RUB

SHORTGUIDE
ZUGRIFFSBESCHRÄNKUNG AUF ZENTRALEN WEBSERVERN

FÜR MITGLIEDER UND ANGEHÖRIGE DER RUB

Grundlagen

Es gibt zwei verschiedene Möglichkeiten, Zugriffsbeschränkungen für WWW-Seiten auf den Servern der Ruhr-Universität zu realisieren. Zum einen über Benutzername und Passwort und zum anderen über die IP-Adresse bzw. den Namen des Rechners, der eine WWW-Seite anfordert. Bei beiden Möglichkeiten wird immer eine Datei mit dem Namen **.admopts** benötigt. In dieser Datei wird die Art der Zugriffssbeschränkung festgelegt. Bei der Zugriffsbeschränkung durch Benutzername und Passwort muss zusätzlich die Datei **.admusers**, die Benutzernamen und verschlüsselte Passwörter enthält, erstellt werden.

Grundsätzlich müssen beide Dateien als reine Textdateien vorliegen. Nehmen Sie zum Editieren ein geeignetes Programm wie den Windows Editor Notepad oder jeden anderen Text-Editor und speichern Sie die Dateien als Textdateien ohne Endung bzw. entfernen Sie die Dateiendung nach dem Speichern. Nach dem Editieren müssen Sie die Datei(en) mit einem beliebigen FTP-Programm auf den Webserver laden. Die Datei .admopts steuert nun den Zugriff auf das Verzeichnis, in dem sie liegt, sowie auf alle in diesem Verzeichnis vorhandenen Dateien. Die Einstellungen gelten auch für etwaige Unterverzeichnisse und dort vorhandene Dateien, sofern dort keine weitere .admopts Datei mit anderen Einstellungen liegt. Sie können auch einzelne Dateien mit einer Zugriffsbeschränkung belegen (siehe Box 5 in dieser Anleitung).

Auf dem Homepage- und dem WWW-Server läuft das Serverprogramm Apache. Wenn Sie eine Zugriffsbeschränkung auf einem nicht von IT.SERVICES administrierten Apache-Server anlegen möchten, beachten Sie bitte, dass der Standardname für die Datei zur Zugriffssteuerung .htaccess lautet.

ZUGRIFFSBESCHRÄNKUNGEN EINRICHTEN

Zugriffsbeschränkung durch Benutzername und Passwort

Zunächst sollten Sie die Datei .admusers erstellen. In diese Datei tragen Sie zeilenweise Benutzername und dazugehöriges verschlüsseltes Kennwort, jeweils durch einen Doppelpunkt getrennt, ein. Hier ein Beispiel:

```
Benutzer1:p8KRGXDSQX/qQ
Benutzer2:p8lX4erUUYGJI
```

Zur einfachen Erstellung eines verschlüsselten Kennworts haben wir folgendes Skript auf unseren Seiten bereitgestellt:
http://www.ruhr-uni-bochum.de/cgi-bin/crypt
Geben Sie das gewünschte Kennwort in das Formular ein, drücken Sie die Eingabetaste und kopieren Sie das nun angezeigte verschlüsselte Kennwort am besten mit Cut-and-Paste in die Datei .admusers.
Nun sollten Sie die Datei .admopts erstellen. Hier ein Beispiel (alle kursiv geschriebenen Angaben müssen Sie durch Ihre individuellen Parameter ersetzen):

```
AuthName "Name des geschützten Bereiches"
AuthType Basic
AuthUserFile Pfad zur Datei .admusers
Require valid-user oder user Benutzername(n)
```

Zur Erläuterung:

Zeile 1: Geben Sie in Anführungsstrichen einen frei wählbaren Namen für den geschützten Bereich ein. Dieser Name wird beim Aufrufen des geschützten Bereiches im Eingabefenster für Benutzername und Passwort angezeigt.

Zeile 2: Übernehmen Sie diese Zeile ohne Änderungen.

Zeile 3: Hier muss der vollständige Pfad zur Datei .admusers angegeben werden. Die häufigste Fehlerquelle bei der Zugriffsbeschränkung durch Benutzername und Passwort liegt in einer falschen Pfadangabe an dieser Stelle. Da die Server auf einem UNIX-System laufen, muss die Pfadangabe mit dem Backslash („/“) und nicht umgekehrt („\“) gebildet werden. Hier nun die Regeln zur Bildung der vollen Pfadangabe (alle kursiv geschriebenen Angaben sind durch Ihre individuellen Parameter zu ersetzen):

- bei Gruppendiensten:
  /home/www/groups/*Gruppenkennung/Gruppenname/evtl. Unterverzeichnis(se)*/.admusers
  Beispiel: /home/www/groups/judounzi/judo/intern/.admusers

- bei älteren WWW-Berechtigungen unter „www-public“:
  /WWW/*LoginID/evtl. Unterverzeichnis(se)*/.admusers
  Beispiel : /WWW/judounzi/intern/.admusers
- für den Homepageserver:
  /home/www/home/*erster Buchstabe LoginID/LoginID/evtl. Unterverzeichnis(se)*/.admusers
  Beispiel: /home/www/home/p/passembk/geheim/.admusers

Zeile 4: Hier legen Sie schließlich fest, welche Benutzer Zugriff auf die geschützten Seiten haben sollen. Wenn Sie „Require valid-user“ eintragen, werden alle in der Datei .admusers erfassten Benutzer akzeptiert. Sie können auch einzelne Benutzer auswählen, indem Sie zuerst das Wort „user“ und dann deren Benutzernamen an Stelle von „valid-user“ durch Leerzeichen getrennt eintragen.

Zugriffsbeschränkung durch IP-Adresse bzw. Domain

Neben der Zugriffsbeschränkung durch Benutzername und Passwort ist auf den WWW-Servern eine Zugriffsbeschränkung anhand von IP-Adressen bzw. Domainnamen möglich. So können Sie zum Beispiel den Zugriff auf Ihre WWW-Seiten nur für Rechner mit einer IP-Adresse der Ruhr-Universität Bochum oder nur für Rechner aus dem Subnetz Ihres Instituts erlauben.

Ebenso wie für die Zugriffsbeschränkung durch Benutzername und Passwort müssen Sie für die Zugriffsbeschränkung durch IP-Adresse bzw. Domain die Datei .admopts anlegen, editieren und in das gewünschte Verzeichnis Ihrer WWW-Präsenz laden.

Hier ein Beispiel für die Einträge zur Zugriffsbeschränkung durch IP-Adresse bzw. Domain für die Datei .admopts (wenn Sie bereits eine Zugriffsbeschränkung durch Benutzername und Passwort eingerichtet haben, fügen Sie die Angaben bitte am Ende der Datei ein):

```
Order deny,allow
deny from all
allow from 134.147.128
```

Generell gibt es für die Zugriffsbeschränkung durch IP-Adresse bzw. Domainname zwei Direktiven zur Zugriffssteuerung: deny (verbieten) und allow (zulassen). Die erste Zeile im Beispiel bewirkt, dass zunächst die deny-Direktive und erst danach die allow-Direktive abgearbeitet wird. Durch die zweite Zeile unterbinden Sie aus Sicherheitsgründen den Zugriff auf das Verzeichnis und die darin liegenden Dateien komplett, um dann nur den in der dritten Zeile definierten Rechnern Zugriff zu geben. In unserem Beispiel ist dies das gesamte Subnetz 134.147.128.

Neben Subnetzen können Sie auch komplette IP-Adressen oder Domainnamen wie etwa it-services.ruhr-uni-bochum.de verwenden. Zudem können Sie mehrere „allow from“-Einträge vornehmen. Wenn Sie kein komplettes Class-C Subnetz besitzen, den Zugriff aber nur für Ihr Subnetz freigeben und nicht jede IP-Adresse Ihres Subnetzes einzeln eintragen möchten, geben Sie einfach ‚Subnetznummer/Subnetzmaske‘ in einem „allow from“-Eintrag an.

Zugriffsbeschränkung auf RUB-intern bei IPv6 und IPv4

Seit Einführung der IPv6-Adressen in großen Teilen der RUB muss für eine uniinterne Zugriffsbeschränkung mehr gemacht werden als nur den IP-Bereich 134.147 freizugeben. IPv (Internet Protocol Version) ist ein Verfahren zur Übertragung von Daten in paketvermittelnden Rechnernetzen. Im Internet löst IPv6 die vorherige Version des Internet Protocols ab, da es eine deutlich größere Zahl möglicher Adressen bietet.

Alle Rechner der RUB, die über IPv4 ins Internet gelangen, haben eine IP-Adresse aus dem Class-B Netz und damit eine IP-Adresse 134.147.x.y. Dies gilt ebenfalls für externe Rechner, die sich über einen VPN-Tunnel Zugang ins Hochschulnetz holen.

Bei IPv6 ist zusätzlich ein weiterer Adressbereich freizuschalten. Eine IPv6-Adresse wird inzwischen immer häufiger in lokalen Subnetzen genutzt, sowie automatisch bei Zugängen über H.I.R.N.-Port oder Eduroam (WLAN oder Studierendenwohnheime) zugeteilt. Auch verbreiten sich innerhalb der RUB zunehmend lokale, ungeroutete IP-Adressen aus dem 10er Netz, d.h. IP-Adressen der Form 10.x.y.z

```
order deny,allow
deny from all
allow from 134.147
allow from 2001:638:50c::/48
allow from 10
allow from .ruhr-uni-bochum.de
allow from .ipv6.ruhr-uni-bochum.de
deny from www-cache.ruhr-uni-bochum.de
```

Kombination der beiden Arten der Zugriffsbeschränkung

Eine sinnvolle Kombination von Zugriffsbeschränkung durch IP-Adresse bzw. Domain und Benutzername / Passwort ist folgender Fall: Sie möchten den Zugriff auf Ihre WWW-Präsenz von Ihrem Institut aus uneingeschränkt erlauben, von außerhalb aber automatisch Benutzername und Passwort abfragen, damit ausgewählte Benutzer die Informationen auch außerhalb Ihres Instituts mit Benutzername und Passwort abrufen können.

Legen Sie wie beschrieben die Dateien .admusers und .admopts an und fügen Sie am Ende der Datei .admopts die Zeile ‚Satisfy any‘ ein. Durch diesen Eintrag wird zunächst überprüft, ob der aufrufende Computer zu den in „Allow from“ definierten Rechnern gehört. Ist dies nicht der Fall, wir die Passwortabfrage gestartet. Wenn Sie den Eintrag „Satisfy any“ nicht vornehmen, müssen alle Bedingungen aus der Datei .admopts erfüllt sein, d.h. der zugreifende Rechner muss eine Adresse aus den in den „Allow from“-Einträge definierten IP-Adressen bzw. Domains haben und Benutzername und Passwort werden abgefragt.

Hier ein Beispiel für die Datei **.admopts**:

```
AuthName „Name des geschützten Bereiches“
AuthType Basic
AuthUserFile Pfad zur Datei .admusers
Order deny,allow
Require valid-user
Deny from all
Allow from 134.147.128
Satisfy any
```

Alle Rechner mit einer IP-Adresse, die mit 134.147.128 beginnt, können die Dateien ohne Benutzereingabe anzeigen. Bei allen anderen Rechnern wird der Benutzer zur Eingabe von Benutzername und Passwort aufgefordert. Akzeptiert werden alle Benutzer/Passwort-Kombinationen aus der Datei, die mit dem Eintrag „AuthUserFile“ bestimmt wird.

Zugriffsbeschränkung für ausgewählte Dateien

Wenn Sie nur ausgewählte Dateien mit einer Zugriffsbeschränkung belegen möchten nutzen Sie bitte folgendes Beispiel für die Datei **.admopts**:

```
AuthName „Name des geschützten Bereiches“
AuthType Basic
AuthUserFile Pfad zur Datei .admusers
Order deny,allow
<Files Dateiname>
Require valid-user oder user Benutzername(n)
Deny from all
Allow from 134.147.128
Satisfy any
</Files>
```

Geben Sie in Zeile 5 an Stelle des Dateinamen den Namen der zu schützenden Datei an. Alle zwischen <Files *Dateiname*> und </Files> eingetragenen Einstellungen gelten nun nur für den angegebenen Dateinamen. Sie können hier natürlich auch andere Einträge als in unserem Beispiel vornehmen.

Bei Fragen & Problemen

Bei Fragen und Problemen können Sie sich an unseren Helpdesk wenden: **its-helpdesk@ruhr-uni-bochum.de.**