Távoli munkavégzés biztonsága

- **Igény**
  - Manapság egyre nagyobb az igény a távoli munkavégzésre (Home Office)
    - Tehát távmunka vezetés nélkül azon a gépen, ami a céges környezeten belül helyezkedik el, ahol a hálózathoz is hozzá lehet férni.
    - RDP
    - HTTPS
    - VPN
    - SSH
- **Problémák**
  - Távoli elérés sosem biztonságos, mert:
    - Más is használhatja a távoli gépet.
    - Nincs felügyelet, nincs központi figyelés.
    - Nincs Group Policy, nincs központi antivirus szoftver.
  - Adatlopás
  - Identitáslopás
- **"Scam", vagyis csaló email-ek**
  - Viszonylag ez a legtöbbet használt "támadási" fajta, amivel elhiteljük a potenciális áldozattal, hogy például nyert x összeget a lottón és azt átutaljá, ha megadja a bankszámla adatait.
  - A támadók ezt a folyamatot automatizálják.
    - Ezt úgy tudjuk elkerülni, hogy vagy szűrőt használunk, ami alapján blokkolja a csaló emaileket vagy megbizonyosodunk a küldőről, hogy tényleg az, akinek ő hiteli magát.
- **Gyenge jelszavak**
  - Kódolatlan HTTP weboldalak
  - Jelszó nyílt szöveg-ként (plain-text) van tárolva
  - Használjunk komplex jelszavakat, HTTPS oldalak biztonságosabbak

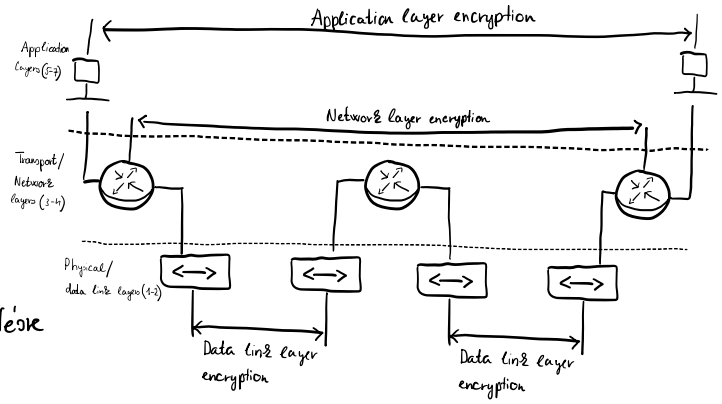
- Gyenge biztonsági ellenőrzések
  - Vállalaton belüli tűzfal szabályok alkalmazása.
    - Csak a tényleges szolgáltatásokat engedjük át, többit zároljuk le.
  - Fontos a monitorozás is, de előfordulhat olyan, hogy a vállalat ad egy laptopot a dolgozóknak, így technikailag nem a vállalat környezetén belül dolgozik, hanem fizikailag azon a laptopon.
    - Ezzel az a probléma, hogy a vállalat nem tudja 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 (MiTM)
  - Előfordulhat az is, hogy érzékeny adatok vannak a kijelzőn és azt valaki meglátja és hasznot húz belőle vagy a laptop tulajdonosa ott hagyja felügyelet nélkül.
- Titkosítatlan fájlmegosztás
  - FTP nem biztonságos
    - Plain-text felhasználónév és jelszó, és az adatátvitel nincs titkosítva.
      - Packet sniffing, spoofing
  - Sokkal biztonságosabb az SFTP, ami Secure Shell kriptográfián alapszik és gyorsabb is az adatátvitel

- **VPN** -> Virtual Private Network
  - Virtuális -> A magán hálózat forgalma nyilvános hálózaton halad keresztül egy virtuális alagúton.
  - Védett -> Átmenő forgalom titkossága biztosított.

- **Rendeltetése**
  - Biztonság növelése, anonimitás
  - Nem elérhető tartalomhoz jutás
  - Adatvédelem

- **Alaptípusai**
  - IPSec – Internet Protocol Security
  - L2TP – Layer 2 Tunneling Protocol
  - PPTP – Point-to-Point Tunneling Protocol
  - SSL / TLS, OpenVPN, SSH

- **VPN megvalósításai a különböző OSI rétegekben**



- L2 VPN
  - Független a felső protokolltól
  - Adatkapcsolati rétegben helyezkedik el
  - Egy-egy kapcsolatot véd, így minden összeköttetésre külön alkalmazni kell.

- L3 VPN
  - Hálózati rétegben helyezkedik el
  - Média és alkalmazás független
  - IPSec, GRE, MPLS

- L4 VPN
  - SSL-el biztosítja a titkosságot, a felhasználók hitelességét és az adatok sértetlenségét a TCP alkalmazások számára.
  - Nem rugalmas, nehéz megvalósítani és nem alkalmazás független

- L7 VPN
  - A alkalmazás rétegbeli VPN-t minden alkalmazásban külön-külön meg kell valósítani.