

1.4.A Anwendung/Berechtigungen – Arbeitsblatt

- Bearbeitungsdauer: 60 min
- Ergebnissicherung: Auf dem Server
- Hilfsmittel: Leittext, Software

Aufgabe 1: Zugriffsrechte für Dateien

Erstellen Sie die folgenden Berechtigungen! Versuchen Sie, so wenig Rechte wie möglich zu geben!

- Legen Sie folgende Verzeichnisse **direkt** in ihrem persönlichen Verzeichnis (hier gekennzeichnet durch ~) an!
~/daten/docs
~/daten/sources
~/daten/scripts
~/public_html
~/public_html/upload
~/public_html/download
- Erstellen Sie folgende Dateien:
~/daten/sources/geheim.tex
~/daten/scripts/backup.py
~/public_html/index.html
- Die Datei geheim.tex soll nur für den Besitzer schreib- und lesbar sein; alle anderen haben keinen Zugriff.
- Die Datei index.html soll für den Besitzer und die Besitzgruppe schreib- und lesbar sein. Alle anderen sollen nur Leserecht erhalten.
- Die Skript-Datei backup.py soll für den Besitzer les-, schreib- und ausführbar sein; die Gruppenmitglieder sollen die Datei ausführen können; alle anderen sollen auf die Datei in keiner Weise zugreifen können.

Aufgabe 2: Zugriffsrechte für Verzeichnisse

Erstellen Sie die folgenden Berechtigungen! Versuchen Sie auch hier, so wenig Rechte wie möglich zu geben! Die Besitzer und Besitzgruppen sollen hier nicht verändert werden.

- Im Verzeichnis docs soll nur der Besitzer Dateien anlegen und löschen können, alle anderen sollen nicht einmal sehen können, welche Dateien in diesem Verzeichnis liegen.
- Im Verzeichnis sources soll nur der Besitzer Dateien anlegen und löschen können. Die Gruppenmitglieder sollen sehen können, welche Dateien und sonstigen Elemente in diesem Verzeichnis liegen. Alle anderen sollen beides nicht können.
- Im Verzeichnis scripts soll der Besitzer Dateien anlegen und löschen können. Die Mitglieder der Gruppe und alle anderen sollen die Elemente des Verzeichnisses benutzen können.
- Im Verzeichnis public_html soll der Besitzer Dateien anlegen und löschen können; die Mitglieder der Gruppe sollen in Unterverzeichnisse wechseln können; die Mitglieder der Gruppe und alle anderen sollen sehen können, welche Elemente in dem Verzeichnis liegen.
- Das Verzeichnis download soll für Besitzer und Gruppenmitglieder nur erlauben, die Namen der enthaltenen Dateien aufzulisten und die Inhalte dieser Dateien zu benutzen. Alle anderen sollen nichts können.
- Das Verzeichnis upload soll für Besitzer und Gruppenmitglieder nur erlauben, Dateien anzulegen und zu löschen. Alle anderen sollen nichts können.

Aufgabe 3: Tabelle der erlaubten Aktionen

- Legen Sie das Verzeichnis `~/verz/` und darin eine (nicht leere) Textdatei `~/verz/datei.txt` an!
- Tragen Sie bitte ein, welche der folgenden Aktionen für die Datei `~/verz/datei.txt` erlaubt sind, falls jeweils die entsprechenden Berechtigungs-Bits gesetzt wurden:
 - C = create = Datei anlegen, mit Editor
 - D = delete = Datei löschen, mit `rm`
 - E = delete = Datei nur als Eigentümer löschen, mit `rm`
 - R = read = Datei-Inhalt lesen, mit `cat`
 - W = write = Datei-Inhalt schreiben, mit Editor
 - X = execute = Datei ausführen (Eingabe des Namens)
 - = none = keine der genannten Aktionen

	Dat	---	--x	-w-	-wx	r--	r-x	rw-	rwX
Verz	-	0	1	2	3	4	5	6	7
d---	0								
d--x	1								
d-w-	2								
d-wx	3								
dr--	4								
dr-x	5								
drw-	6								
drwx	7					CDR			
drwt	17								

- Zur Hilfe bei der Lösung bietet sich (im Zweifelsfall) das Ausprobieren anhand der angelegten Datei an.
- Mit dem Programm `opendatei.c` kann man außerdem erkennen, welcher der folgenden Systemaufrufe nach dem Setzen der Berechtigungen erlaubt ist und welcher nicht:
 - `opendir()` und `readdir()`: den Verzeichnisinhalt öffnen und jeweils einen Eintrag lesen,
 - `stat()`: den I-Node (und damit den Status bzw. die Eigenschaften) der Datei lesen,
 - `open()` und `read()`: den Dateiinhalt öffnen und lesen.