

8.b Ismertesse egy általános célú, több belső és külső szolgáltatást nyújtó Windows hálózati kiszolgáló biztonsági konfigurációs (hardening) lehetőségeit intézményi környezetben!

### Fizikai védelem

- **Szerverterem**
  - o Zárt helyiség, ellenőrzött bejutás
  - o Folyamatos áramellátás biztosítása
    - PDU, UPS
  - o Megfelelő hőmérséklet biztosítása, monitorozása
- **Erős BIOS jelszó beállítása**

### Hálózati védelem

- Tűzfal megfelelő beállítása
- Távoli eléréshez VPN kiépítése
  - o Tanúsítványok megkövetelése

### Vírusvédelem

- Vírusirtó szoftver telepítése
  - o Szoftver adatbázisnak frissítése

### Active Directory Védelem

- Telepítésnél a helyreállítási jelszó tárolva legyen
- Csak arra a jogosult személy léphet be a kiszolgálókra
  - o Erős jelszó megkövetelése, havonta csere
    - Group Policy-val jelszoházirend megkövetelése
  - o Tanúsítványok érvényessége
- A user szerepkörök szabályozása
  - o Belső tevékenység szabályozása, ki-mihez férhet hozzá
  - o Állomány hozzáférés szabályozás
    - Organization Unit
    - Group
    - Group Policy

### Frissítések kezelése

- Sérülékenység kihasználásával fontos adatokhoz lehet jutni.
- Rosszindulatú kód bejuttatása.
- Belső/külső feltörések
- **Megoldás:**
  - o Javítások ellenőrzött és gyors telepítése véd a felsoroltak ellen.
  - o Központosított frissítéskezelés.
  - o Frissítéskezelés automatizálása.

## WSUS (Windows Server Update Services) működése

- **Szerver**
  1. WSUS időzített letöltés
  2. Teszt?
    - a. A frissítések tesztelése, ha igen.
    - b. A csomagok engedélyezése, ha nem.
- **Kliens**
  1. WSUS frissítés figyelése.
  2. Admin van belépve?
    - a. Figyelmben kívül hagyhatja a telepítést, ha igen.
    - b. Időzített letöltés és telepítése.
      - i. Szükséges a restart?
        1. Restart, ha igen.
        2. Következő ellenőrzésre várakozás, ha nem.

## Biztonsági javítások – Patch Management

- **Típusai**
  - o **Service Pack**
    - Ritkábban kiadott, de nagyobb méretű javítás, ami új elemeket is tartalmazhat.
  - o **Security Rollup Package**
    - Csak biztonsági javító csomag.
  - o **Hotfix/Patch**
    - Kisebb hibákat megjavít.

## Biztonsági mentés fontossága

- A mentés célja a helyreállíthatóság biztosítása, adatvesztések elkerülése, minimalizálása másolati adathordozók készítésével.

### Mentés célja

- Üzletfolytonosság biztosítása
- **Adatvesztés**
  - o A felhasználó véletlenül vagy szándékosan
  - o Számítógépes vírus
  - o Áramkimaradás
  - o Lemezproblémák, hibás formázás

### Leggyakrabban előforduló hibák, és azok okozói

- **Mechanikai (60%)**
  - o Por, karcolás
  - o A környezet magas hőmérséklete
  - o Túlfeszültség
  - o Fizikai ütés
- **Logikai**
  - o Véletlen törlések
- **Elektronikai**

### Megoldás

- Mentés, archiválás
- **Fontos**, hogy helyreállítási próbálkozások helyett professzionális adatmentő céghez fordulni.

## Hova mentsünk?

- Belső vagy külső merevlemezre
- DVD/CD, de ez manapság már nem annyira népszerű.
- SD/MMC/MS kártyára
- Hálózati mentés, egy központi szerverre

## Hogyan döntsünk?

- Biztonság
- Tartósság
- Megbízhatóság
- Újraírható legyen vagy ne
- Kapacitás
- Átlagos hozzáférési idő
- Átviteli teljesítmény
- Mobilitás
- Ár

## Gyakori adatmentési hibák

- Csak egy vagy két folyton felülírt mentés van.
- A mentés visszatölthetőségét nem ellenőrzik.
- Nem minden fontos adat kerül be a mentésbe.
- Nincs kijelölve a mentésért felelős személy.
- A dolgozók nem tudják, hogy hova mentsenek.

## Központi loggyűjtés a tevékenységekről

- Sikertelen bejelentkezések
- Operációs rendszer hibák

## Monitoring rendszer kialakítása

- CPU, RAM, DISK terheltség
- Service-k állapota
- Riasztási küszöb beállítása