Windows hardening

- **Hálózati védelem**
  - Tűzfal megfelelő beállítása
  - Távoli eléréshez VPN kiépítése → Tanúsítványok megkövetelése
- **Vírusvédelem**
  - Vírusirtó szoftver telepítése → Szoftver adatbázisának frissítése
- **Active Directory Védelem**
  - Telepítésnél a helyreállítási jelszó tárolva legyen
  - Csak arra jogosult személy léphet be a kiszolgálóra
    - Erős jelszó megkövetelése, havonta csere → Group policy-val
  - Tanúsítványok érvényessége
  - User szerepkörök szabályozása
    - Belső tevékenység szabályozása → ki, mihez férhet hozzá
    - Állomány hozzáférés szabályozás
      - Organization Unit
      - Group / Group Policy
- **Frissítések kezelése**
  - Sérülékenységek kihasználásával fontos adatokhoz lehet jutni.
  - Rosszindulatú kód bejuttatása.
  - Belső/külső felülről
  - Megoldás
    - Javítások ellenőrzött és gyors telepítése véd a felsorolt ellen.
    - Központosított frissítéskezelés
    - 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. Figyelmen kívül hagyhatja a telepítést, ha igen.
       b. Időzített letöltés és telepítés, ha nem.
          i. Szükséges a restart?
             1. Restart, ha igen.
             2. Következő ellenőrzése 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 mentések fontossága**
  - A mentés célja a helyreállíthatóság biztosítása, adatvesztések elkerülése, minimalizálása másolati példányok segítségével. -> Üzletfolytonosság biztosítása
  - Adatvesztés
    - Logikai -> Véletlenül vagy szándékosan
    - Mechanikai -> Por, karcolás, túlfeszültség
    - Elektronikai

- **Professzionális adatmentés**
  - 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 kártya
  - Hálózati mentés egy központi szerverre
- **Hogyan döntsünk**
  - Biztonsági Tartósság; Megbizhatóság; Kapacitás; Teljesítménybeli Ár
- **Gyakori adatmentési hibák**
  - Korábbi mentések felülírása
  - Nincs elég kapacitás
  - Dolgozók nem tudják hova kell menteni
- **Központi loggyűjtés tevékenységekről**
  - Sikertelen bejelentkezések
  - OS hibák
- **Monitoring rendszer kialakítása**
  - CPU, RAM, Disk terheltség
  - Service-k állapota
  - Riasztási küszöb beállítása