

1.2.6. Sicherheitsgrundlagen in Linux

Lernsituation Dateiberechtigungen

Ausgangssituation:

Du bist Teil der IT-Abteilung eines mittelständischen Unternehmens, das das Sicherheitsniveau seiner Linux-Server erhöhen möchte. Deine Aufgabe ist es, zu lernen, wie man Dateiberechtigungen korrekt vergibt und verwaltet. In einem Testsystem wirst du verschiedene Benutzer und Gruppen anlegen, um die Berechtigungen auf Dateien und Verzeichnisse zu testen. Dabei lernst du, wie du den Zugriff auf sensible Daten einschränken und die Sicherheitsrichtlinien des Unternehmens umsetzen kannst.

Lernaufgabe:

Du bist neu im Team und erhältst die Aufgabe, die Dateiberechtigungen auf einem Linux-Server zu überprüfen und zu optimieren. Folge diesen Schritten:

1. **Anlegen von Benutzern und Gruppen:**
 - Erstelle drei neue Benutzer: `alice`, `bob`, und `charlie`.
 - Erstelle eine neue Gruppe `projektteam` und füge alle drei Benutzer dieser Gruppe hinzu.
2. **Verzeichnisstruktur einrichten:**
 - Erstelle ein Verzeichnis namens `/projekt` und stelle sicher, dass nur Mitglieder der Gruppe `projektteam` darauf zugreifen dürfen.
 - Innerhalb dieses Verzeichnisses erstellst du zwei Unterverzeichnisse: `/projekt/daten` und `/projekt/berichte`.
 - Achte darauf, dass nur `alice` Schreibrechte für das Verzeichnis `/projekt/berichte` hat, während die anderen Benutzer nur Lesezugriff haben.
3. **Überprüfung der Berechtigungen:**
 - Verwende den Befehl `ls -l`, um die aktuellen Berechtigungen der Verzeichnisse und Dateien zu überprüfen.
 - Ändere die Berechtigungen mit `chmod`, um sicherzustellen, dass alle Anforderungen erfüllt sind (z.B. Schreibrechte für eine bestimmte Gruppe).
4. **Spezielle Berechtigungen anwenden (Recherche & Extraaufgabe):**
 - Setze das Sticky-Bit für das Verzeichnis `/projekt/daten`, damit nur die Ersteller von Dateien diese löschen können.
 - Für ein Skript in `/projekt/skripte/start.sh` vergibst du die Berechtigung, dass es immer mit den Rechten des Eigentümers (`SUID`) ausgeführt wird, um bestimmte Systemaufgaben zu erledigen.
5. **Fehlerbehebung und Optimierung (Recherche & Extraaufgabe):**

- Du entdeckst, dass **charlie** unbefugten Zugriff auf sensible Daten hat. Überprüfe seine Dateiberechtigungen und passe sie entsprechend an.
- Implementiere das "Least-Privilege-Prinzip", sodass jeder Benutzer nur die minimal notwendigen Rechte für seine Aufgaben erhält.

Reflexion:

- Erkläre, warum es wichtig ist, die Dateiberechtigungen sorgfältig zu verwalten.
- Welche Risiken bestehen, wenn die Berechtigungen nicht richtig gesetzt sind?
- Wie trägt das Sticky-Bit zur Sicherheit in gemeinsamen Verzeichnissen bei?

(Recherche & Extraaufgabe)