11.b Mutasson rá a szerverek és munkaállomások operációs rendszereinek sérülékenységeire! Mutasson példát az Operációs rendszerek szabályozásoknak való megfelelésének vizsgálati lehetőségeire (pl. MS MBSA). Ismertesse a szoftverjavítások, szoftverfrissítések fontosabb típusait, valamint vázolja a szoftverfrissítéseket támogató infrastruktúra kialakítási lehetőségét!

Security Management eszközök

- **Elemzés**
  - Microsoft Baseline Security Analyzer
  - Systems Management Server
  - Microsoft Software Update Services
  - Security Configuration and Analysis snap-in
  - RSoP
- **Management**
  - Group Policy Management Console
  - Microsoft Operations Manager
  - Systems Management Server
  - Microsoft Software Update Services
  - ISA Server

Frissítés szükségessége

- 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 üzemeltetés

- Windows Server Update Services
- Kiszolgáló előfeltételek megteremtése
- Adatbázis kezelő telepítése
- WSUS kiszolgáló telepítése és konfigurálása
- Tűzfal konfigurálása
- Kliens telepítés megtervezése, beállítása
- Csoportos házirend, Gépek csoportosítása, teszt kijelölése
- Üzemeltetés

WSUS követelmények

- **Szerver**
  - x64 alapú, legalább 2GHz
  - RAM 2 GB felett, Tárhely 10GB felett
  - Internet sebessége legalább 100Mbps
- **Kliens**
  - Minimum Windows 2000 Server

WSUS konfigurálása

1. Be kell állítani, hogy a kiszolgáló honnan töltse le a frissítéseket. **Upstream Server,** ahol két opció közül lehet választani:
   - **Microsoft Update-ből való szinkrinozálás:**
     - A Microsoft Update-ről tölti le a frissítéseket.
   - **Szinkronizálás egy másik WSUS kiszolgálóról:**
     - Ha már van egy meglévő WSUS kiszolgáló, akkor innen tölti le a frissítéseket.
     - Meg kell adni a kiszolgáló nevét és portját.
2. **Proxy szerver megadása**
   a. Kiszolgáló, port megadása és opcionálisan a szükséges hitelesítő adatok megadása.
3. **Nyelv és Productok kiválasztása, amit frissíteni szeretnénk.**
4. **Update Classifications**
   a. Frissítési „besorolásokat” lehet kiválasztani:
      i. Kritikus
      ii. Biztonsági
      iii. Rollup
      iv. Driverek
      v. Toolok
      vi. stb
5. **Szinkronizálási ütemterv megadása**
   a. Manuálisan vagy automatikusan egy adott időpontban és hogy napi hányszor.

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.

Microsoft Baseline Security Analyzer

- Sérülékenysége vizsgálat
- Helyi és távoli kiszolgálók biztonsági hiányosságait igyekszik felderíteni.
- Kiszolgáló fájljait hasonlítja össze egy internetről letöltött XML állománnyal.
- Megmutatja, hogy milyen javítások hiányoznak.
- Ellenőrzi a beállításokat, és ha azokat nem találja biztonságosnak, akkor jelzi az elkészült jelentésben.
- Egy tapasztalt szakértőt szimulál, aki ellenőrzi a gépen futó szoftverek és beállítások mennyire biztonságosak.

Sérülékenység vizsgálat életciklusa

- Feltárás
- Eszközök prioritásának meghatározása
- Felmérés
- Jelentés
- Javítás
- Ellenőrzés

Sérülékenysége vizsgálat módjai

- **Black box:** A vizsgálat az infrastruktúra előzetes ismerete nélkül történik.
- **Gray box:** A vizsgálat feltételezi a vizsgált infrastruktúra részleges ismeretét.
- **White box:** A vizsgálat előtt a tesztelők megismerik a teljes infrastruktúrát, a hálózati diagramokat, forráskódot, az IP cím információkat.