# **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

* Kódolatlan HTTP weboldalak.
* Plain-text-ben való jelszó megosztás.
  + 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.

## 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.

## VPN – Virtual Private Network

* **Virtuális:**
  + A magánhálózat forgalma nyilvános hálózaton halad keresztül egy virtuális alagúton.
* **Védett:**
  + Átmenő forgalom titkossága biztosított.

## VPN Rendeltetése

* Biztonság növelése
* Anonimitás
* Nem elérhető tartalomhoz jutás (adott országon belül például tiltva van)
* Adatvédelem

## VPN Alaptípusai

* IPSec – Internet Protocol Security
* L2TP - Layer 2 Tunneling Protocol
* PPTP – Point-to-Point Tunneling Protocol
* SSL és TLS
* OpenVPN
* SSH – Secure Shell

# VPN megvalósítások a különböző OSI rétegekben

A képen szöveg, képernyőkép, diagram, sor látható

Automatikusan generált leírás

## L2 VPN

* Független a felső protokolltól
* Adatkapcsolati rétegben helyezkedik el
* Egy-egy kapcsolatot véd, így minden összeköttetésre külön alkalmazni kell.
* MITM támadás lehetséges

## L3 VPN

* Hálózati rétegben helyezkedik el
* Média és alkalmazás független
* IPSec, GRE, MPLS

## L4 VPN

* SSL-lel biztosítja a titkosságot, a felhasználók hitelességét és az adatok sértetlenségét a TCP alkalmazások számára.
* Nem rugalmas, nehéz megvalósítani
* Nem alkalmazás független

## L7 VPN

* Az alkalmazás rétegbeli VPN-t minden alkalmazásban külön-külön meg kell valósítani.

# Megoldások

* Többlépcsős autentikáció használata (2FA).
* Jelszó kezelő szoftverek használata.
* Vállalaton belüli VPN
* Tűzfal alkalmazása szigorú szabályokkal
* Jogosultságkezelés
* Végponti biztonság fokozása