**Riadenie prístupových práv**

* vždy musíme upravovať prístupové práva aby si hoc kto nemohol robiť čo len chce, ale zase musíme im dať také práva aby mohli robiť to čo musia ... 🤯
* keď už máš Active Directory tak normálne nenájdeš userov, preto musíš ísť takto :

1. Server Manager

2. Active Directory Users and Groups

NA PISOMKE !

* implicitne = defaultne, tak to je v systéme a nikto to nijak inak nenastaví
* explicitne = ja niečo prikážem
* audit = záznam, vo win serveri to môže znamenať -> niekto pride na server, skúsi urobiť niečo na čo nemá práva, systém mu povie že oof, toto nemožeš... a urobí audit/záznam že sa niekto pokúsil urobiť niečo sus

**Typy používateľských skupín**

* Distribučné skupiny (Distribution) = slúžia pre emailové aplikácie a nedajú sa používať na prideľovanie práv a povolení. Poslaním emailu na distribučnú skupinu sa email prepošle všetkým členom skupiny.
* Bezpečnostné skupiny (Security) = slúžia pre prideľovanie práv a povolení a riadenie bezpečnosti pre zdieľané zdroje. Môžu sa použiť aj pre preposlanie e-mailov.

Stratégie prideľovania práv :

**Stratégia A G DL P -> toto musíš vedieť, druhú stratégiu ani nn**

* skôr na menšie firmy

A = Accounts

G = Global group

DL = Domain Local group

P = Permissions

Priklad :

Máme firmu kde sú účtovníci a skladníci

DL = Faktúry ReadOnly

DL = Faktúry ReadWrite

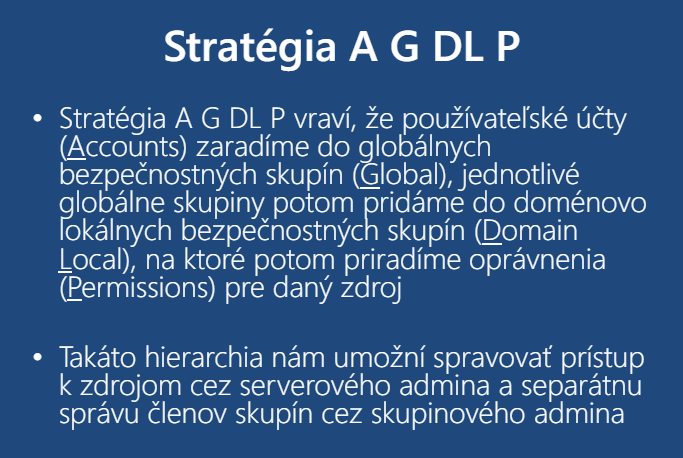
Učtovnici, G-Učtovnici

Sklad, G-Skladnici

Dôvod :

Práva skupín sme robili na to, že keby napr. nejaky skladnik ide do dôchodku a príde nový, tak starému nemusíme manualne odstraňovať práva a novému pridávať, stačí keď ich iba odstránime a pridáme do skupiny

Urobili sme 2 skupiny z dôvodu bezpečnosti, účtovníci do faktúr potrebujú aj zapisovať, no skladníkom sa stačí pozrieť čo vlastne prišlo, keby môžu zapisovať tak by mohli urobiť ZLOBU 😈



**Stratégia A G U DL P**

* skôr na veľké firmy s veľa doménami

