7. A távoli munkavégzés biztonsági problémái. Windows Server 2012 komponensek.

**Növekvő igény**

* **Egyre nagyobb igény a távoli elérésre:**
  + Távmunkások, mobil felhasználók (otthonról, hotelekből stb.)
  + Vezeték nélkül (hotspot-ok, repterek stb.)
  + Dolgozók, partnerek, beszállítók, vevők stb.
  + Szoftvertelepítés
* **Szükséges minimum:**
  + A belső webes alkalmazások külső elérése
    - Webszerverek, SharePoint, Exchange komponensek
* **Gyakran szükséges:**
  + Emeltszintű munkavégzés
  + A dolgozók továbbképzése, felkészítése a távoli munkavégzésre
    - a desktop elérése (RDP, RDP over SSL)
    - HTTPS
    - VPN
    - SSH
* **Problémák:**
  + A távoli elérés sosem biztonságos
    - Biztonságos-e a távoli gép?
    - Más is használhatja a távoli gépet.
    - Nincs felügyelet és központi kezelés.
    - Nincs GP, WSUS, központi AV, szoftvertelepítés stb.

**Levelezés, csoportmunka**

* **VPN** – csak levelezésre nem szükséges és veszélyes (bekábelezzük a vírusos otthoni gépet a vállalathoz).
* Exchange **Outlook Webaccess** – be lehet állítani, hogy titkosítatlanul ne menjen soha a jelszó, de nem lehet offline módban használni.
* **Outlook Mobile Access** – könnyen lehet titkosítani, de nem lehet offline módban használni.
* **Outlook** – RPC over http, SSL alagútba tereli a forgalmat a tűzfaltól kifele ill. a tűzfalig. Jelenleg csak az Outlookot lehet ezen keresztül használni, de tervben van a fájl elérés is.
* **Pop3, IMAP** – nem túl nehéz letiltani a titkosítatlan változatot, ami nem csak a jelszavakat védi, hanem a levél tartalmát SSL csatornába tereli.

**Fájl megosztások elérése**

* Nincs egyszerű és biztonságos módszer.
* SSL-en keresztül a SharePoint segítségével.
* Ha nincs lehetőség SharePoint-ra, akkor VPN alagutat kell használni, de célirányosan korlátozva – karantén alagút.
* A karantén lokális hálózati párja a Network Access Protection (ez is beteg vagy –gyógyulj meg technológia alapján működik).
* Monitorozhatjuk hogy, ki mekkora mennyiségű adatot tölt le-fel

**Hozzáférések korlátozása:**

* Szabályozzuk, hogy a cég tulajdonában álló eszközöket ne használhassa a munkavállalón kívül más felhasználó
* Megadhatunk időkorlátokat arra, hogy kinek meddig lehet hozzáférése az erőforrásokhoz

**TÁVOLI ELÉRÉS - SSH (Secure Shell, biztonságos héj)**

* Segédprogram, protokoll, titkosító eszköz ügyfél-kiszolgáló alkalmazás és parancsfelület is egyben.
* **Cél**: két számítógép között egy potenciálisan nem biztonságos hálózaton (pl. Interneten) keresztül egy titkosított kommunikációs út kiépítése.
* Alkalmazási platformjai:
  + - Macintosh, Microsoft Windows, UNIX, Linux, Cisco útválasztó mobil eszközök, stb.
  + alapján képes engedélyezni vagy letiltani a csomópontokat (IP és DNS szűrés).

**Az SSH lehetővé teszi bizonyos, a végpont (port) számával azonosított forgalom SSH alagúton történő átirányítását.**