

## Teil 1: Die Grundlagen schaffen – Die OU-Struktur

**Ziel:** Eine saubere und logische Struktur für das Unternehmen aufbauen. OUs (Organisationseinheiten) sind die Container, in denen wir später Benutzer und Gruppen organisieren und mit Richtlinien (GPOs) steuern.

### Aufgaben:

#### 1. Erstellen Sie eine Haupt-OU für das Unternehmen:

- Rechtsklick auf Ihre Domäne (z.B. firma.local).
- Wählen Sie Neu -> Organisationseinheit.
- Nennen Sie sie Firma\_GmbH.
- **Wichtig:** Stellen Sie sicher, dass der Haken bei "Container vor versehentlichem Löschen schützen" gesetzt ist.

#### 2. Erstellen Sie eine funktionale Unterstruktur innerhalb von Firma\_GmbH:

- Rechtsklick auf Firma\_GmbH -> Neu -> Organisationseinheit: Nennen Sie sie \_Benutzerkonten.
- Rechtsklick auf Firma\_GmbH -> Neu -> Organisationseinheit: Nennen Sie sie \_Gruppen.
- Rechtsklick auf Firma\_GmbH -> Neu -> Organisationseinheit: Nennen Sie sie \_Computer.
- Rechtsklick auf \_Benutzerkonten -> Neu -> Organisationseinheit: Nennen Sie sie Vertrieb.
- Rechtsklick auf \_Benutzerkonten -> Neu -> Organisationseinheit: Nennen Sie sie Buchhaltung.
- Rechtsklick auf \_Benutzerkonten -> Neu -> Organisationseinheit: Nennen Sie sie \_Deaktivierte\_Benutzer.

*Warum der Unterstrich?* Das sortiert diese wichtigen OUs im Alphabet immer nach oben.

## Teil 2: Benutzerkonten anlegen und verwalten (Der Lebenszyklus eines Mitarbeiters)

**Ziel:** Lernen, wie man neue Mitarbeiter anlegt, verwaltet und sauber aus dem System entfernt.

### Aufgaben:

#### 1. Einen neuen Mitarbeiter im Vertrieb anlegen:

- Navigieren Sie zur OU Vertrieb.
- Rechtsklick in den leeren Bereich -> Neu -> Benutzer.
- **Seite 1:**
  - Vorname: Max
  - Nachname: Muster
  - Benutzeranmeldename: m.muster (eine gängige Namenskonvention)

- **Seite 2 (Kennwort):**
  - Geben Sie ein sicheres Startkennwort ein (z.B. Sommer2024!).
  - Setzen Sie den Haken bei "**Benutzer muss Kennwort bei der nächsten Anmeldung ändern**". (Das ist Standard und sehr wichtig!)
  - Klicken Sie auf Fertig stellen.

## 2. Eine Mitarbeiterin geht in Elternzeit (Konto deaktivieren):

- Die Mitarbeiterin Maria Berg (legen Sie sie kurz in der Buchhaltung an, falls nicht vorhanden) geht für ein Jahr in Elternzeit. Ihr Konto soll inaktiv sein, aber nicht gelöscht werden.
- Finden Sie Maria Berg in der OU Buchhaltung.
- Rechtsklick auf den Benutzer -> **Konto deaktivieren**.
- Sie sehen nun ein kleines Pfeil-Symbol nach unten am Benutzerkonto.

## 3. Die Mitarbeiterin kommt zurück (Konto aktivieren):

- Maria Berg ist aus der Elternzeit zurück.
- Rechtsklick auf Maria Berg -> **Konto aktivieren**. Das Symbol verschwindet.

## 4. Ein Mitarbeiter verlässt die Firma (Best Practice):

- Max Muster hat gekündigt. Sein Konto soll sofort gesperrt und archiviert werden. **Löschen Sie Konten nie sofort!**
- **Schritt A:** Deaktivieren Sie das Konto von Max Muster (Rechtsklick -> Konto deaktivieren).
- **Schritt B:** Verschieben Sie das deaktivierte Konto in die Archiv-OU. Rechtsklick auf Max Muster -> Verschieben... -> Wählen Sie die OU \_Deaktivierte\_Benutzer.

## Teil 3: Gruppenverwaltung & Berechtigungen (Das Herzstück)

**Ziel:** Das **AGDLP-Prinzip** verstehen und anwenden: **A**ccounts in **G**lobale Gruppen, **G**lobale Gruppen in **D**omain **L**okale Gruppen, **P**ermissions (Berechtigungen) auf die Domain Lokale Gruppe.

### Aufgaben:

#### 1. Gruppen erstellen:

- Navigieren Sie zur OU \_Gruppen.
- **Globale Gruppe für die Abteilung:**
  - Rechtsklick -> Neu -> Gruppe.
  - Gruppenname: G\_Vertrieb\_Benutzer (G für Global)
  - Gruppenbereich: **Global**
  - Gruppentyp: **Sicherheit**
- **Domain Lokale Gruppe für die Berechtigung:**

- Rechtsklick -> Neu -> Gruppe.
- Gruppenname: DL\_Fileshare\_Vertrieb\_Aendern (DL für Domain Local)
- Gruppenbereich: **Domänenlokal**
- Gruppentyp: **Sicherheit**

## 2. Benutzer und Gruppen verbinden (AGDLP anwenden):

- **Schritt A (Account in Globale Gruppe):**
  - Gehen Sie zu dem Benutzer Max Muster (verschieben Sie ihn testweise zurück in Vertrieb).
  - Rechtsklick -> Eigenschaften -> Tab Mitglied von.
  - Klicken Sie auf Hinzufügen... -> Geben Sie G\_Vertrieb\_Benutzer ein -> Namen überprüfen -> OK.
- **Schritt G -> DL (Globale Gruppe in Domänenlokale Gruppe):**
  - Gehen Sie zur Gruppe DL\_Fileshare\_Vertrieb\_Aendern.
  - Rechtsklick -> Eigenschaften -> Tab Mitglieder.
  - Klicken Sie auf Hinzufügen... -> Geben Sie G\_Vertrieb\_Benutzer ein -> Namen überprüfen -> OK.

## 3. Das Ergebnis überprüfen (Schritt P - Permission):

- Stellen Sie sich vor, Sie haben einen Ordner \\server\Vertriebsdaten. Sie würden jetzt die Berechtigung "Ändern" auf diesen Ordner **nur für die Gruppe DL\_Fileshare\_Vertrieb\_Aendern** vergeben.
- **Vorteil:** Wenn ein neuer Vertriebsmitarbeiter kommt, müssen Sie ihn nur noch in die Gruppe G\_Vertrieb\_Benutzer hinzufügen. Er erhält automatisch die richtigen Berechtigungen. Sie fassen die Berechtigungen am Ordner nie wieder an.

## Teil 4: Effizienz & Sicherheit steigern

**Ziel:** Aufgaben schneller erledigen und die Sicherheit durch gezielte Rechtevergabe erhöhen.

### Aufgaben:

#### 1. Eine Benutzervorlage erstellen:

- Erstellen Sie in der OU Vertrieb einen neuen Benutzer.
- Vorname: \_Vorlage | Nachname: Vertrieb |  
Benutzeranmeldename: vorlage.vertrieb
- Füllen Sie in den Eigenschaften unter dem Tab Organisation schon mal die Abteilung aus: Vertrieb.
- Gehen Sie zum Tab Konto und setzen Sie ganz unten den Haken bei **Konto ist deaktiviert**.

- **Anwendung:** Wenn Sie nun einen neuen Vertriebsmitarbeiter anlegen, machen Sie einen **Rechtsklick auf die Vorlage** und wählen **Kopieren....** Alle voreingestellten Felder werden übernommen!

## 2. Rechte delegieren (z.B. Kennwort zurücksetzen):

- Der Abteilungsleiter vom Vertrieb soll die Kennwörter seiner eigenen Mitarbeiter zurücksetzen dürfen, aber sonst nichts.
- Rechtsklick auf die **OU Vertrieb** -> **Steuerung delegieren....**
- **Assistent:**
  - Hinzufügen... -> Wählen Sie den Benutzer des Abteilungsleiters aus.
  - Folgende allgemeinen Aufgaben delegieren: -> Setzen Sie den Haken bei **Benutzerkennwörter zurücksetzen und ... ändern erzwingen**.
  - Klicken Sie sich durch bis zum Ende.
- **Ergebnis:** Der Abteilungsleiter kann nun Passwörter zurücksetzen, aber **nur** für Benutzer innerhalb der OU Vertrieb. Er kann keine Benutzer in der Buchhaltung verändern.