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

# Fizikai védelem

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

# Hálózati védelem

* Tűzfal megfelelő beállítása
* Távoli eléréshez VPN kiépítése
  + Tanúsítványok megkövetelése

# Vírusvédelem

* Vírusírtó szoftver telepítése
  + Szoftver adatbázisnak frissítése

# Active Directory Védelem

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

# Frissítések kezelése

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

## WSUS (Windows Server Update Services) működése

* **Szerver**

1. WSUS időzített letöltés
2. Teszt?
   1. A frissítések tesztelése, ha igen.
   2. A csomagok engedélyezése, ha nem.

* **Kliens**

1. WSUS frissítés figyelése.
2. Admin van belépve?
   1. Figyelmben kívül hagyhatja a telepítést, ha igen.
   2. Időzített letöltés és telepítése.
      1. Szükséges a restart?
         1. Restart, ha igen.
         2. Következő ellenőrzésre várakozás, ha nem.

## Biztonsági javítások – Patch Management

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

# Biztonsági mentés fontossága

* A mentés célja a helyreállíthatóság biztosítása, adatvesztések elkerülése, minimalizálása másolati adatpéldányok készítésével.

## Mentés célja

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

## Leggyakrabban előfordulú hibák, és azok okozói

* **Mechanikai (60%)**
  + Por, karcolás
  + A környezet magas hőmérséklete
  + Túlfeszültség
  + Fizikai ütés
* **Logikai**
  + 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