelle ich Ihnen die Tipps und Tricks der XAMPP-Kenner vor.

13.1 Allgemeines

Wenn Sie Ihre XAMPP-Installation eingerichtet haben und womöglich auch eine Anwendung darauf aufsetzen lassen, so will man diese häufig unter realen Bedingungen testen und das lokale XAMPP-System auch aus dem Internet erreichbar machen.

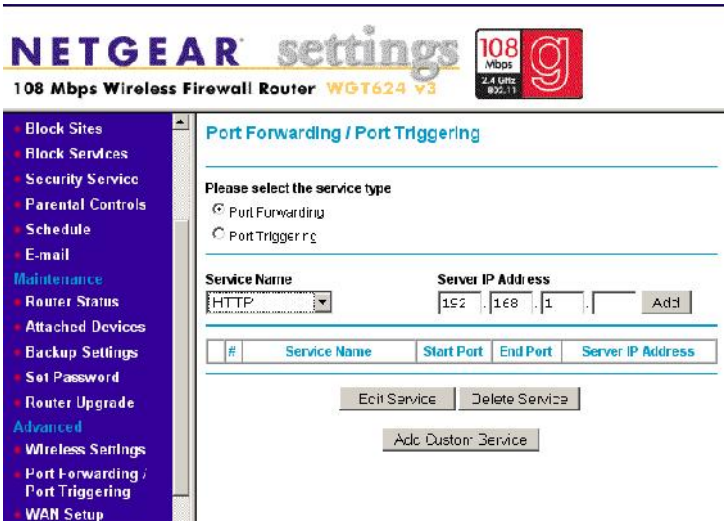
Wenn Sie über eine permanente Internet-Verbindung (nicht über DSL) samt statischer IP-Adresse verfügen, so ist das recht einfach über die sogenannte Port-Weiterleitung (PORTFORWARD) möglich. Sie sorgt dafür, dass die HTTP-Requests auf den Rechner weitergeleitet werden, auf dem Ihre XAMPP-Installation mit eventuell aufsetzender PHP-Anwendung betrieben wird. Das funktioniert natürlich auch in einem lokalen Netzwerk.

Wenn Ihr lokales Netzwerk über einen handelsüblichen Router mit dem Internet verbunden ist, so müssen Sie die jeweiligen Router-Einstellungen so konfigurieren, dass der gewünschte Traffic an das XAMPP-System weitergereicht wird. Da die Einstellungen von Gerät zu Gerät naturgemäß sehr unterschiedlich sind, müssen Sie gegebenenfalls die Gerätedokumentation zurate ziehen.

In diesem Beispiel dient ein Router aus dem Hause Netgear der Außenanbindung. Er agiert auch als lokaler Access-Point für die Anbindung drahtloser Geräte.

Bei diesem Gerät, das über eine Web-Schnittstelle administriert und konfiguriert wird, finden Sie die Port-Weiterleitungsfunktionen im Bereich *Advanced*. Folgen Sie dem Verweis *Port Forwarding/Port Triggering*.

Wählen Sie dann den Typ aus, in unserem Fall ist es *Port Forwarding*. Dann bestimmen Sie den Service, hier HTTP, und geben unter Server IP Address die Adresse des XAMPP-Systems ein. Mit einem Klick auf *Add* ist die erste Weiterleitung aktiviert. Wenn Sie weitere Dienste weiterleiten wollen, so führen Sie die entsprechenden Schritte mit dem jeweiligen Dienst aus.



Die Konfiguration der Port-Weiterleitung bei einem handelsüblichen Router.

In der Regel erzeugt man meist folgende Weiterleitungen:

- TCP-Port 80 (HTTP) für das XAMPP-System mit seinem Apache.
- TCP-Port 21 für FTP-Zugriff.
- TCP-Port 3306, falls Sie den Zugriff auf MySQL gestatten wollen.
- TCP-Port 143 für den IMAP-Zugang.
- TCP-Port 25 für den SMTP-Server.
- TCP-Port 110 für den POP3-Mailserver.

Beachten Sie, dass Port Forwarding gelegentlich auch mal als Port Redirection oder NAT-Konfiguration bezeichnet wird. Der verwendete Begriff variiert von Hersteller zu Hersteller.

Beachten Sie in solchen Fällen, dass Sie den oder die notwendigen Ports auf Ihrer Firewall freischalten, damit die Verbindung nicht abgelehnt wird.

Sie können natürlich auch die Startseite des Systems ändern. Die Dokumente einer XAMPP-Installation liegen im Ordner */xampp/htdocs*. Die Datei *index.html* ist die Standard-Startseite des Systems, die beim Aufruf von *http://localhost* initialisiert wird.

Es steht Ihnen frei, diese zu löschen und durch eine eigene Seite zu ersetzen. Die Hierarchie der Index-Seiten sieht unter XAMPP übrigens wie folgt aus:

- index.php
- index.php4
- index.php3
- index.cgi
- index.pl
- index.html
- index.htm
- index.html.var
- index.phtml

Diese Einstellungen lassen sich über die Apache-Konfigurationsdatei gegebenenfalls ändern.

13.2 Tipps für Linux-Anwender

Wenn Sie vorzugsweise mit Linux arbeiten, so gibt es eine Vielzahl von Kniffen, mit denen Sie sich das Arbeiten mit XAMPP vereinfachen können. Die beliebtesten Tipps stelle ich Ihnen in diesem Abschnitt vor.

13.2.1 Hinweise zum Starten

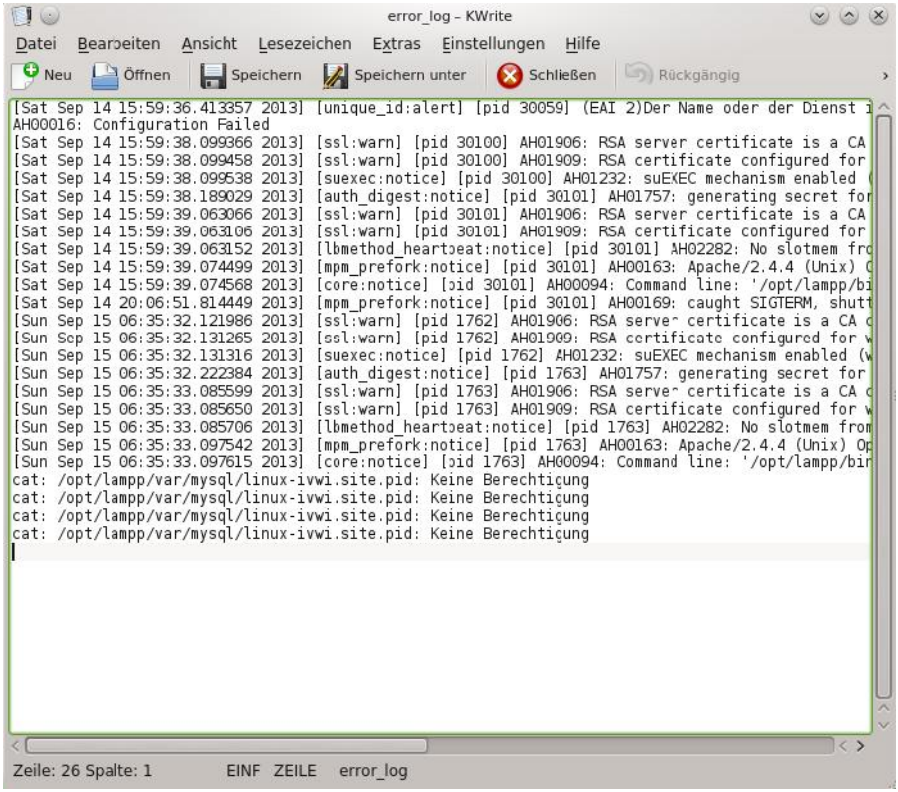
Beim Starten gibt es immer wieder Probleme oder Ungereimtheiten, die manchen Anwendern zu schaffen machen. Etwa, wenn Ihnen beim Start folgende Meldung ausgegeben wird:

```
LAMPP: Ein Apache läuft bereits.
```

In diesem Fall hat das XAMPP-Start-Programm erkannt, dass bereits ein Web-Server auf Port 80 des Systems ausgeführt wird. Womöglich haben Sie vor der XAMPP-Installation einen Apache oder einen anderen Server auf Ihrem System in Betrieb genommen.

Eine ähnliche Meldung kann auch im Zusammenhang mit dem MySQL-Datenbankserver ausgegeben werden:

```
LAMPP: Ein MySQL läuft bereits.
```



Die Fehlerprotokolldatei gibt eventuell Aufschluss über einen aufgetretenen Fehler.

Gelegentlich tritt bei der Ausführung des Systems der Fehler 1 bzw. Error 1 auf. Für diesen Fehler kann es mehrere Ursachen geben. Der nachstehende Befehl hilft Ihnen, der Ursache auf die Spur zu kommen:

```
tail -2 /opt/lampp/logs/error_log
```

Dieser Befehl gibt die letzten beiden Zeilen der Protokolldatei aus. Prüfen Sie die Ausgabe auf eine mögliche Antwort auf Ihr Problem. Unter Umständen hilft auch ein direkter Blick in die Fehlerprotokolldatei */opt/lampp/logs/error_log*.

Ein Problem kann auch die fehlende Zuordnung von Rechnername und IP-Adresse des Systems darstellen. In einem solchen Fall wird eine Fehlermeldung wie die folgende ausgegeben:

```
Invalid argument: Configuration failed
```

Zur Behebung des Konfigurationsfehlers verwenden Sie folgenden Befehl:

```
echo 127.0.0.1 `hostname` >> /etc/hosts
```

13.2.2 Betrieb von XAMPP

Linux ist, was die automatische Ausführung von zusätzlichen Diensten betrifft, weitaus zurückhaltender als Windows – aus gutem Grund. Unter Linux müssen Sie als Administrator selbst Hand anlegen und dafür sorgen, dass ein Dienst wie XAMPP auch beim nächsten Systemstart automatisch geladen wird.

Die typische Vorgehensweise sieht wie folgt aus. Zunächst müssen Sie herausfinden, welchen Standard-Runlevel Ihr Linux-System besitzt. Das gelingt mit folgendem Befehl:

```
egrep :initdefault: /etc/inittab
```

Eine typische Ausgabe zeigt an, dass es sich um einen Runlevel von 3 oder 5 handelt. Hier ein Beispiel:

```
id:5:initdefault:
```

Wechseln Sie als Nächstes in das Verzeichnis, das diesen Runlevel konfiguriert. Für den Runlevel 3 ist das beispielsweise */etc/rc.d/rc3.d*, für Runlevel 5 entsprechend */etc/rc.d/rc5.d*.

Um die Konfiguration anzupassen, führen Sie folgende Befehle aus:

```
ln -s /opt/lampp/lampp S99lampp
ln -s /opt/lampp/lampp K01lampp
```

Ab sofort wird XAMPP bei jedem Neustart Ihres Linux-Systems ebenfalls gestartet.

Neben MySQL und SQLite können Sie auch mit anderen Datenbanken arbeiten. Sie sind keineswegs nur an diese beiden gebunden. Wenn Sie mit einer Oracle-Datenbank arbeiten wollen, so können Sie die OCI8/Oracle-PHP-Erweiterung einfach mit folgendem Kommando aktivieren:

```
/opt/lampp/lampp oci8
```

Ein einfacher Dialog verlangt von Ihnen die Pfadangabe zur Oracle-Installation. Hier eine typische Ausgabe:

```
Please enter the path to your Oracle installation:
ORA_HOME [/opt/oracle]
installing symlinks...
patching php.ini...
PHP-OCI8-Aktivierung wahrscheinlich erfolgreich.
LAMPP: Stoppe Apache mit SSL...
LAMPP: Starte Apache mit SSL...
```

Datensicherheit ist natürlich bei relevanten Daten großzuschreiben. Im Kapitel Sicherheit haben Sie eine Möglichkeit kennengelernt, wie Sie Ihre Datenbankdaten sichern können.

Die Linux-Variante von XAMPP verfügt über einen weiteren Mechanismus: ein Back-up-Skript. Es ist erst seit XAMPP für Linux 1.4.2 integriert und sollte daher mit der gebotenen Vorsicht verwendet werden.

Das Erstellen eines Back-ups ist simpel. Führen Sie einfach folgenden Befehl aus:

```
/opt/lampp/lampp backup
```

Wenn Ihr MySQL-System durch ein Passwort geschützt ist – und das sollte es –, verwenden Sie folgenden Befehl:

```
/opt/lampp/lampp backup passwort
```

Dabei gibt *passwort* das MySQL-Passwort des Root-Benutzers an.

Das Back-up-Skript erzeugt etwa folgende Ausgabe:

```
# /opt/lampp/lampp backup
Backing up databases...
Backing up configuration, log and htdocs files...
Calculating checksums...
Building final backup file...
Backup finished.
Take care of /opt/lampp/backup/xampp-backup-17-09-13.sh
```

Die Sicherungsdatei */opt/lampp/backup/xampp-backup-datum.sh* beinhaltet die gesicherten Daten Ihres XAMPP-Systems. Sie muss auf einem Dritt-Medium oder -Rechner gespeichert werden, damit man von einer echten Sicherung sprechen kann.

Das Wiederherstellen ist ebenfalls recht einfach. Führen Sie dazu als Root-User folgenden Befehl aus:

```
sh xampp-backup-10-10-10.sh
```

Die zugehörige Ausgabe sieht dann in etwa wie folgt aus:

```
# sh xampp-backup-10-10-10.sh
Checking integrity of files...
Restoring configuration, log and htdocs files...
Checking versions...
Installed: XAMPP 1.7.3
Backup from: XAMPP 1.7.3
Restoring MySQL databases...
```

```
Restoring MySQL user databases...
Backup complete. Have fun!
You may need to restart XAMPP to complete the restore.
```

Alternativ können Sie natürlich auch andere Sicherungsfunktionen Ihres Linux-Systems verwenden. So fortschrittliche Funktionen wie ein inkrementelles Back-up etc. hat das XAMPP-Back-up-Skript nicht zu bieten.

13.3 Windows-spezifische Kniffe

Wenn Sie mit XAMPP für Windows arbeiten, so warten naturgemäß andere Probleme auf Sie. In diesem Abschnitt stelle ich Ihnen die besten Tipps und Problemlösungen für die Windows-Variante vor.

13.3.1 XAMPP für die Westentasche

Tools für die Westentasche haben momentan Hochkonjunktur, denn Sie erlauben es, Anwendungen immer und überall verwenden zu können. Auch XAMPP ist für derlei Aufgaben und Anwendungen gerüstet. Sie können XAMPP problemlos auf einem USB-Stick mitnehmen und so an anderer Stelle mit minimalem Aufwand einen voll funktionstüchtigen Webserver aus der Tasche, genauer dem Stick, zaubern. Der Stick sollte zumindest über 512 MB Speicherplatz verfügen, denn das gesamte entpackte XAMPP-System belegt bereits alleine ca. 250 MB Speicherplatz.

Wenn Sie auf bestimmte Anwendungen verzichten können, tut es auch XAMPP Lite, das Sie unter *http://portableapps.com/apps/development/xampp* finden. XAMPP Lite ist wesentlich platzsparender und passt schon auf einen „kleinen" USB-Stick, denn die abgespeckte Variante benötigt lediglich ca. 150 MB Speicherplatz.

Eine Installation im herkömmlichen Sinne ist nicht erforderlich. Laden Sie sich einfach das Paket herunter, entpacken Sie es und kopieren Sie es auf den Stick. Mit dem einzigen Nachteil von XAMPP Lite werden Sie vermutlich leben können: Diese Variante wird nicht so häufig aktualisiert. Um aber mal eben eine Präsentation einer eigenen Entwicklung durchzuführen oder vergleichbare Aktionen, ist XAMPP Lite bestens geeignet.

13.3.2 Probleme mit dem Windows XP SP 2

Das Windows XP Service Pack macht so mancher XAMPP-Installation das Leben schwer, denn sie blockiert durch die „verbesserte“ Firewall-Funktionalität – leider ungefragt – den Zugriff auf das System. Das Service Pack 2, kurz SP2, blockiert insbesondere die wichtigen Ports 80 (http) und 443 (https).

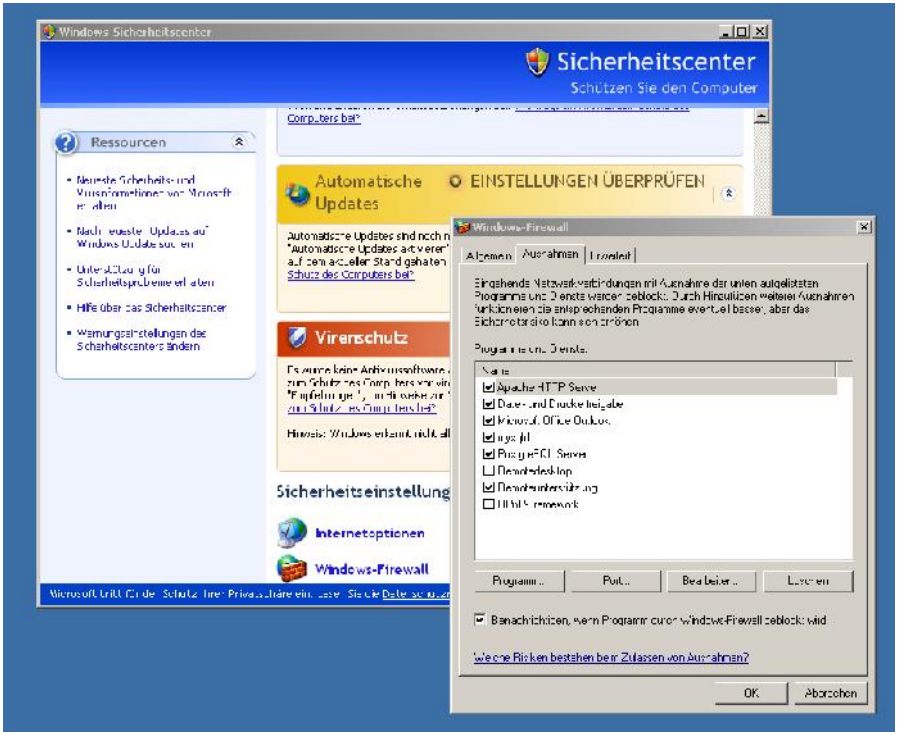
Die Lösung ist recht einfach: Deaktivieren Sie die Microsoft Firewall über die Taskleiste oder definieren Sie im Sicherheitscenter die für Ihren Anwendungsbereich notwendigen Ausnahmen.

Für die XAMPP-Grundfunktionen werden folgende Ports benötigt:

- 80 (HTTP)
- 443 (SSL)
- 3306 (MySQL)

Wenn Sie darüber hinaus weitere Server nutzen sollten, müssen diese ebenfalls freigeschaltet werden:

- 21 (FTP)
- 25 (SMTP)
- 110 (POP3)
- 143 (IMAP)
- 8009 (AJP/1.3)
- 8080 (Tomcat)



Über das Windows-XP-Sicherheitscenter öffnen Sie die notwendigen Firewall-Ports.

13.3.3 Probleme mit Vista

Wenn Sie zu den Anwendern gehören, die mit Windows Vista arbeiten, so warten zwei neue Probleme auf Sie. Das Erste wird durch den sogenannten Benutzerkontenschutz verursacht, das Zweite durch das fiktive Programme-Verzeichnis.

Der Benutzerkontenschutz trägt im Englischen die Bezeichnung UAC (User Account Control). Das wichtigste Ziel von UAC war die Reduzierung der Angriffsfläche des Betriebssystems. Dazu arbeiten alle Benutzer als Standardbenutzer. Der administrative Zugriff ist auf autorisierte Prozesse eingeschränkt. Diese Einschränkung minimiert die Möglichkeiten der Benutzer, Änderungen vorzunehmen, die sich auf die Stabilität des Computers auswirken können oder den Computer versehentlich für Maleware oder Viren anfällig machen. Diesen Mechanismus kennen Linux-Anwender natürlich.

An sich ist es ja schon ein wenig verwunderlich, dass Microsoft hier eine altbekannte Technik in sein Betriebssystem übernimmt. In der Praxis tauchen allerdings Probleme meist nach der Installation einer Anwendung auf. Ursache ist dabei häufig der neue Benutzerkontenschutz von Vista. Konkret fehlt es den Anwendungen oft an den erforderlichen Schreibrechten.

Die Lösung hier ist indes recht einfach: Entweder erweitern Sie die Schreibrechte für das Verzeichnis über den Explorer mit einem Rechtsklick und der Bearbeitung der Sicherheitseinstellungen oder aber Sie schalten den Benutzerkontenschutz komplett ab.

Der Benutzerkontenschutz wirkt sich auch auf Dienste und Programme aus, die Sie über das XAMPP Control Panel aufrufen wollen. So kann es passieren, dass Sie Apache und MySQL als Dienst installiert haben, aber über das Control Panel weder die Anwendungen anhalten bzw. starten, noch die Dienste entfernen können. In diesem Fall kommen Sie mit der Dienste-Verwaltung von Windows weiter, auf die Sie über *Start > Systemsteuerung > Verwaltung > Dienste* zugreifen.

Sie können für das Deaktivieren der Benutzerkontensteuerung das Programm msconfig verwenden, das Sie über *Start > Ausführen > msconfig* starten.

Ein weiteres Problem für Ihre XAMPP-Installation stellt das fehlende Programme-Verzeichnis dar. Der Windows Explorer gaukelt Ihnen zwar einen Programme-Ordner vor, doch eigentlich handelt es sich dabei um das Verzeichnis *program files*. Probleme ergeben sich dabei insbesondere durch fehlerhafte Verweise, beispielsweise zu Konfigurationsdateien.

So präsentiert Ihnen der Explorer beispielsweise das Apache2-Verzeichnis unter *C:\Programme\apache2*, tatsächlich ist es aber unter *C:\program files\apache2* zu finden. Wenn der Webserver nun versucht, eine Konfiguration aus der Konfigurationsdatei *C:\Programme\apache2\conf\httpd.conf* zu laden, die ja nicht existiert, so führt das unweigerlich zu einem Fehler (*httpd.conf not found*).

Wenn Sie derlei Fehlermeldungen erhalten, sollten Sie die Pfade zu den entsprechenden Konfigurationsdateien suchen und gegebenenfalls korrigieren.

13.3.4 Tomcat

Inzwischen gehört auch das Tomcat-Modul zur XAMPP-Grundausstattung. Was kann man nun mit dieser Server-Komponente anfangen? Die Antwort: sehr viel, man muss nur wissen, was. Anhand eines Beispiels wird das deutlich.

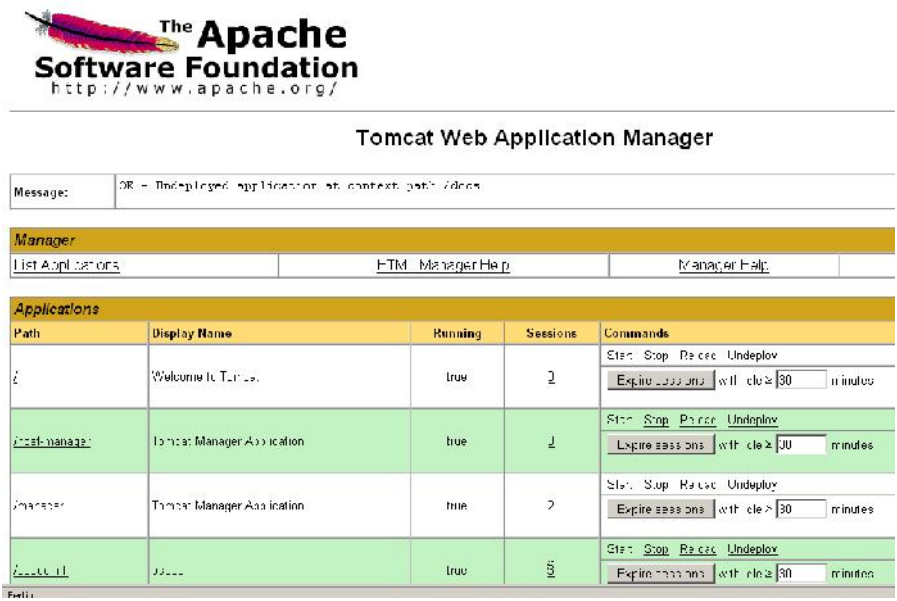
Momentan gibt es mit osSEO (*http://osseo.wiki.sourceforge.net*) endlich wieder ein vielversprechendes Werkzeug, das sich an der Suchmaschinenoptimierung versucht. Es unterstützt Sie dabei, in Suchmaschinen ein besseres Ranking zu er-

reichen und somit Besucher anzuziehen. Bei osSEO handelt es sich dabei um eine Java-basierte Lösung, die auf einem Tomcat-Server (*http://tomcat.apache.org*) aufsetzt.

osSEO unterstützt lediglich die sogenannte White hat SEO. Darunter versteht man die „ethische Suchmaschinenoptimierung“. Als ethisch wird die Suchmaschinenoptimierung bezeichnet, die sich an die Vorschriften der Suchmaschinen hält. Zu den Methoden, nach denen die White hat SEO arbeitet, gehören beispielsweise die folgenden:

- Legale OnPage-Optimierung durch hochqualitative Contents (Seiteninhalte).
- Quellcodegestaltung nach den Bestimmungen der Suchmaschinen.
- Durchführung von regelmäßigen Analysen der aktuellen Rankings mit dem Ziel, bei Bedarf neue Optimierungsschritte vorzunehmen.

Um osSEO ausführen zu können, müssen Sie auf Ihrem System zunächst eine JDK6- und Tomcat6-Installation aufsetzen. Dazu eignet sich das Tomcat-Add-on. Nach der Installation können Sie über den sogenannten Tomcat-Application-Manager die osSEO-WAR-Datei installieren. Dazu wechseln Sie zum Bereich *Deploy*, suchen die WAR-Datei und führen einen Upload mit einem Klick auf *Deploy* aus. Nach der erfolgreichen Installation finden Sie osSEO in der Liste der verfügbaren Tomcat-Anwendungen.

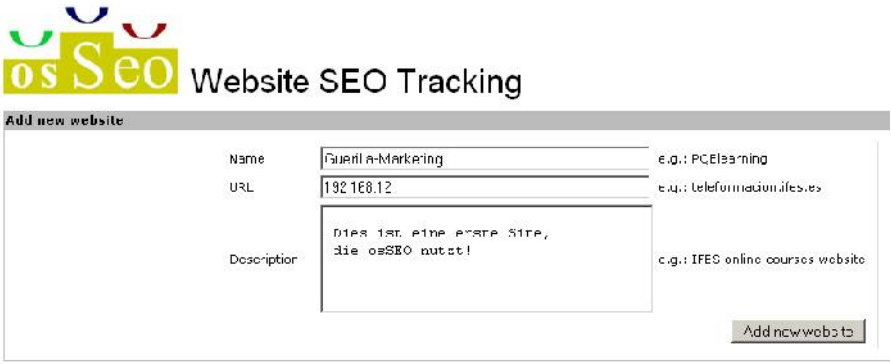


Der Tomcat-Application-Manager zeigt die Verfügbarkeit und die Ausführung von osSEO an.

Der Tomcat-Anwendungsmanager zeigt neben der Anwendungsbezeichnung auch deren Status und die Anzahl der Sessions an. Über die *Commands*-Spalte können Sie die Anwendung anhalten, beenden, neu laden und entfernen. Der Zugriff erfolgt auf die jeweilige Anwendung am Einfachsten über den Path-Link.

In unserem Fall klicken Sie auf den Anwendungseintrag *osseo-intl* und Sie landen im ersten Dialog von osSEO. Die URL lautet dann *http://localost_bzw_ip-adresse/osseo-intl/*.

Beim ersten Zugriff meldet sich der Dialog zum Hinzufügen einer neuen Website, deren Daten in Zukunft an wichtige Suchmaschinen übergeben werden sollen. Auf dem ersten Dialog finden Sie außerdem den Link *Manage Websites*, über den Sie auf die Liste der bereits erzeugten Einträge zugreifen und weitere Sites eintragen können.



Eine erste Website wird angelegt, deren Daten osSEO verwaltet.

Mit einem Klick auf *Add new website* landen Sie im ersten Keyphrase-Dialog, den Sie mit einer Phrase füttern, die Ihre Website beschreibt.

Die Eingabe einer ersten Keyphrase.

Über die Schaltfläche *Add new keyphrase* speichern Sie die erste Phrase. Sie können und sollten natürlich Weitere hinzufügen.

Die erste Site ist eingetragen. osSEO füttert nun die Suchmaschinen mit den Site-relevanten Informationen.

Mit einem Klick auf *Manage website* gelangen Sie zur Liste der Sites, die osSEO verwaltet (siehe voranstehende Abbildung). Wenn Ihr System über eine permanente Internet-Verbindung verfügt, werden in Zukunft drei wichtige Suchmaschinen mit den Site-relevanten Daten gespeist.

osSEO erzeugt auf Grundlage der von Ihnen hinterlegten Daten und der Rückgabe der Suchmaschinen Berichte, die Ihnen anzeigen, wie es mit Ihrem Suchmaschinen-Ranking aussieht. Aktuell unterstützt osSEO lediglich drei Suchmaschinen:

- Google
- MSN
- Yahoo

Sie können allerdings auch Weitere einführen, wenn eine spezifische Suchmaschine für Sie von besonderer Bedeutung ist. Dazu müssen Sie einen XML-basierten Suchmaschinen-Deskriptor erzeugen. Der sieht im Falle von Google wie folgt aus:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE searchEngine PUBLIC "SYSTEM" "searchEngine.dtd">
<!-- XML representation of a SearchEngine. See
es.f2020.osseo.domain.SearchEngine -->
<searchEngine>
      <domain>google.com</domain>
      <name>Google</name>
      <description>Google</description>
```

```
        <color>FFBB33</color>
        <crawler>

        <searchUrl>http://www.google.com/search?q=KEYPHRASE</se
archUrl>
                <additional-
PagesSearchUrl>http://www.google.com/search?q=KEYPHRASE&amp;s
tart=START</additionalPagesSearchUrl>
                <additionalPagesStartOffset>-
1</additionalPagesStartOffset>
                <notIndexedToken>class=j</notIndexedToken>
                <splitResultsToken>class=r</splitResultsToken>
                <site-
SearchUrl>http://www.google.com/search?as_q=KEYPHRASE&amp;as_
sitesearch=SITEURL</siteSearchUrl>
        </crawler>
</searchEngine>
```

Beispiel für eine Berichtausgabe (Quelle: osSEO-Team).

osSEO kommuniziert standardmäßig jede Nacht mit den drei hinterlegten Suchmaschinen. Den Berichten, die osSEO erzeugt, können Sie den zeitlichen Verlauf Ihrer Aktionen und die Position Ihrer Phrasen entnehmen. Im Idealfall ist eine Steigerung der Platzierung zu verzeichnen. Wie Sie voranstehendem Beispielbericht entnehmen können, präsentiert Ihnen das Tool zu jeder Phrase die Ergebnisse samt Tagesplatzierung und grafischer Auswertung der Position.

Außerdem werden die Ergebnisse farblich gekennzeichnet:

- **Grün**: Diese Markierung steht für eine hervorragende Platzierung. Das Ergebnis findet sich unter den ersten zehn und damit meist auf der ersten Ausgabeseite der Suchmaschine.
- **Blau**: Diese Kennzeichnung zeigt eine mittelmäßige Platzierung an. Ihre Website wird unter den ersten 100 Websites geführt.
- **Rot**: Diese Kennzeichnung verwendet osSEO für verschiedene Zustände. Meist für eine Platzierung auf Rang 101 oder höher. Alternativ kann Ihre Site auch nicht für den verwendeten Begriff indiziert sein. Schließlich kann es auch daran liegen, dass die Suchmaschinen noch nicht abgefragt wurden.
- **Grau**: Die graue Markierung wird verwendet, wenn für den aktuellen Tag noch kein Ergebnis vorliegt und osSEO daher das des Vortags verwendet.

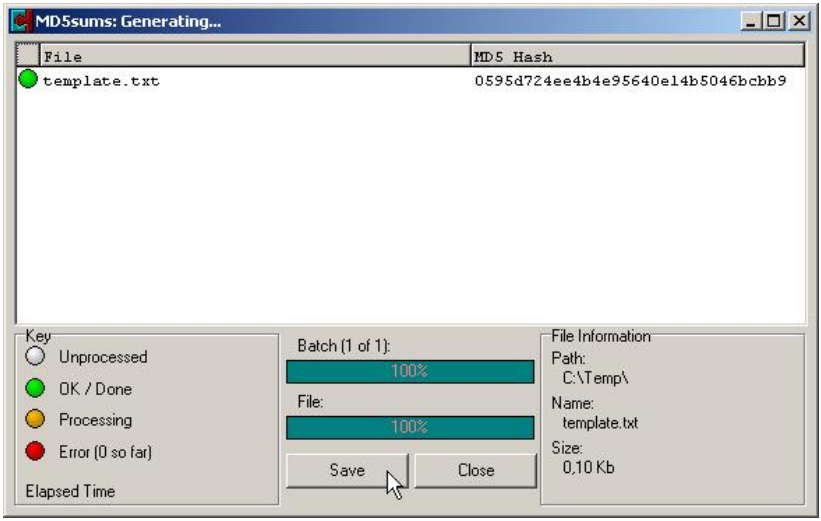
Insgesamt stellt osSEO ein sehr interessantes Werkzeug dar, von dessen Weiterentwicklung sich Marketingspezialisten noch Einiges erwarten dürfen. Bleibt zu hoffen, dass dieses Projekt nicht einschläft. Die Anfänge sind sehr vielversprechend.

13.3.5 MD5-Prüfsumme prüfen und erstellen

Eine gängige Methode, um die Integrität von Dateien sicherzustellen, ist die Verwendung von MD5-Prüfsummen. Auch für die über die Apachefriends-Website verfügbaren Downloads sind MD5-Prüfsummen verfügbar. Wenn Sie Dateien aus dem Netz herunterladen oder selbst welche anbieten, sollten Sie möglichst die Originalität prüfen bzw. eigene Downloads mit einer Prüfsumme versehen, damit Dritte sicherstellen können, dass die Daten nicht manipuliert wurden.

Linux-Anwender sind hier wieder im Vorteil, denn sie finden auf ihren Systemen die notwendigen Tools zum Erstellen bzw. Prüfen von MD5-Prüfsummen.

Doch das ist kein Problem, denn mit dem MD5Summer (*http://www.md5summer.org*) steht Ihnen ein frei erhältliches Werkzeug zur Verfügung, mit dem Sie MD5-Summen erstellen und prüfen können. MD5Summer ist eine Anwendung für Windows 9x, ME, NT, 2000 und XP. Es unterliegt der GPL und ist somit kostenfrei einsetzbar. Es kommt mit einer kompakten grafischen Oberfläche daher, die die Anwendung einfach macht.



Der MD5Summer hat für eine Datei eine Prüfsumme erstellt.

13.3.6 Änderungen an der php.ini greifen nicht

Wenn Sie Änderungen an der *php.ini*-Datei vorgenommen haben (wie Sie beispielsweise zur Ausführung von eGroupWare womöglich erforderlich sind), so scheint es, dass diese einfach nicht greifen.

Das kann mehrere Gründe haben. Beachten Sie zunächst, dass die aktive *php.ini* immer unter *xampp\apache\bin* zu finden ist, und zwar dort, wo sich auch die *apache.exe* befindet.

Und noch ein letzter Hinweis: Änderungen an der *php.ini* und der *httpd.conf* erfordern immer einen Neustart des Apache-Webservers.

13.3.7 Kein Speicherplatz im Umgebungsbereich

Bei den verschiedenen Windows-Homesystemen kann es zu der Fehlermeldung kommen, dass kein ausreichender Speicherplatz im Umgebungsbereich verfügbar ist. Die Ursache für dieses Problem ist die miserable Speicherverwaltung der Windows-Homesysteme. Sie lässt Anwendungen über die Datei *command.com* von höchstens 160 KB zu. Verschiedene Server benötigen aber gelegentlich mehr.

Die Lösung dieses Problems ist recht einfach: Erweitern Sie einfach die *c:\config.sys* um folgende Zeile:

```
shell=c:\windows\command.com c:\windows /e:2048 /p
```

Diese Konfiguration sorgt dafür, dass ab dem nächsten Neustart der Speicher bis auf 2048 KB genutzt werden kann. Dieser Wert sollte in der Regel ausreichen.

13.3.8 Apache startet nicht

Wenn der Apache unter XAMPP für Windows nicht startet, so kann das mehrere Gründe haben. Eine mögliche Ursache ist, dass Sie einen anderen Webserver wie beispielsweise den Internet Information Server oder den Sambar Webserver parallel gestartet haben. Es versteht sich von selbst, dass immer nur ein Webserver den Port 80 belegen kann.

Die beiden folgenden Fehlermeldungen des Apache unter Windows deuten darauf hin, dass das der Fall ist:

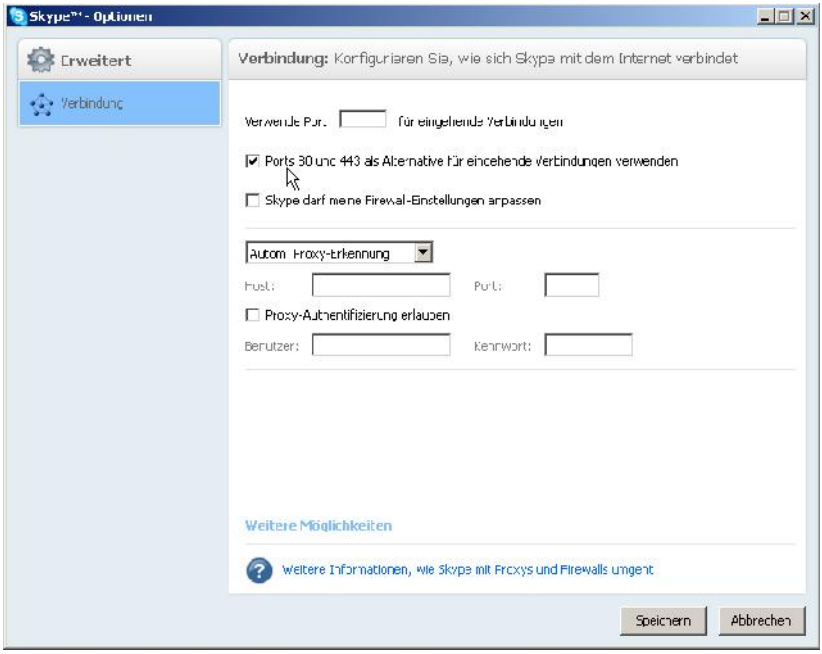
```
(OS 10048)... make_sock: could not bind to adress 0.0.0.0:85
no listening sockets available, shutting down
```

```
(OS 10038)Socket operation on non-socket: make
_sock: for address 0.0.0.0:443, apr_socket_opt_set:
(SO_KEEPALIVE)
no listening sockets available, shutting down
```

Wenn bei Ihnen ein zweiter Webserver in Betrieb ist, so sollten Sie diesen entweder anhalten oder einem von beiden einen anderen Port zuweisen.

Außerdem kann es natürlich sein, dass eine aktive Firewall den Zugriff auf den Webserver blockiert (siehe oben). Hier hilft meist eine Deaktivierung der Firewall bzw. ein Freischalten des Ports 80.

Wenn Sie mit Windows XP Professional bislang ohne das Service Pack 1 arbeiten, so kann auch das ein Grund dafür sein, dass der Apache nicht startet. Bringen Sie Ihr System in diesem Fall auf den neuesten Stand.

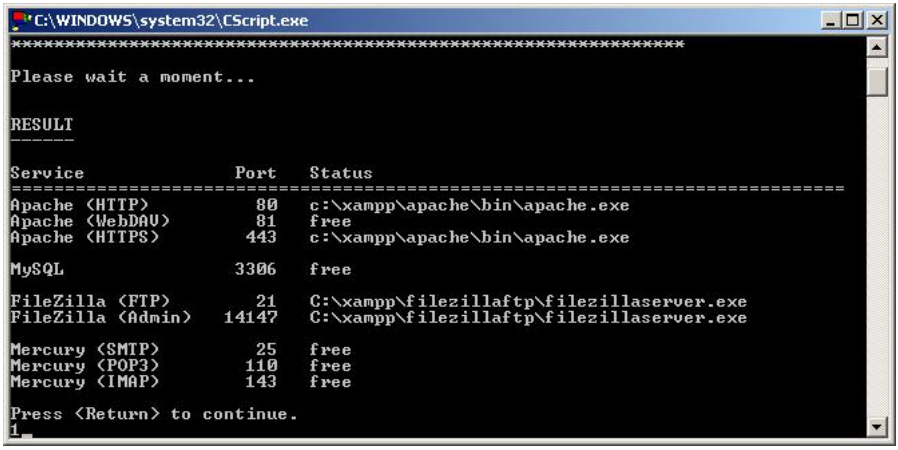


Die Standardeinstellung von Skype verhindert den Zugriff auf den Apache-Webserver.

Es gibt weitere mögliche Ursachen für die Nicht-Erreichbar- bzw. Nicht-Verfügbarkeit des Apache-Webservers. Eine Ursache kann eine bestehende Skype-Installation (*http://www.skype.com/intl/de/*) sein. Die Internet-Telefonie-Software ist standardmäßig so konfiguriert, dass Sie eingehende Verbindungen auf den Ports 80 und 443 entgegennehmen. Damit auch Ihr Apache erreichbar ist, sollten Sie unter *Aktionen > Optionen > Verbindung* die Option *Port 80 und 443 als Alternative für eingehende Verbindungen verwenden* deaktivieren.

Schließlich können Ihnen noch unter Windows 95 und seinen Nachfolgern veraltete oder veränderte Winsock-Installationen Probleme beim Zugriff bereiten. Auch beim Einsatz eines Virenscanners kann es Probleme geben. Deaktivieren Sie zu Testzwecken daher gegebenenfalls Ihren Virenscanner.

Bleibt nur die Frage, wie Sie herausfinden, wie es um den Status des Ports bestellt ist. Auch hierfür hat das XAMPP-Paket das passende Tool. Sie finden in Ihrem XAMPP-Installationsverzeichnis das Programm *xampp-portcheck.exe*. Starten Sie es mit einem Doppelklick, und schon zeigt es Ihnen an, welcher Port frei und welcher belegt ist.



Das Port-Check-Programm zeigt die freien und belegten Ports an.

13.3.9 Extrem hohe CPU-Auslastung

Unter Windows-Betriebssystemen kann der Apache Ihr System fast lahmlegen und eine CPU-Auslastung von weit über 90 Prozent bewirken. Dieses Problem lässt sich recht einfach durch einen Eingriff in die Apache-Konfigurationsdatei beheben.

Editieren Sie die Datei *\xampp\apache\conf\httpd.conf* und suchen Sie folgende Zeile:

```
# Win32DisableAcceptEx
```

Entkommentieren Sie diese Option und schon sollte die extrem hohe CPU-Auslastung der Vergangenheit angehören:

```
Win32DisableAcceptEx
```

Von diesem Problem sind nicht nur die gängigen Home-Varianten von Windows betroffen, sondern auch verschiedene Professional-Versionen.

13.3.10 Wo sind die Bilder und Style Sheets?

Bei verschiedenen auf XAMPP aufsetzenden Anwendungen wie beispielsweise phpBB kommt es immer wieder zu Problemen bei der Anzeige größerer Dateien wie Style Sheets oder Bildern. Dieses Problem lässt sich womöglich durch einen Eingriff in die Apache-Konfigurationsdatei beheben. Entkommentieren Sie dazu folgende Zeilen:

```
#EnableSendfile off
#EnableMMAP off
```

Nach einem Neustart des Webservers ist im Idealfall das Problem gelöst.

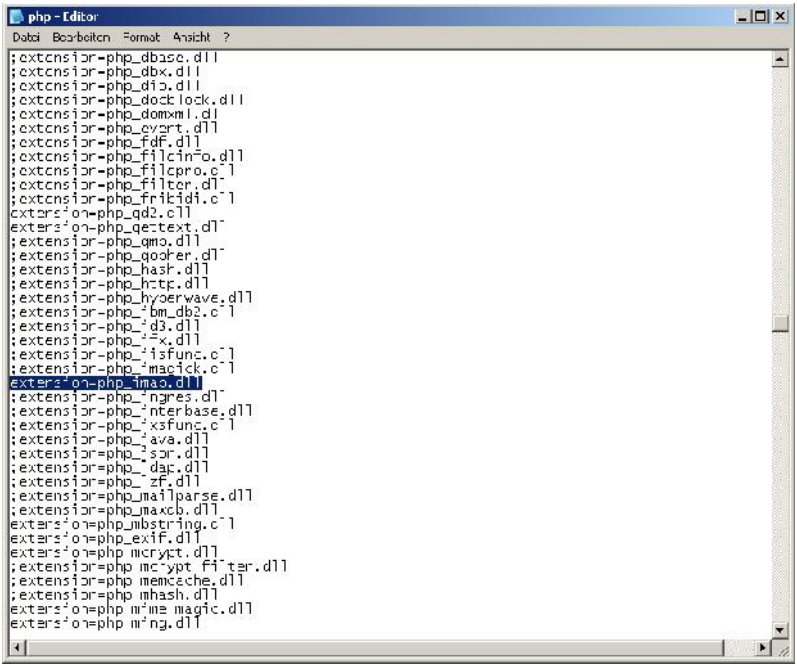
13.3.11 IMAP-Unterstützung für PHP

Unter XAMPP für Windows ist die IMAP-Unterstützung für PHP womöglich auf Ihrem XAMPP-System deaktiviert. Der Grund hierfür: Es kommt bei verschiedenen Home-Versionen zu rätselhaften Initialisierungsfehlern.

Wenn Sie mit einem NT-System arbeiten, bearbeiten Sie die Datei *\xampp\apache\bin\php.ini*. Entkommentieren Sie dort folgende Zeile:

```
# extension=php_imap.dll
```

Auch hier ist ein Neustart erforderlich, damit die Änderung greift. Entsprechend können Sie weitere (dynamische) Module aktivieren.



Das Aktivieren einer dynamischen Windows-Erweiterung, hier die IMAP-Unterstützung.

Anhang A – More Info

Dieses Handbuch ist ein Einstieg in die Welt von XAMPP und seinen verschiedenen Modulen. Wenn Sie die ersten Schritte gemeistert haben, werden Sie mehr wissen und ausprobieren wollen. Dann kommen Sie nicht umhin, sich mit entsprechender Literatur einzudecken bzw. an anderer Stelle weiterzulesen. Hier einige Anregungen.

Internet

XAMPP-Homepage

Auf der XAMPP-Homepage finden Sie neben der Software verschiedene Einstiegsdokumente.

http://www.apachefriends.org/de/xampp.html

Apache-Homepage

Hier finden Sie alles rund um den wichtigsten Webserver. Auch jede Menge Dokumentationen zeigen, was Sie alles mit dem Server anstellen können.

http://www.apache.org

MySQL-Homepage

Die Homepage des Datenbankservers bietet alles, was das Herz begehrt: Download, Dokumente und vieles mehr.

http://www.mysql.de

PHP-Homepage

Wenn Sie in die PHP-Programmierung einsteigen wollen, so ist die PHP-Homepage Ihre erste Adresse.

http://php.net

Die XAMPP-Homepage (*http://www.apachefriends.org*) ist die erste Adresse, wenn es um Downloads und weitere Informationen geht.

Literatur

Apache Webserver 2 – Installation, Konfiguration, Programmierung

Gutes Handbuch mit fast 900 Seiten zu allen wichtigen Belangen der Installation und Konfiguration des Apache-Webservers.

Sebastian Wolfgarten, 978-3827325662, Preis 29,95 EUR

phpMyAdmin 4.0 kompakt

Praxisbezogenes Buch, das zeigt, wie Sie typische Aufgaben im Datenbankalltag bewältigen, Daten und Strukturen erzeugen, Inhalte importieren und exportieren, MySQL-Server verwalten etc.

Holger Reibold, 978-3-95444-041-2, Preis 19,80 EUR

MySQL 5 – Einführung, Programmierung, Referenz

Sehr umfangreiches Werk, das Sie zum MySQL-Profi macht – wenn Sie bis zum Schluss durchhalten.

Michael Kofler, 978-3827326362, Preis 39,95 EUR

Anhang B – Wichtiges zu HTTP

Die Datenübertragung im Internet, genauer im World Wide Web, wird über das Hypertext Transfer Protocol, kurz HTTP, gesteuert. Es dient in erster Linie der Kommunikation zwischen einem Webserver und einem Browser.

Es handelt sich um ein zustandsloses Protokoll. HTTP ist durch verschiedene Erweiterungen seiner Anfragemethoden, Header-Informationen und Statuscodes nicht auf die Übertragung von Hypertext beschränkt, sondern kann für den Austausch beliebiger Daten verwendet werden.

Ein wenig Technik

Man bezeichnet die Kommunikationseinheiten, die HTTP-Client und -Server austauschen, als Nachrichten. Dabei unterscheidet man zwischen zwei Typen:

- Anfrage (engl. Request) vom Client an den Server
- Antwort (engl. Response) als Reaktion des Servers auf eine Client-Anfrage

Die Nachrichten bestehen wiederum aus zwei Teilen: dem Nachrichtenkopf (engl. Message Header, kurz: Header oder auch HTTP-Header genannt) und dem Nachrichtenkörper (engl. Message Body, kurz Body).

Im Header sind Informationen über den Nachrichtenkörper wie beispielsweise die verwendeten Kodierungen oder den Inhaltstyp enthalten, damit dieser vom Empfänger korrekt interpretiert werden kann. Der Nachrichtenkörper enthält die eigentlichen Nutzdaten.

Wenn Sie nun mit Ihrem Browser auf die URL *http://www.brain-media.de/beispiel.html* zugreifen, fragt Ihr Client beim Server *www.brain-media.de* an, ob dort die Ressource *beispiel.html* verfügbar ist.

Dabei wird zunächst *www.brain-media.de* über das DNS-Protokoll in eine IP-Adresse umgesetzt. Zur Übertragung wird über TCP auf den Standard-Port 80 des HTTP-Servers eine HTTP-GET-Anforderung gesendet.

Diese Anfrage sieht wie folgt aus:

```
GET /infotext.html HTTP/1.1
Host: www.brain-media.de
```

Sollten in dem Link Zeichen enthalten sein, die in der Anfrage nicht erlaubt sind, werden diese %-kodiert. Zusätzliche Informationen, wie Angaben über den Browser, zur gewünschten Sprache etc., können über den Header während der HTTP-Kommunikation übertragen werden.

Sobald der Header mit einer Leerzeile abgeschlossen wird, sendet der Computer, der einen Web-Server (an Port 80) betreibt, seinerseits eine HTTP-Antwort zurück. Diese besteht aus den Header-Informationen des Servers, einer Leerzeile und dem tatsächlichen Inhalt der Nachricht, also dem Dateiinhalt der *infotext.html*-Datei.

Übertragen werden normalerweise Dateien in Seitenbeschreibungssprachen wie (X)HTML und alle ihre Ergänzungen, zum Beispiel Bilder, Stylesheets (CSS), Skripte (JavaScript).

Die Antwort des Servers sieht dann beispielsweise wie folgt aus:

```
HTTP/1.1 200 OK
Server: Apache/1.3.29 (Unix) PHP/4.3.4
Content-Length: Größe von beispiel.html in Byte
Content-Language: de (nach RFC 3282 sowie RFC 1766)
Content-Type: text/html
Connection: close

Inhalt von beispiel.html
```

Sollten die angeforderten Daten aus irgendeinem Grund nicht übermittelt werden können, sendet der Server eine Fehlermeldung. Darauf kommen wir weiter unten noch zu sprechen.

Momentan begegnet man im Web zwei Protokollversionen, HTTP/1.0 und HTTP/1.1. Zwischen beiden gibt es kleine, aber feine Unterschiede. HTTP/1.0 baut vor jeder Anfrage eine neue TCP-Verbindung auf und schließt diese nach Übertragung der Antwort standardmäßig vom Server wieder. Das Problem dabei: Wenn in einem HTML-Dokument mehrere Bilder oder andere Dateien eingebettet sind, werden entsprechend viele TCP-Verbindungen benötigt.

HTTP/1.1 ist hier weitaus flexibler. Bei dieser Protokollvariante kann der Client mithilfe eines zusätzlichen Header-Eintrags (Keep-Alive) den Wunsch äußern, keinen Verbindungsabbau durchzuführen, um die Verbindung erneut nutzen zu können (persistent connection). Ob das allerdings funktioniert, ist davon abhängig, ob die Gegenseite diese Funktionalität ebenfalls unterstützt.

HTTP/1.1 kann mithilfe der sogenannten HTTP-Pipelining-Technik mehrere Anfragen und Antworten pro TCP-Verbindung versenden. In obigem Beispiel würde eine Verbindung genügen. Eine weiterer Vorteil von HTTP/1.1 gegenüber seinem Vorgänger: Unterbrochene Übertragungen können wieder aufgenommen und fortgesetzt werden.

HTTP/1.1 kann nicht nur Dateien auf das lokale System herunterladen, sondern auch zum Server übertragen. Mithilfe der PUT-Methode können so beispelsweise Webdesigner ihre Seiten direkt über den Webserver per WebDAV publizieren. Mit dem DELETE-Befehl können Sie sogar Daten auf dem Server löschen.

Für die Anforderung von Inhalten kommen verschiedene HTTP-Request-Methoden zum Einsatz. Nachstehende Tabelle fasst deren Eigenschaften zusammen:

Methode	Beschreibung
GET	Diese Methode ist die gebräuchlichste. Sie dient dazu, eine Ressource, also beispielsweise eine Datei, unter Angabe eines URI vom Server anzufordern.
POST	Diese Methode schickt Daten zur weiteren Verarbeitung zum Server. Die Daten werden als Inhalt der Nachricht übertragen und können beispielsweise aus Name-Wert-Paaren bestehen, die aus einem HTML-Formular stammen.
HEAD	Diese Methode weist den Server an, die gleichen HTTP-Header wie bei GET, nicht jedoch den eigentlichen Dokumentinhalt (Body) zu senden.
PUT	Sie dient dazu, eine Ressource unter Angabe des Ziel-URIs auf einen Webserver hochzuladen.
DELETE	Diese Methode löscht die angegebene Ressource auf dem Server. Sie ist allerdings kaum implementiert bzw. in der Standardkonfiguration von Webservern abgeschaltet, um unerwünschte Löschvorgänge zu verhindern.
TRACE	Mit dieser Methode kann überprüft werden, ob und wie die Anfrage auf dem Weg zum Server verändert worden ist. Das

	ist insbesondere für die Fehlersuche nützlich.
OPTIONS	Diese Methode gibt die Liste der vom Server unterstützten Methoden und Features zurück.
CONNECT	Diese Methode wird von Proxy-Servern implementiert, die in der Lage sind, SSL-Tunnel zur Verfügung zu stellen.

WebDAV fügt folgende Methoden zu HTTP hinzu: PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK und UNLOCK.

HTTP-Statuscodes

Die HTTP-Anfrage eines Webbrowser beantwortet der Server immer mit einem sogenannten HTTP-Statuscode. Mit diesem Code gibt er beispielsweise an, ob die Anfrage erfolgreich bearbeitet wurde, oder teilt dem Client, also etwa dem Browser, im Fehlerfall mit, wo (z. B. Umleitung) bzw. wie (z. B. mit Authentifizierung) er die gewünschten Informationen (wenn möglich) erhalten kann.

Diese Informationen sind insbesondere bei der Fehlersuche eine wertvolle Hilfe, weil Sie Ihnen genau entnehmen können, um welchen Fehlertyp es sich handelt. Daraus können Sie dann meist auch die geeigneten Maßnahmen für die Fehlerbehebung einleiten.

Die Status-Codes:

Code-Bereich	Beschreibung
1xx	Informationen Bei diesen Codes handelt es sich um Zwischenantworten, die ausgegeben werden, während eine Anfrage noch in Bearbeitung ist.
2xx	Erfolgreiche Operation Diese Codes werden ausgegeben, wenn eine Anfrage erfolgreich bearbeitet werden konnte und die Antwort an den Anfragesteller zurückgesendet wird.
3xx	Umleitung Sollten weitere Schritte aufseiten des Clients notwendig sein, um die Anfrage erfolgreich bearbeiten zu können,

	werden diese Status-Codes ausgegeben. Das ist z. B. dann der Fall, wenn eine Webseite vom Betreiber umgestaltet wurde, sodass sich eine gewünschte Datei nun an einem anderen Platz befindet. Mit der Antwort des Servers erfährt der Client im Location-Header, wo sich die Datei jetzt befindet.
4xx	Client-Fehler Tritt bei der Verarbeitung des Requests ein Fehler auf und ist der Client dafür verantwortlich, so wird ein Codes diesen Typs ausgegegen. So tritt beispielsweisee der Fehler 404 auf, wenn der Client ein Dokument anfragt, das nicht mehr auf dem Server existiert. Ein 403-Fehler zeigt an, dass der Client nicht die notwendigen Berechtigungen für den Abruf besitzt.
5xx	Server-Fehler Liegt der Fehler beim Server, so wird eine Fehlermeldung diesen Typs ausgegeben. Der Fehler 501 liegt beispielsweise vor, wenn der Server nicht über die erforderlichen Funktionen verfügt, um die Anfrage zu bearbeiten.

Im Header der Server-Antwort ist immer auch eine Kurzinfo enthalten, allerdings in englischer Sprache, die den Fehler kurz beschreibt. Ein Beispiel für einen typischen Fehler 404:

```
HTTP/1.1 404 Not Found
```

Die Liste der HTTP-Statuscodes

Wenn Sie sich intensiv mit dem Apache-Webserver befassen und darauf beispielsweise eine der vielen PHP-Anwendung ausführen, werden Sie immer wieder solchen HTTP-Status-Codes begegnen. Nachfolgend sind die wichtigsten Status-Codes und deren Bedeutung aufgeführt. Das wird Ihnen die Fehlersuche erleichtern.

100 Continue

Die aktuelle Anfrage an den Server wurde noch nicht zurückgewiesen. Der Client kann nun mit der (potenziell sehr großen) Anfrage fortfahren.

101 Switching Protocols

Erhält der Server einen Request mit gesetztem Upgrade-Header-Feld und ist er mit dem Wechsel zu einem anderen Protokoll einverstanden, gibt er diesen Code aus.

102 Processing

Zeigt an, dass der Server noch mit einer zeitintensiven Anfrage beschäftigt ist. Dieser Code wird verwendet, um ein Timeout zu vermeiden, während der Server eine zeitintensive Anfrage bearbeitet.

200 OK

Zeigt an, dass die Anfrage erfolgreich bearbeitet und das Ergebnis auf die Anfrage in der Antwort übertragen wurde.

201 Created

Bestätigt, dass der Request erfolgreich bearbeitet wurde. Die angeforderte Ressource wurde vor dem Senden der Antwort erzeugt. In dem Location-Header-Feld ist eventuell die Adresse der erstellten Ressource enthalten.

202 Accepted

Der Server zeigt an, dass die Anfrage akzeptiert wurde, aber zu einem späteren Zeitpunkt ausgeführt wird. Außerdem kann die erfolgreiche Verarbeitung des Requests nicht garantiert werden.

203 Non-Authoritative Information

Bei dieser Meldung wurde der Request erfolgreich ausgeführt, das Ergebnis ist aber nicht unbedingt vollständig und aktuell.

204 No Content

Zeigt an, dass der Request erfolgreich durchgeführt werden konnte, die Response aber bewusst keine Daten beinhaltet.

205 Reset Content

Auch bei dieser Ausgabe wurde die Anfrage erfolgreich durchgeführt. Der Client soll das Dokument neu aufbauen und Formulareingaben zurücksetzen.

206 Partial Content

Der angeforderte Teil wurde erfolgreich übertragen und kann einen Client über Teil-Downloads informieren.

207 Multi-Status

Die Response des Servers enthält ein XML-Dokument, das mehrere Statuscodes zu unabhängig voneinander durchgeführten Operationen enthält.

300 Multiple Choice

Die angeforderte Ressource steht in verschiedenen Varianten zur Verfügung.

301 Moved Permanently

Die angeforderte Ressource steht ab sofort unter der im Location-Header-Feld angegebenen Adresse bereit. Die alte Adresse ist nicht länger gültig.

302 Found

Zeigt an, dass die angeforderte Ressource vorübergehend unter der im Location-Header-Feld angegebenen Adresse bereitsteht. Die alte Adresse bleibt allerdings weiter bestehen. In HTTP/1.1 wird dieser Code je nach Anwendungsfall durch die Status-Codes 303 bzw. 307 ersetzt.

303 See Other

Bezieht sich auf die im Location-Header-Feld angegebene Adresse.

304 Not Modified

Seit dem letzten Request der angeforderten Ressource hat sich der Inhalt nicht verändert und wird daher auch nicht erneut übertragen.

305 Use Proxy

Zeigt an, dass die angeforderte Ressource nur über einen Proxy erreichbar ist. Im Location-Header-Feld ist die Adresse des Proxy-Servers hinterlegt.

306 (reserviert)

Der Status-Code 306 ist reserviert, wird aber nicht verwendet. Der Code war ursprünglich für Switch Proxy gedacht.

307 Temporary Redirect

Zeigt an, dass die angeforderte Ressource vorübergehend unter der im Location-Header-Feld angegebenen URL zu finden ist. Allerdings bleibt die alte Adresse weiter gültig.

400 Bad Request

Der Server meldet, dass der Request fehlerhaft aufgebaut ist.

401 Unauthorized

Zeigt an, dass die Anfrage nicht ohne gültige Authentifizierung durchgeführt werden kann. Der Server teilt dem Client im WWW-Authenticate-Header-Feld der Antwort mit, wie die Authentifizierung durchgeführt werden soll.

402 Payment Required

Dieser Status-Code ist reserviert.

403 Forbidden

Der Client konnte sich mangels gültiger Zugangskennung keinen Zugang zu dem Server verschaffen.

404 Not Found

Die angeforderte Ressource existiert nicht bzw. wurde nicht gefunden. Dieser Statuscode kann ebenfalls verwendet werden, um eine Anfrage ohne näheren Grund abzuweisen. Man spricht in diesem Zusammenhang auch von toten Links.

405 Method Not Allowed

Zeigt an, dass für den Request eine andere HTTP-Methode verwendet werden muss, beispielsweise GET statt POST. Gültige Methoden für die betreffende Ressource werden im Übrigen im Allow-Header-Feld der Antwort übermittelt.

406 Not Acceptable

Die angeforderte Ressource steht nicht in der gewünschten Form zur Verfügung. Die gültigen Content-Type-Werte können in der Antwort übermittelt werden.

407 Proxy Authentication Required

Ist mit der Ausgabe der Status-Code 401 vergleichbar. Allerdings ist hier zunächst eine Authentifizierung des Clients gegenüber dem verwendeten Proxy erforderlich.

408 Request Time-out

Erhält der Server innerhalb der vom Server erlaubten Zeitspanne keine vollständige Anfrage des Clients, wird dieser Code ausgegeben.

409 Conflict

Zeigt an, dass der Request unter falschen Annahmen gestellt wurde. Bei einer PUT-Anfrage kann das beispielsweise zwischenzeitliche Veränderung der Ressource durch Dritte verursacht werden.

410 Gone

Der Server gibt diesen Code zurück, wenn die angeforderte Ressource nicht mehr bereitsteht oder dauerhaft entfernt wurde.

411 Length Required

Zeigt dem Client an, dass der Request ohne ein Content-Length-Header-Feld nicht bearbeitet werden kann.

412 Precondition Failed

Der Server informiert den Client, dass die in der Anfrage übertragene Voraussetzung nicht zutriff.

413 Request Entity Too Large

Bei dieser Ausgabe war die gestellte Anfrage zu groß, um vom Server bearbeitet werden zu können.

414 Request-URI Too Long

Hierbei handelt es sich um einen Request, dessen URI zu lang war. Meist ist eine Endlosschleife aus Redirects der Grund dafür.

415 Unsupported Media Type

Zeigt an, dass der Inhalt der Anfrage mit ungültigem oder nicht erlaubtem Medientyp übermittelt wurde.

416 Requested range not satisfiable

Der angeforderte Teil einer Ressource war ungültig oder steht auf dem Server nicht zur Verfügung.

417 Expectation Failed

Zeigt an, dass das das im Expect-Header-Feld geforderte Verhalten des Servers nicht erfüllt werden kann.

418 I'm a Teapot

Hierbei handelt es sich um einen Aprilscherz der IETF, der in RFC 2324, Hyper Text Coffee Pot Control Protocol, definiert ist.

421 There are too many connections from your internet address

Der Server zeigt dem Client an, dass die Verbindungshöchstzahl überschritten wurde.

423 Locked

Die angeforderte Ressource ist zurzeit gesperrt.

424 Failed Dependency

Die Anfrage konnte nicht durchgeführt werden, weil sie das Gelingen einer vorherigen Anfrage voraussetzt.

425 Unordered Collection

Dieser Code ist in den WebDav Advanced Collections definiert.

426 Upgrade Required

Der Server verlangt vom Client, dass dieser auf Transport Layer Security (TLS/1.0) umschaltet.

500 Internal Server Error

Hierbei handelt es sich um einen Sammel-Statuscode für unerwartete Serverfehler.

501 Not Implemented

Der Server zeigt dem Client an, dass die Funktionalität, um die Anfrage zu bearbeiten, nicht vom Server bereitgestellt wird. Ursache hierfür kann beispielsweise eine unbekannte oder nicht unterstützte HTTP-Methode sein.

502 Bad Gateway

Zeigt an, dass der Server seine Funktion als Gateway oder Proxy nicht erfüllen kann, weil er eine ungültige Antwort erhalten hat.

503 Service Unavailable

Der Server ist aktuell nicht erreichbar. Grund hierfür können beispielsweise Überlastungen oder Wartungsarbeiten sein.

504 Gateway Time-out

Der Server konnte seine Funktion als Gateway oder Proxy nicht erfüllen, weil er innerhalb einer festgelegten Zeitspanne keine Antwort von Servern oder Diensten erhält, auf die er zugrückgreift.

505 HTTP Version not supported

Die verwendete HTTP-Version wird vom Server nicht unterstützt oder abgelehnt.

507 Insufficient Storage

Die Anfrage kann nicht bearbeitet werden, weil der Speicherplatz des Servers dazu nicht ausreicht.

509 Bandwidth Limit Exceeded

Die Anfrage wurde verworfen, weil sonst die verfügbare Bandbreite überschritten werden würde.

510 Not Extended

Die Anfrage enthält nicht alle Informationen, die die angefragte Server-Extension zwingend erwartet.

Anhang C – Wissenwertes über FTP

Nachdem in Kapitel 6 alle wesentlichen Funktionen von FileZilla-Client und -Server ausführlich erläutert wurden, sollen hier noch einige Hinweise gegeben werden, die zwar nicht das Programm direkt betreffen, die jedoch für den erfolgreichen Betrieb wesentlich sind.

FTP-Verbindung

FTP (File Transfer Protocol) ist ein Netzwerkprotokoll zur Fernübertragung von Dateien innerhalb von TCP/IP-Netzwerken. Dabei unterscheidet man die Übertragung von Dateien vom Server zum Client (Herunterladen/Download), vom Client zum Server (Hochladen/Upload) oder clientgesteuert zwischen zwei Endgeräten. Außerdem können mit FTP Verzeichnisse angelegt und ausgelesen sowie Verzeichnisse und Dateien umbenannt oder gelöscht werden.

Für die Steuerung und Datenübertragung werden separate Verbindungen benutzt. Eine FTP-Sitzung beginnt, indem vom Client zum Control-Port des Servers (standardmäßig ist dies Port 21) eine TCP-Verbindung aufgebaut wird. Über diese Verbindung werden Befehle zum Server gesendet. Der Server antwortet auf jeden Befehl mit einem Statuscode, oft mit einem angehängten, erklärenden Text.

Zum Senden und Empfangen von Dateien sowie zur Übertragung von Verzeichnislisten (standardmäßig via Port 20) wird für jeden Vorgang eine separate TCP-Verbindung verwendet. Dies kann bei FTP auf zwei verschiedenen Wegen geschehen, nämlich im passiven oder im aktiven Modus.

Passiver Modus

Im passiven Modus hat der Client keinerlei Kontrolle darüber, welchen Port der Server für die Datenverbindung auswählt, deshalb müssen Sie abgehende Verbindungen zu allen Ports in Ihrer Firewall erlauben, wenn Sie den passiven Modus verwenden möchten.

Aktiver Modus

Im aktiven Modus öffnet der Client einen Socket und wartet darauf, dass der Server die Verbindung zur Übertragung herstellt.

Wenn Sie eine direkte Verbindung zum Internet (ohne Router) verwenden und Ihre Firewall so eingestellt ist, dass eingehende Verbindungen an allen Ports mit höherer Nummer als 1024 erlaubt sind, erfragt der FileZilla-Client beim Betriebssystem die IP-Adresse des Rechners sowie einen freien Port.

Die meisten Nutzer von Breitbandanschlüssen verwenden jedoch heutzutage einen NAT-Router (Network Address Translation), entweder als Standalone-Gerät oder in einen DSL-Router integriert. Dieser Router ist so etwas wie eine Tür zur Außenwelt. Die dahinterliegenden Geräte bilden das lokale Netzwerk oder LAN (Local Area Network). Jedes dieser Geräte hat eine lokale IP-Adresse, und wenn Sie die NAT-Funktionalität verwenden, müssen Sie dem FileZilla-Server Ihre externe IP-Adresse mitteilen, sonst sind aktive Verbindungen mit Servern außerhalb Ihres Netzwerks nicht möglich.

Wenn Sie eine feste externe IP-Adresse verwenden, tragen Sie diese in das Konfigurationsfenster ein. Haben Sie eine dynamische IP-Adresse, fordert der FileZilla-Server diese automatisch an. Sollten Sie unsicher sein, welche der beiden Methoden Sie verwenden, wählen Sie die letztere Option.

Wenn Sie nicht an allen Ports eingehende Verbindungen erlauben möchten, müssen Sie dem FileZilla-Server mitteilen, welche Ports für aktive Verbindungen benutzt werden sollen. Diese Ports müssen dann auch in der Firewall freigeschaltet werden. Bei Verwendung eines NAT-Routers müssen diese Ports an den lokalen Rechner weitergegeben werden, auf dem der FileZilla installiert ist.

Gültige Portnummern sind 1 – 65535, die Nummern kleiner 1024 sind allerdings für andere Protokolle reserviert.

Ports

Die meisten üblichen FTP-Server verwenden Port 21, um sich mit anderen Rechnern zu verbinden. SFTP-Server verwenden standardmäßig Port 22, FTP over SSL/TLS (implicit mode) Port 990. Dies sind keine erzwungenen Einstellungen, es ist daher am Besten, abgehenden Verbindungen die Wahl des Remote-Ports frei zu lassen.

Jede FTP-Verbindung beginnt mit der Authentifizierung des Benutzers. Anschließend erfolgt der Aufbau des Steuerkanals über Port 21 und des Datenkanals über Port 20. Wenn die Dateiübertragungen abgeschlossen sind, werden die Verbindungen vom Benutzer oder vom Server (Timeout) beendet.

Für die Übertragung von Daten kennt das FTP-Protokoll ebenfalls zwei verschiedene Modi, nämlich den ASCII-Modus und den Binary-Modus. Diese beiden Modi unterscheiden sich in der Art der Kodierung. Der ASCII-Modus wird zur Übertragung von reinen Text-Dateien verwendet. Hier muss die Zeilenstruktur des Textes umkodiert werden. Bei diesem Vorgang wird der Zeichensatz der Datei an das Zielsystem angepasst. Der Binary-Modus überträgt die Dateien byteweise, ohne die Daten zu ändern. Dieser Modus wird am häufigsten genutzt. Vorzugsweise natürlich bei Binär-Dateien.

Die Fehlerkontrolle bei der Datenübertragung überlässt FTP komplett dem TCP-Protokoll. Kommt es doch zu einem Verbindungsabbruch, sieht die FTP-Spezifikation die Wiederaufnahme von unterbrochenen Übertragungen vor. Die Header der einzelnen Datenpakete enthalten Restart-Markierungen. Versucht der FTP-Client, die Übertragung wieder aufzunehmen, gleichen Client und Server die Markierungen ab. Anschließend wird die Übertragung wieder fortgeführt.

FTP-Befehle

In der einfachsten Form, d. h., wenn Sie keine FTP-Software wie FileZilla zur Verfügung haben, findet die Kommunikation zwischen FTP-Client und -Server als Austausch von textbasierten Kommandos statt. Diese FTP-Befehle gibt es unter anderem für das Senden, Empfangen, Löschen und Umbenennen von Dateien, sowie für das Einrichten, Löschen und Wechseln von Verzeichnissen.

Auch FileZilla arbeitet auf der Basis dieser Befehle, nur dass es Ihnen eine grafische Oberfläche zur Verfügung stellt, die das Bedienen einfach und intuitiv macht.

Sowohl der FileZilla-Client als auch der FileZilla-Server verfügen über ein Protokollfenster, in dem nicht nur die erwähnten FTP-Befehle, sondern auch alle sonstigen Ereignisse und Nachrichten, die im Verlauf einer Session auftauchen, geloggt werden. Um verstehen zu können, was hier im Einzelnen abläuft, sollte man die FTP-Befehle und ihre Bedeutung kennen.

Die wesentlichen Anweisungen finden Sie im Folgenden aufgelistet und kurz erklärt:

Befehl	Name	Beschreibung
ABOR	Abort	Voriges Kommando abbrechen
ACCT	Account	Benutzerkennung
APPE	Append	Hereinkommende Daten an existierende Datei anhängen

CDUP	Change directory upwards	Wechsel zum übergeordneten Verzeichnis
CWD	Change working directory	Wechsel des Arbeitsverzeichnisses
DELE	Delete file	Datei löschen
HELP	Help	Hilfeinformationen ausgeben
LIST	List directory	Verzeichnisliste übertragen (Dieser Befehl wird sukzessive durch MLSD und MLST ersetzt.)
MDTM	Modification time	Datum der letzten Änderung einer Datei
MKD	Make directory	Neues Verzeichnis anlegen
MLSD		Alle Dateien des Verzeichnisses anzeigen
MLST		Daten zum genannten Objekt anzeigen
MODE	Mode	Übertragungsmodus festlegen
NLST	Name list	Verzeichnisinhalt übertragen
NOOP	No operation	Keine Operation
PASS	Password	Benutzerpasswort abfragen
PASV	Passive mode	Passive FTP-Verbindung anfordern
PORT	Data port	Port-Adresse öffnen
PWD	Print working directory	Momentanes Verzeichnis zurückgeben
QUIT	Quit connection	Verbindung beenden
REIN	Reinitialize connection	Verbindung beenden und neu starten
REST	Restore transfer	Transfer neu starten – kommt immer vor einem Befehl zum Datentransfer (RETR oder STOR)
RETR	Retrieve	Datei vom Server kopieren

RMD	Remove directory	Verzeichnis löschen
RNFR	Rename from	Alter Name einer umzubenennenden Datei
RNTO	Rename to	Neuer Name für umzubenennende Datei
SITE	Site-specific	Serverspezifische Informationen liefern
STAT	Status	Server-Status ausgeben
STOR	Store	Datei zum Server kopieren
STOU	Store uniquely	Datei unter anderem Namen zum Server kopieren
STRU	Structure	Dateistruktur bestimmen
SYST	System type	Betriebssystem bestimmen
TYPE	Transfer type	Typ der Daten bestimmen
USER	User name	Benutzername

FTP-Status-Codes

Ebenfalls von Interesse sind die Status-Codes, die der Server auf jeden vom FTP-Client gesendeten Befehl hin zurückgibt. Diese Codes werden normalerweise von einer Meldung im Klartext begleitet.

Der Status-Code ist eine 3-stellige Nummer, die Informationen über die Verfügbarkeit der angeforderten Daten enthält. Zum Beispiel wird über den Status-Code eine Fehlermeldung übermittelt.

Die Status-Codes sind in folgende 5 Gruppen unterteilt:

Code-Bereich	Beschreibung
100-199	Vorläufige positive Antwort Vorgang wurde erfolgreich ausgeführt, jedoch erwartet der Server vom Client eine weitere Antwort, bevor er mit einem neuen Befehl fortfahren kann.
200-299	Positive Antwort bei erfolgreichem Vorgang Vorgang wurde erfolgreich abgeschlossen. Der Client ist

	bereit für neue Anweisungen.
300-399	Positive Zwischenantwort Vorgang wurde erfolgreich ausgeführt, der Server erwartet jedoch weitere Informationen vom Client, um die Bearbeitung abzuschließen.
400-499	Vorübergehende negative Antwort Befehl konnte nicht ausgeführt werden, wobei lediglich ein temporäres Problem vorliegt. Möglicherweise wird beim erneuten Versuch die Bearbeitung erfolgreich abgeschlossen.
500-599	Dauerhafte negative Antwort Befehl konnte nicht ausgeführt werden, wobei hier ein permanentes Problem vorliegt. Der erneute Versuch, den Befehl auszuführen, würde zum selben Resultat führen.

Einige der wichtigsten Status-Codes sind nachfolgend zusammengefasst. Neben der Code-Nummer sind die Meldung in englischer Sprache und eine Erläuterung in Deutsch angegeben sowie, wo es sinnvoll erscheint, eine kurze Erläuterung der Ursache für den betreffenden Code. Die Status-Codes im Überblick:

110 Restart marker reply

Markierung zur Wiederaufnahme der Übertragung.

120 Service ready in n minutes

Dienst steht in n Minuten zur Verfügung.

125 Data connection already open; transfer starting

Datenverbindung besteht bereits, Übertragung beginnt.

150 File status okay; about to open data connection

Dateistatus OK, Datenverbindung wird aufgebaut.

FTP verwendet zwei Anschlussnummern: 21, zum Senden von Befehlen, und 20, zum Senden von Daten. Ein Statuscode von 150 weist darauf hin, dass der Server

im Begriff ist, eine neue Verbindung zum Anschluss 20 herzustellen, um Daten zu senden.

200 Command okay

Befehl OK.

202 Command not implemented

Befehl nicht implementiert.

211

Antwort für Systemstatus oder Hilfefunktion des Systems.

212

Verzeichnisstatus.

213

Dateistatus.

214

Meldung der Hilfefunktion.

215 NAME system type

Angabe des Systemtyps.

220 Service ready for new user

Dienst bereit für neuen User.

221 Service closing control connection

Steuerverbindung wird getrennt und User abgemeldet.

225 Data connection open; no transfer in progress

Datenverbindung besteht, derzeit keine Übertragung.

226 Closing data connection. Requested file action successful

Datenverbindung wird getrennt; angeforderte Dateioperation war erfolgreich. Per Befehl wurde eine Datenverbindung zu Port 20 hergestellt, um einen Vorgang auszuführen, z. B. die Übertragung einer Datei. Der Vorgang wurde erfolgreich beendet und die Datenverbindung getrennt.

227 Entering Passive Mode

Passiver Modus aktiviert.

230 User logged in, proceed

User ist angemeldet, bitte fortfahren.

Dieser Statuscode erscheint immer dann, wenn ein Client das passende Kennwort gesendet hat. Er weist darauf hin, dass sich der Benutzer erfolgreich angemeldet hat.

250 Requested file action okay, completed

Angeforderte Dateioperation OK und abgeschlossen.

257 "PATH" created

PFAD wurde erstellt.

331 User name okay, need password

Benutzername OK, Kennwort benötigt.

Dieser Statuscode erscheint, wenn der Client einen Benutzernamen gesendet hat. Es erscheint immer der gleiche Statuscode, unabhängig davon, ob der Benutzername auf dem System gültig ist oder nicht.

332 Need account for login

Benutzerkonto zur Anmeldung benötigt.

350 Requested file action pending further information

Mehr Informationen benötigt für angeforderte Dateioperation.

421 Service not available, closing control connection

Dienst nicht verfügbar, Steuerverbindung wird getrennt.

Diese Meldung kann auf einen beliebigen Befehl folgen, wenn ein Herunterfahren des Dienstes ansteht.

425 Can't open data connection

Datenverbindung kann nicht hergestellt werden.

426 Connection closed; transfer aborted

Verbindung getrennt, Übertragung abgebrochen.

Per Befehl wurde eine Datenverbindung hergestellt, um einen Vorgang auszuführen. Der Vorgang wurde jedoch abgebrochen und die Datenverbindung getrennt.

450 Requested file action not taken. File unavailable

Angeforderte Dateioperation nicht ausgeführt, Datei nicht verfügbar (möglicherweise gesperrt)

451 Requested action aborted: local error in processing

Angeforderte Aktion abgebrochen, lokaler Bearbeitungsfehler.

452 Requested action not taken; Insufficient storage space in system

Angeforderte Aktion wurde nicht ausgeführt, ungenügender Systemspeicherplatz.

500 Syntax error

Syntaxfehler, unbekannter Befehl.

501 Syntax error in parameters or arguments

Syntaxfehler, unbekannte(r) Parameter.

502 Command not implemented

Befehl nicht implementiert.

503 Bad sequence of commands

Falsche Befehlsabfolge.

504 Command not implemented for that parameter

Befehl für diesen Parameter nicht implementiert.

530 Not logged in

Nicht angemeldet.

Dieser Statuscode weist darauf hin, dass sich der Benutzer nicht anmelden kann, weil die Kombination aus Username und Kennwort ungültig ist. Möglicherweise haben Sie das Kennwort für Ihr Benutzerkonto falsch geschrieben, oder der Server ist ausschließlich für einen anonymen Zugriff konfiguriert. Erscheint dieser Statuscode, wenn Sie versucht haben, sich anonym anzumelden, ist IIS möglicherweise so konfiguriert, dass ein anonymer Zugriff nicht zugelassen wird.

532 Need account for storing files

Anmeldung benötigt zum Speichern der Dateien.

550 Requested file action not taken. File unavailable

Angeforderte Dateioperation nicht ausgeführt; Datei nicht verfügbar (Datei gelöscht oder keine Zugriffsberechtigung). Der Befehl wird nicht ausgeführt, weil die angegebene Datei nicht vorhanden ist. Dieser Statuscode wird z. B. angezeigt, wenn mittels GET eine Datei angefordert wurde, die auf dem System nicht vorhanden ist, oder wenn mittels PUT eine Datei in einem Verzeichnis erstellt werden soll, in dem Sie keine Schreibberechtigung haben.

551 Requested action aborted: page type unknown

Angeforderter Vorgang abgebrochen, unbekannter Seitentyp.

552 Requested file action aborted. Exceeded storage allocation

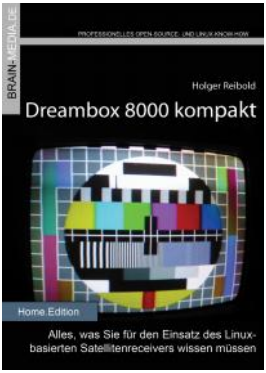
Angeforderter Dateivorgang abgebrochen, ungenügender Speicherplatz zugewiesen.

553 Requested action not taken. File name not allowed

Angeforderter Vorgang nicht ausgeführt, unzulässiger Dateiname.

Index

Weitere Brain-Media.de-Bücher



Dreambox 8000 kompakt

Die Dreambox 8000 stellt ihre Vorgänger allesamt in den Schatten. Was Sie alles mit der Dreambox 8000 anfangen können, verrät Ihnen die Neuauflage unseres Dreambox-Klassikers.
Mit einem Vorwort des Dream Multimedia-Geschäftsführers Karasu.

Umfang: 450 Seiten plus CD
ISBN: 978-3-939316-90-9
Preis: 29,80 EUR

Scribus 1.4 kompakt

Scribus ist längst ein ebenbürtiger Gegenspieler von InDesign & Co. In unserem Handbuch erfahren Sie alles, was Sie für den erfolgreichen Einstieg wissen müssen. Auf über 450 Seiten lernen Sie nahezu jede Programmfunktion kennen. Praxisbezogene Beispiele zeigen, wie Sie mit Scribus schnell ans Ziel gelangen.

Umfang: 465 Seiten plus DVD
ISBN: 978-3-939316-91-6
Preis: 29,80 EUR

X-Plane 10 kompakt

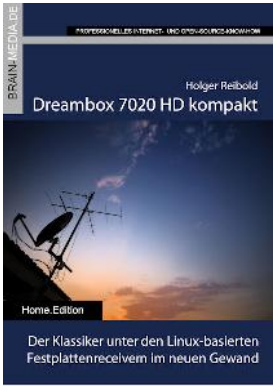
Der Klassiker unter den Flugsimulatoren geht in die zehnte Runde. Viele neue Funktionen und verbessertes Handling warten auf die Anwender. Kein Wunder also, dass die Fangemeinde wächst und wächst.
Unser Handbuch beschreibt alles, was Sie für das Fliegen mit X-Plane wissen sollten.

Umfang: 430 Seiten
ISBN: 978-3-939316-96-1
Preis: 24,80 EUR

Audacity 2.0 kompakt

Audacity ist zweifelsohne das beliebteste freie Audioprogramm. Vom anfänglichen Geheimtipp hat sich der Editor zum Standard für die Aufzeichnung und Bearbeitung von Audiodaten gemausert.
Das Vorwort steuert der ehemalige Core-Entwickler Markus Meyer bei.

Umfang: 306 Seiten
ISBN: 978-3-95444-027-6
Preis: 24,80 EUR



Dreambox 7020 HD kompakt

Der Klassiker im neuen Gewand: Die Dreambox 7020 HD besticht durch das OLED-Display an der Front sowie ihr flexibles Tuner-Konzept. In diesem Handbuch lernen Sie die vielfältigen Einsatzmöglichkeiten der Box kennen.
Mit einem Vorwort des Dream Multimedia-Geschäftsführers Karasu.

Umfang: 430 Seiten
ISBN: 978-3-939316-99-2
Preis: 24,80 EUR

Weitere Titel in Vorbereitung

Wir bauen unser Programm kontinuierlich aus. Aktuell befinden sich folgende Titel in Vorbereitung:

- Android Forensik
- X-Plane 10 Power Package
- OpenCart kompakt
- Galaxy Note 3 kompakt
- Galaxy S 5 kompakt
- Dreambox Goliath
- vTiger 6.0 kompakt
- PlayStation 4 kompakt
- FreeMind 1.0 kompakt
- Anti-Spam SMTP Proxy Server kompakt

Plus*

Plus* – unser neues Angebot für Sie ... alle E-Books im Abo. Sie können 1 Jahr alle Brain-Media-Bücher als E-Book herunterladen und diese auf Ihrem PC, Tablet, iPad und Kindle verwenden - und das ohne irgendwelche Einschränkungen. Das Beste: Plus+ schließt auch alle jene Bücher ein, die in diesem Jahr noch erscheinen.

Und das zum Sonderpreis von 29 Euro! Ein unschlagbares Angebot!

Auf unserer Website steht ein detaillierter Überblick aller Titel im PDF-Format zum Download bereit, der bereits zu Plus* gehörende Titel aufführt und die in naher Zukunft hinzukommen.

Plus* startet im Herbst 2013.