Datei- und Verzeichnisrechte, Erläuterungen für PRES-Nutzer

1. Benutzer-/Gruppenrechte
   1. Einführung
   2. Benutzerrechte
   3. Gruppenrechte
   4. Rechte anderer
2. Rechteanpassung
   1. Webspace
   2. (Virtual-)Root-Server

1. Benutzer-/Gruppenrechte

1. Einführung

Linux-basierende Systeme, also die, die die meisten Webhoster nutzen, haben ein recht ausgeklügeltes Rechtesystem. So werden dort für den Benutzer, die zugehörige Gruppe und für alle Anderen jeweils eigene Rechte verteilt. In den meisten FTP-Programmen sind diese meist auf 2 verschiedene Arten dargestellt.

Entweder werden die Rechte in einer Zahlendarstellung angezeigt, oder es werden die Rechte einzeln, wie auch unter Linux selbst, detailliert dargestellt.

Beispiel: „774“ und „rwxrwxr--“ stellen beide die selben Rechte dar, nur in unterschiedlicher Schreibweise.

So ist bei der Übertragung in die detaillierte Darstellung nur zu beachten, dass
r = 4
w=2
x=1

Damit lassen sich die Ansichten in einander übertragen.

2. Benutzerrechte

Jeder Benutzer kann für seine Dateien und Verzeichnisse einzeln Rechte vergeben, um z.B. zu verhindern, dass bestimmte Dateien auch von einem selbst zufällig verändert werden.

3. Gruppenrechte

Bei den Gruppenrechten gilt das gleiche, wie bei den Benutzerrechten, nur dass diese Rechte für die Gruppe gelten, der die Dateien oder Ordner zugeordnet sind.

4. Rechte Anderer

Die Rechte Anderer sind der letzte Block, den es zu beachten gilt, denn diese Rechte gelten für alle, die nicht mit den Benutzerrechten oder den Gruppenrechten erfasst werden. Bei einem Webserver sind meistens diese Rechte entscheidend, da die meisten Daten mit einem Benuteraccount(FTP/SSH/SCP) auf den Server hoch geladen werden. Um diesen Umstand etwas zu verbessern, lesen sie bitte im 2. Abschnitt weiter, dort wird ihnen erklärt, wie sie diese Rechteverteilung besser an ihr Sicherheitsgefühl anpassen können.

2. Rechteanpassung

1. Webspace

Bei einem normalen Webspace-Account ist es meistens nicht so ohne weiteres möglich, die Rechte anzupassen. In Ihrem FTP-Programm(Vielleicht verwenden Sie auch hier bereits SSH/SCP, auch dort gibt es entsprechende Anzeigen und Einstellmöglichkeiten, lesen Sie dazu bitte Unterabschnitt 2. bei den Servern nach.) sollte Ihnen angezeigt werden, welchem Benutzer, bzw. welcher Gruppe ihre Daten derzeit zugeordnet sind. Sollten Sie über FTP Zugang zu den Log-Files ihrer Domain haben, schauen Sie dort bitte nach, welcher Gruppe diese Dateien gehören. Ich werde Ihnen im folgenden eine kleine Aufstellung von häufig benutzten Namen geben.

Häufig genutzte Gruppennamen für die Webserver sind:

- www
- www-data
- nogroup

Sollten Ihre Log-Dateien etwas anderes als Gruppennamen haben, könnte auch dies richtig sein, denn es gibt keine all gemeingültige Konvention über die Nutzung eines bestimmten Gruppennamens.
Wenn Sie auf Nummer sicher gehen möchten, kontaktieren Sie doch ihren Hoster, oder lesen Sie sich die FAQ's durch, vielleicht sind die benötigten Informationen dort bereits enthalten.

Wenn Sie dies getan haben, dann ändern Sie bitte den Gruppennamen der „page.restrictor.php“ in den von Shnen gefundenen Gruppennamen.
TIPP: Ändern Sie nicht den Benutzernamen, denn sonst könnte es passieren, dass Sie nicht mehr an ihre Daten kommen, bzw. Sie diese nicht mehr verändern können.

Danach können Sie die Rechte der „page.restrictor.php“ auf 760(bzw. „rwxrw----“) oder auch 764(bzw. „rwxrw-r--“) ändern, so dass nur Sie selbst den vollen Zugriff auf die Datei haben und der Webserver diese Datei noch lesen und auch schreiben kann, was zum Updaten nötig ist.

Mit der Datei „page.restrictor.log“ kann genauso verfahren werden, die Datei „page,restrictor.inc“ benötigt keine Schreibrechte im Gruppenbereich und kann daher mit 740(bzw. „rwxr-----“) oder auch 744(bzw. „rwxr—r--“) gesetzt werden. Des weiteren kann auch die erste 7 im Benutzerbereich durch eine 6 ersetzt werden, da auch der Benutzer die Dateien nicht unbedingt ausführen können muss.

Somit sind Ihre Dateien vor einem Angriff von anderen Mitbenutzern ihres Servers besser geschützt. Nicht jedoch vor Veränderungen durch verschaffen des Zugangs über ihr Benutzerkonto oder auch vor Veränderungen durch die Rechte des Systemadministrators, dessen Rechte sich Hacker auch gern zu nutze machen.

2. (Virtual-)Root-Server

Bei einem eigenen Server ist die Sache ähnlich zu der oben Beschriebenen Problematik, jedoch ist es hier einfacher, den benutzten Gruppennamen herauszufinden. Denn entweder haben Sie diesen bereits selbst einmal konfiguriert, oder können ihn ganz einfach aus der Konfigurationsdatei ihres Web-Server-Programms auslesen.

Schauen Sie bitte den benutzten Gruppennamen in der Datei „httpd.conf“, bzw. „apache.conf“ oder auch „apache2.conf“ nach.

Danach verfahren Sie wie bereits im vorherigen Abschnitt beschrieben, da Sie aber wahrscheinlich eher SSH, bzw SCP als Übertragungssystem einsetzen, werden Sie wahrscheinlich die Rechte entweder über den Eintrag Eigenschaften im Kontext-Menu ändern, oder, falls Sie eher auf der Konsole ihres Servers arbeiten, die Kommandos „chgrp“ und „chmod“ verwenden.

Und auch hier gilt, Ihre Daten sind nur so sicher, wie die Sicherheitsrichtlinie Ihres Servers.