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.

**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.

**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**
   1. Kiszolgáló, port megadása és opcionálisan a szükséges hitelesítő adatok megadása.
3. **Nyelv és Productok kiválasztása, amit frissíteni szeretnénk.**
4. **Update Classifications**
   1. Frissítési „besorolásokat” lehet kiválasztani:
      1. Kritikus
      2. Biztonsági
      3. Rollup
      4. Driverek
      5. Toolok
      6. stb
5. **Szinkronizálási ütemterv megadása**

Manuálisan vagy automatikusan egy adott időpontban és hogy napi hányszor.

**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.