Passwortschutz für die Website

Geschlossene Gesellschaft

Ob für Fotos Ihrer Geburtstags-Fete oder interne Infos Ihres Vereins – so richten Sie in Ihrer Website einen passwortgeschützten Bereich ein

Von Oberammergau bis Australien haben Millionen Surfer weltweit Zugriff auf Ihre Webseiten. Aber vielleicht sind nicht alle Informationen für die breite Öffentlichkeit gedacht. Halten Sie etwa Verwandte und Bekannte mit privaten Fotos Ihres Nachwuchses auf dem Laufenden? Oder bieten Sie den Besuchern Ihrer Seminare ergänzende Unterlagen exklusiv online an? Es gibt jede Menge Beispiele für Daten, die nicht jeden etwas angehen. Richten Sie für diese Zwecke einen geschützten Bereich innerhalb Ihrer Website ein. Die Surfer erhalten zu diesen Seiten nur dann Zugang, wenn sie die korrekten Zugangsdaten wissen.

com! stellt Ihnen drei Lösungen für passwortgeschützte Webseiten vor: Sie können die Seiten mit Hilfe einer *.htaccess*-Datei, mit Javascript oder mit PHP vor neugierigen Blicken verbergen. Zu allen Möglichkeiten finden Sie ein Beispiel auf der com!-Heft-CD 1 unter „HomeP@ge“, „Praxis & Tuning“.

.htaccess-Datei anlegen

Mit *.htaccess*-Dateien schützen Sie Verzeichnisse auf dem weit verbreiteten Apache-Webserver. Gehört Ihr Provider zu den wenigen, die einen Windows-Server einsetzen, können Sie diesen Weg nicht beschreiten. Will jemand über den Browser auf ein so geschütztes Verzeichnis zugreifen, muss er eine Benutzerkennung und das dazugehörige Passwort eingeben.

Den Schutz richten Sie in vier Schritten ein: Sie legen eine *.htaccess*-Datei an und laden diese Datei in das zu schützende Verzeichnis. Anschließend tragen Sie die Benutzerkennungen und Passwörter in eine Datei mit dem Namen *.htpasswd* ein und kopieren diese in das Stammverzeichnis Ihrer Homepage.

So gehen Sie im Einzelnen vor: Starten Sie den Windows-Editor oder Wordpad und geben Sie folgende Zeilen ein:

```
AuthUserFile /pfad/.htpasswd
AuthName "Bitte anmelden"
AuthType Basic
Require valid-user
```

Bei **`AuthUserFile`** tragen Sie den kompletten Pfad zu der Datei *.htpasswd* ein, in der die Benutzerkennungen und Passwörter gespeichert sind. Beachten Sie: Der Pfad ist weder ein URL noch bezieht er sich auf das oberste Verzeichnis Ihrer Website. Geben Sie vielmehr den tatsächlichen Verzeichnispfad auf dem Rechner Ihres Providers an. Kennen Sie diesen nicht, lesen Sie die Informationsseiten Ihres Webhosters oder fragen Sie den Administrator Ihres Webservers.

Bei **`AuthName`** geben Sie einen Text an, der in dem Fenster als Meldung erscheint, das um die Eingabe der Zugangsdaten bittet. Mit **`AuthType Basic`** legen Sie fest, dass Sie den Standard-Passwortschutz verwenden möchten. Bei diesem Schutztyp sind die Zugriffsberechtigungen in einer separaten Datei ausgelagert. Mit Windows kann es passieren, dass sich die Datei nicht unter dem Namen *.htaccess* speichern lässt. Dieses Problem umgehen Sie wie folgt: Legen Sie die Datei unter dem Namen *htaccess.txt* auf Ihrer Festplatte ab. Laden Sie diese per FTP in das gewünschte Verzeichnis auf dem Webserver und benennen Sie die Datei dort mit der entsprechenden Funktion Ihres ▶

Foto: Corbis

Um auf das Verzeichnis zugreifen zu können, sind Kennung und Passwort einzugeben

FTP-Programms in *.htaccess* um. Wichtig beim Upload: Stellen Sie als Übertragungsmodus *ASCII* ein.

Benutzer anlegen

Im gegenwärtigen Zustand darf kein Mensch auf das geschützte Verzeichnis zugreifen, da es noch keine Benutzer gibt. Legen Sie daher nun die Accounts für die Besucher an, die Sie für den geschützten Bereich zulassen möchten. Erstellen Sie entweder für jeden Benutzer eine eigene Kennung mit Passwort oder richten Sie lediglich eine einzige Zugangskennung ein, die Sie dem gesamten Nutzerkreis bekannt geben.

Schreiben Sie sämtliche Zugangsdaten in eine Datei mit dem Namen *.htpasswd*. Verwenden Sie in der Datei für jeden Account eine eigene Zeile. Fügen Sie in die Zeile den Benutzernamen und das Passwort getrennt durch einen Doppelpunkt ein. Beachten Sie dabei, dass das Passwort bei Unix- und Linux-Servern, die bei den meisten Providern zum Einsatz kommen, verschlüsselt angegeben werden muss. Aber wie verschlüsseln Sie die Angaben?

Im Web finden Sie diverse Online-Generatoren, die das Passwort in die verschlüsselte Form umwandeln. Geben Sie etwa unter *www.kxs.net/support/htaccess_pw.html* den Benutzernamen und das Passwort ein. Über einen Mausklick auf *Create Password* erstellt der Generator eine Zeile mit dem verschlüsselten Passwort, die Sie aus dem Browser-Fenster in die Passwort-Datei kopieren.

Bei *www.kxs.net* lassen sich die Passwörter für die Datei *.htpasswd* online generieren

Unter der Webadresse *www.affordable-website-design.me.uk/htaccess_generator.html* erzeugen Sie nicht nur den passenden Eintrag für die Passwort-Datei, sondern zusätzlich eine vollständige *.htaccess*-Datei.

Haben Sie sämtliche Benutzer in die Datei *.htpasswd* eingetragen, können Sie diese im Ascii-Modus auf Ihren Webserver laden. Legen Sie *.htpasswd* anschließend in dem Verzeichnis ab, das Sie zuvor in der Datei *.htaccess* angegeben haben. Mögen Sie es noch etwas komfortabler? Auf der com!-Heft-CD finden Sie eine Testversion des praktischen Tools Htpasswd Generator. Mit diesem klei-nen Programm lassen sich die beiden Dateien *.htaccess* und *.htpasswd* in wenigen Schritten erzeugen und – das ist der besondere Clou – per integrierter FTP-Funktion direkt an die passende Stelle auf den Webserver hochladen. Besser geht's nicht.

Passwortschutz testen

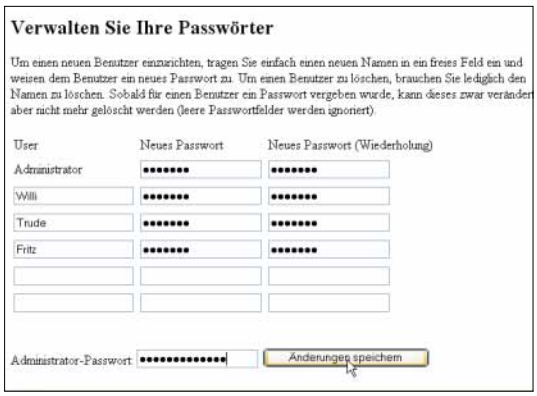
Mit dem Tool Htpasswd Generator schieben Sie die Dateien für den *.htaccess*-Schutz per FTP auf den Webserver

Der Verzeichnisschutz ist nun eingerichtet. Rufen Sie das Verzeichnis jetzt über den Browser auf und testen Sie, ob sich die Tür mit Ihrer Kennung und dem Passwort öffnen lässt. Gibt es dabei Probleme, prü-

Beispiel Strato

Was Sie von Ihrem Webhoster bei der Einrichtung eines geschützten Bereichs erwarten dürfen, zeigt com! Ihnen am Beispiel von Strato. Bei den Powerweb- und Premium-Paketen lassen sich Ihre Verzeichnisse mit *.htaccess* sichern.

Bei Strato müssen Sie *.htaccess* und *.htpasswd* nicht von Hand erstellen und pflegen. In der CGI-Bibliothek finden Sie zwei Module, mit denen sich diese Arbeiten über eine komfortablere Weboberfläche ausführen lassen.



Bei Strato verwalten Sie die Nutzerdaten für die geschützten Bereiche komfortabel über ein Webformular

Das Grundgerüst für die Datei *.htaccess* erstellen Sie mit dem CGI-Skript *www.wunschname.de/cgi-bin/htaccess.pl*. Das Skript gibt Ihnen unter anderem den tatsächlichen Pfad zum obersten Verzeichnis Ihrer Website aus. Der entsprechende Eintrag lautet beispielsweise:

```
AuthUserFile /home/strato/www/mu/
www.mustersite.de/htdocs/.htpasswd
```

Laden Sie die Datei *.htaccess* in sämtliche Verzeichnisse Ihrer Website hoch, bei denen Sie den Zugriff einschränken möchten. Erstellen Sie im nächsten Schritt mit dem Windows-Editor die Datei *.htpasswd* und fügen Sie dort die folgende Zeile für den Benutzer Administrator ein:

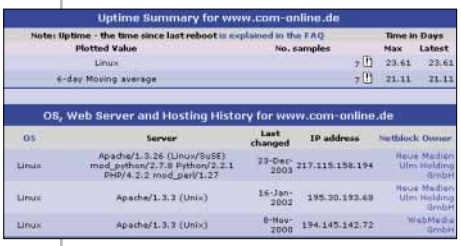
```
Administrator:abu8zJlPjwMSU
```

Das verschlüsselte Passwort lautet ebenfalls *Administrator*. Laden Sie diese Datei in das oberste Verzeichnis Ihrer Website.

Die weiteren Benutzer verwalten Sie nun recht komfortabel und schnell. Rufen Sie dazu das Skript *www.wunschname.de/cgi-bin/passwortschutz.pl* auf. Über ein Formular lassen sich die neuen Accounts hinzufügen und die Passwörter der bestehenden Benutzerkennungen ändern.

Server-Typ ermitteln

Der *.htaccess*-Schutz funktioniert nicht mit allen Webserver-Typen. Bevor Sie mit Ihrem Provider Kontakt aufnehmen, lässt sich auf der Seite *http://uptime.netcraft.com* ermitteln, welchen Webserver dieser einsetzt. Geben Sie dazu Ihren Domain-Namen in das Eingabefeld hinter *Whats that site running?* ein, und drücken Sie die Eingabetaste. In einem ausführlichen Bericht erfahren Sie, auf welchem Betriebssystem und mit welchem Webserver Ihr Webspace läuft.



Bei *http://uptime.netcraft.com* erhalten Sie Informationen über den Webserver

fen Sie noch einmal die folgenden Punkte: Setzt Ihr Provider tatsächlich einen Apache-Server ein, bei dem sich die Verzeichnisse mit *.htaccess* schützen lassen? Haben Sie die beiden Dateien im Ascii-Modus auf den Webserver übertragen? Haben Sie bei **`AuthUserFile`** den tatsächlichen Pfad der Passwort-Datei auf dem Server angegeben? Prüfen Sie noch einmal den Inhalt der *.htaccess*-Datei. Entfernen Sie überflüssige Zeilenumbrüche und Leerzeichen.

In seltenen Fällen ist die Möglichkeit, per *.htaccess*-Datei zu schützen, abgeschaltet. Wenden Sie sich an Ihren Provider, um diese Frage zu klären. Um den Passwortschutz später wieder aufzuheben, löschen Sie lediglich die Datei *.htaccess* aus dem jeweiligen Verzeichnis.

Schutz mit Javascript

Unterstützt Ihr Webserver den Passwortschutz mit *.htaccess*-Dateien nicht, versuchen Sie es mit Javascript. Im Web finden Sie verschiedene Lösungen für den Passwortschutz. Lassen Sie jedoch die Finger

Seitenschutz mit Javascript: Das Passwort ist zugleich der Name der geschützten Datei

von Skripts, bei denen Sie das Passwort unverschlüsselt in den Quelltext eingeben müssen. Ein Blick in den Code genügt, und schon haben die Besucher den Schlüssel zu Ihren privaten Seiten.

Raffinierter und weitaus sicherer ist die im Folgenden beschriebene Lösung: Bei diesem Javascript notieren Sie das Passwort nicht im Quelltext, sondern es ist Teil des Namens der zu schützenden Datei. Fügen Sie dazu das folgende Formular in den **`<body>`**-Bereich der aufrufenden Seite ein:

```
<form name="eingabe"
onSubmit="return false;">
Passwort:
<input type="text" name="pw"
size="10">
<input type="button" value="Los!"
onClick="zugang();">
</form>
```

So funktioniert das Skript im Einzelnen: In das Eingabefeld **`pw`** geben Sie das Passwort ein. Mit einem Klick auf die Schaltfläche *Los!* rufen Sie die Funktion **`zugang()`** auf.

Fügen Sie diese Funktion mit den folgenden Skriptzeilen in den **`<head>`**-Bereich der Seite ein:

```
<script language="JavaScript">
function zugang()
{
top.location.href=document.eingabe
.pw.value+".html";
}
</script>
```

An die eingegebene Zeichenkette **`document.eingabe.pw.value`** hängt das Skript die Endung *.html* an. Speichern Sie in demselben Ordner wie die aufrufende Seite beispielsweise die Datei *1T45xyz.html* ab, so lautet das Passwort *1T45xyz*. Es ist sehr unwahrscheinlich, dass ein Surfer diesen Namen errät.

Eine Hintertür sollten Sie jedoch noch schließen: Gibt ein Besucher lediglich den Verzeichnisnamen ein, so zeigt der Browser je nach Einstellung des Servers eine Liste mit allen Dateien des Ordners an. Die Liste enthält also auch den Namen der versteckten Datei. Fügen Sie in das Verzeichnis daher stets eine Datei mit dem Namen *index.html* ein. Diese Standardseite erscheint dann an Stelle der Liste im Browser-Fenster.

Alternative PHP

Eine weitere sichere Möglichkeit bietet PHP. Die Skriptbefehle werden auf dem Server ausgeführt und nur das Ergebnis ist im Browser zu sehen. So haben die Surfer über den Browser keine Möglichkeit, das Passwort einzusehen. Fügen Sie auf der Seite, über die der Zugang schließlich erfolgen soll, das folgende Formular ein:

```
<form action="intern.php"
 method="post">
<input type="password" name="pwd">
<input type="submit"
value="Eintreten"> </form>
```

Mit dem Formular fragen Sie das Passwort für den geschützten Bereich ab. Klicken Sie auf die Schaltfläche *Eintreten*, so wird das bei **`action`** angegebene PHP-Skript *intern.php* aufgerufen. Beim folgenden Beispiel leiten Sie damit den Surfer bei korrekter Eingabe des Passworts direkt zu einem anderen URL weiter:

```
<html>
<head>
<?php
if($_POST[pwd] == "willi"){
echo "<meta http-equiv=\"refresh\"
content=\"0;URL=
http://www.com-online.de\">"; } ?>
</head>
<body>
Kein Zugang!
</body>
</html>
```

Falls das eingegebene Passwort nicht mit der Vorgabe **`willi`** übereinstimmt, bleibt der Text **`Kein Zugang!`** im Browser-Fenster stehen. ■

Volker Hinzen/Andreas Dumont
homepage@com-online.de

Sinnvolle Passwörter

Der Schutz Ihrer Seiten ist nur so gut wie das verwendete Passwort. Beachten Sie die folgenden Hinweise bei der Wahl eines geeigneten Zugangsschlüssels:

Ein Passwort sollte mindestens sechs Zeichen lang sein. Kombinieren Sie Zahlen, Buchstaben und Sonderzeichen. Schreiben Sie die Buchstaben zum Teil groß und zum Teil klein. Vermeiden Sie triviale Passwörter wie „1234“ oder „xxx“. Verwenden Sie die Benutzerkennung nicht auch als Passwort. Das Passwort sollte dennoch leicht zu merken sein, damit die Nutzer es nicht aufschreiben müssen. Vermeiden Sie Begriffe, die zum Thema Ihrer Website passen. Das Passwort „HTML“ ist für eine Site zum Thema Webdesign ungeeignet.