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 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**
    - **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.

Mentések

Biztonsági mentés fontossága

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

Mentés célja

- Üzletfolytonosság biztosítása
- **Törlés**
    - A felhasználó véletlenül vagy szándékosan
- **Meghibásodás**
    - Egy tároló eszköz vagy elromlott a rendszer

Mentési stratégia kialakítását befolyásoló tényezők

- **Adattípusok**
    - Adatok jellege
    - Mennyire kritikus adat
    - Meddig kell tárolni
- **Adatmennyiség**
    - Mentési időt befolyásolja
- **Adatok helye**
    - Honnan/hova szeretnénk menteni
- **Mentési gyakoriság**
    - Adatok fontossága, mennyisége
- **Mentési típusok**
    - Teljes
    - Differenciális
    - Inkrementális

Differenciális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző teljes mentés óta történt változások
    - Nagyobb, egyre növekvő napi adatmennyiség
- Gyorsabb és hatékonyabb, mint a teljes mentés
- Maximum 2 helyreállítási folyamatot igényel az adat visszaállítása

Inkrementális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző óta történt változások
    - Kis adatmennyiség, emiatt gyors és kisebb követelményei vannak, mint a differenciális mentésnél.
- Hosszú visszaállítási idő
    - Az adatok visszaállítása, több egymást követő mentásekből álló folyamatot igényel.

Központi loggyűjtés a tevékenységekről

- Kategorizáció

Monitoring rendszer kialakítása

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