# 14.b Elemezze a távoli munkavégzést a biztonság szemszögéből! Relevancia. Problémák az elérendő célok szerint. Kivitelezési lehetőségek.

## Igény

- Manapság egyre nagyobb az igény a távoli munkavégzésre, amit manapság „Home Office”-nak is nevezünk.
    - Tehát távmunka vezeték nélkül azon a gépen, ami a céges környezeten belül helyezkedik, ahol a hálózathoz is hozzá lehet férni.
- Általában ehhez szükséges:
    - RDP
    - HTTPS
    - VPN
    - SSH

### Problémák

- **Távoli elérés sosem biztonságos, mert:**
    - Más is használhatja a távoli gépet.
    - Nincs felügyelet, nincs központi figyelés.
    - Nincs Group Policy, központi antivirus szoftver
- Adatlopás
- Identitáslopás

## Példák

### „Scam”, vagyis csaló email-ek

- Viszonylag ez a legtöbbet használt „támadási” fajta, amivel elhitetjük a potenciális áldozattal, hogy például nyert x összeget a lottón és azt átutalják, ha megadja a bankszámla adatait az illető.
- A támadók általában valamilyen programot, bot-ot használnak, hogy automatizálják a „támadást”.
- Ezt úgy tudjuk elkerülni, hogy vagy szűrőt használunk, ami alapján blokkoljuk a csaló email-eket vagy megbizonyosodunk a küldőről, hogy tényleg az, akinek ő hiteti magát.

### Gyenge jelszavak

- Single Sign On, vagyis mindenhol ugyanaz a jelszó van használatban.
- Kódolatlan HTTP weboldalak.
- Plain-text-ben való jelszó megosztás.
- **Megoldás:**
    - Ne használjuk a vállalati jelszavunkat, ha a weboldal kódolatlan HTTP oldal.
    - Ne használjuk ugyanazt a jelszót, használjunk jelszó generátort komplexebb mintákkal.

### Gyenge biztonsági ellenőrzések

- A vállalaton belül tűzfal szabályokat kell bevezetnie.
    - Csak a tényleges szolgáltatásokat engedjük át, amit nem használunk vagy nem is tudunk róla, hogy mi célt szolgál, azt kapcsoljuk le.
- Fontos a monitorozás is, de előfordulhat olyan is, hogy például a vállalat ad egy laptopot a dolgozónak, így technikailag nem a vállalat környezetén belül dolgozik, hanem fizikailag azon a laptopon.
    - Ezzel az a probléma, hogy így már nem tudja a vállalat feltétlenül monitorozni például a hálózati forgalmat.

### Hálózati támadások

- Tegyük fel, hogy miután az áldozat rákattintott egy linkre, amit az áldozat küldött email-ben, az adatokat gyűjtött az áldozatról.
    - Megszerzett olyan adatokat, mint az IP, lokáció, név.
    - Ez alapján végrehajthat egy port szkenneléses támadást.
    - Majd rájön, hogy az RDP port nyitva van, így brute force, vagyis nyers erő módszerével megpróbálja feltörni az áldozat gépét.
- Meg is tudja bénítani az áldozatot DDoS támadással vagy elérheti, hogy a teljes vállalat hálózata ne legyen elérhető.

### Nyilvános helyen történő munkavégzés

- Például egy dolgozó egy kávézóban dolgozik épp a laptopján és rácsatlakozik a nyilvános, ingyenes Wi-Fi-re, akkor azt könnyedén le lehet hallgatni.
- Előfordulhat az is, hogy érzékeny adatok vannak a kijelzőn és azt valaki meglátja és hasznot húz belőle vagy ott hagyja a laptopot felügyelet nélkül.

### Titkosítatlan fájlmegosztás

- Mai napig sokan használják az FTP szolgáltatást fájlmegosztásra, ami nem túl biztonságos.
    - Plain-text felhasználónév és jelszó és az adatátvitel nincs titkosítva.
    - Emiatt használhatóak a packet sniffing, spoofing és brute force támadások.
- Sokkal biztonságosabb az SFTP, ami Secure Shell kriptográfián alapszik adatátvitelkor.
    - Mivel az információt csomagokban továbbítják, nem pedig plain-text-ben, ami gyorsabb átviteli időt eredményez az FTP-hez képest.

### Rossz konfigurációk környezeten belül

- Jogosultság kezelést be kell vezetni a környezeten belül, viszont előfordulhat, hogy a vállalat nem fordít rá elég figyelmet, hogy kinek mihez is van joga.
    - Például egy asszisztens ne férhessen hozzá a fejlesztők fájljaihoz.

### Webkamerás támadás

- A támadó ezzel személyiségi jogok megsértését hajtja végre.
- Előfordulhat, hogy például egy dokumentum olyan látószögben van, ami alapján láthatóak a privát vállalati adatok, ami a támadó számára értékes lehet.

## Megoldások

- Többlépcsős autentikáció használata.
- Jelszó kezelő szoftverek használata.
- Vállalaton belüli VPN
- Tűzfal alkalmazása szigorú szabályokkal
- Jogosultságkezelés
- Végponti biztonság fokozása