Hálózati operációs rendszerek

1. A hálózati operációs rendszerek tulajdonságai

A hálózatok felügyeletéhez, működtetéséhez szükség van megfelelő operációs rendszerre. Legtöbb esetben külön beszélhetünk a szerver operációs rendszeréről és külön a munkaállomások operációs rendszeréről.

A hálózati operációs rendszereknek különböző szolgáltatásaik vannak, mint a memória- és egyéb erőforrások megosztása a felhasználók között, folyamatok menedzselése, kommunikáció megvalósítása, fájlkezelés. Az operációs rendszerek hierarchikus felépítése lehetővé teszi a különböző funkcióknak a megfelelő szintekhez való rendelését. Az alacsonyabb szintek szoftverjei az egyfelhasználós funkciókat, míg a magasabb szintek szoftverei a hálózati működtetéssel kapcsolatos feladatokat látják el.

2. A hálózati operációs rendszerek biztonsági rendszerei

A korszerű hálózati operációs rendszerek mindegyike legalább négyszintű biztonsági rendszerrel rendelkezik. Ezek:

- bejelentkezési védelem
- jogosultságok védelmi rendszere
- attribútumok védelmi rendszere
- szerver (kiszolgáló) védelem

Bejelentkezési védelem (Login Security)

A hálózatba csak olyan felhasználó jelentkezhet be, aki a rendszer számára "ismert". Bejelentkezéskor minden felhasználónak névvel és jelszóval kell azonosítania magát a rendszer felé. A hálózati jelszót minden esetben vakon kell begépelni, hogy a képernyőről ne tudja senki se leolvasni. A hálózat tervezésekor a felhasználókat több kategóriába sorolják, ezek közül az alábbiak szinte minden rendszerben megjelennek.

- **Egyszerű felhasználók**(user-ek): Semmilyen rendszer-karbantartási műveletet nem végezhetnek el, csak használhatják a hálózati erőforrásokat.
- **Kiemelt felhasználók**: Általában valamilyen rendszeradminisztrációs tevékenységgel megbízott felhasználók.
- **Rendszergazda**: Az egész rendszerre kiterjedő felügyeleti joggal rendelkezik, az ő feladata a hálózat biztonságos és zökkenőmentes működtetése.

Installáláskor “automatikusan” keletkezik két felhasználó: a rendszergazda (Administrator, Supervisor) és a **vendég** (Guest). A vendég egy korlátozott jogokkal rendelkező egyszerű felhasználó aki általában jelszó nélkül használhatja a rendszert. A rendszergazda szintű használat minden esetben jelszóval védett.

Az azonos feladatokat végző felhasználókat célszerű csoportokba (group-okba) szervezi. Ezzel leegyszerűsíthető a rendszeradminisztrációs tevékenység. A hálózat biztonságosabbá tétele érdekében a felhasználói nevekhez tartozó jelszavakra számos előírás adható meg. Ilyenek például:

- Előírható a jelszó minimális hossza. (Ajánlott érték: minimum 6-8 karakter)
- Előírható, hogy a jelszó feltétlenül tartalmazzon betűket és számokat is.
- Megadható, hogy a felhasználónak milyen időközönként kelljen megváltoztatni a jelszavát.

A bejelentkezési védelmet tovább szigoríthatjuk azzal, hogy előírjuk, hogy az adott felhasználó milyen időpontokban és melyik munkaállomásokról léphet csak be a hálózatba.

Jogosultságok védelmi rendszere (Rights Security)

A jogosultsági rendszer ellenőrzi, hogy az adott felhasználó mely könyvtárakkal, alkönyvtárakkal, fájlokkal milyen műveleteket végezhet el. A jogosultsági rendszer konkrét megvalósítása a különböző hálózati operációs rendszerek esetében eltérő lehet, de mindegyik tartalmazza az alábbi alapvető jogosultságokat:

- **Olvasás:** A felhasználó megtekintheti az adott fájl tartalmát.
- **Írás:** A felhasználó módosíthatja az adott fájl tartalmát.
- **Végrehajtás:** A felhasználó futtathatja az adott fájlt.
- **Törlés:** A felhasználó törölheti az adott fájlt.
- **Engedélyek módosítása:** A felhasználó módosíthatja a fájl jogosultsági információit.

Ezek a jogosultsági információk egyaránt beállíthatók fájlokra és könyvtárakra is. A könyvtárakra beállított jogosultságokat az adott könyvtárban lévő alkönyvtárak és fájlok is öröklik.

Attribútumok védelmi rendszere (Attribute Security)

A könyvtárakhoz vagy fájlokhoz attribútumokat adhatunk meg, amelyek “erősebbek” az előbb tárgyalt jogosultságoknál. Egy adott fájl, vagy könyvtár

attribútumait azok a felhasználók változtathatják meg, akik a fájlra, vagy könyvtárra módosítási joggal rendelkeznek.

Szerver védelem

A szerverek minden hálózati operációs rendszer esetén kitüntetett szereppel bírnak, ezért a szerverhez való hozzáférést külön is lehet korlátozni. A szerver konzolja minden esetben jelszóval védhető, megadható, hogy mely felhasználók jogosultak bejelentkezni a szerveren, kik férhetnek hozzá az eseménynaplóhoz, kik kezdeményezhetik a rendszer leállítását stb.

3. A leggyakoribb hálózati operációs rendszerek:

- Novell NetWare
- Windows NT és továbbfejlesztései
- UNIX és Linux rendszerek