# **4.b** Ismertesse az informatikai rendszerek főbb elemeit és azok sérülékenységeit, valamint a tipikus védelmi megoldási formákat!

# Informatikai rendszer

* Az adatok kezelésére használt elektronikus eszközök, eljárások és az ezeket kiszolgáló és a felhasználó személyek együttese.
* Egymással szervesen együttműködő és kölcsönhatásban lévő elemek összessége.

## Adatkezelés

* Adatok gyűjtése, felvétele, tárolása, feldolgozása, továbbítása, törlése, hasznostása és a felhasználásuk megakadályozása.

# Informatikai rendszer elemei

* A környezet infrastruktúra elemei
* A rendszerelemekkel kapcsolatba kerülő személyek
* Hardver elemek
* Szoftver elemek
* Adathordozók, adatok, dokumentumok
* A kommunikáció elemei

# Sérülékenységek

## A környezet infrastruktúra

* Nem védett, helytelenül tervezett átviteli vezetékek.
* Cégen kívüli személyek bent tartózkodása.
* Nem felügyelt munkálatok az épületekben vagy azokon kívül (ablak tisztítás, építési munkálatok)
* Informatikai berendezések nem védett helyezete
* Gyenge belépési biztonság

## Hardver elemek

* A készülékek kismértékű súlya, így könnyen lopható
* Ütésérzékeny

## Szoftverek

* Specifikációs hiba, helytene program-előállítás
* Nincs hitelesítés, implementálási hibák
* Bonyolult felhasználói felület
* Hiányos dokumentáció
* Titkosító algoritmus ismerete
* Gyenge jelszavak, változtatás hiánya
* Vírusfertőzés
* Távolról való adminisztráció

## Adathordozók

* Nem védett tárolás
* Kapcsolható írásvédelem
* Érzékenység
* Ellenőrizetlen használat
* Újrafelhasználhatóság elégtelen kezelése

## Dokumentumok

* Hiányos dokumentálás
* Nem védett tárolás
* Ellenőrizetlen sokszorosítási lehetőségek
* Nincs felhasználói dokumentáció

## Adatok

* Adatvesztések, károsodások
* Hibás manuális adatbeadás/változtatás
* Hibás utasítás, rendszermegszakítás
* Adatok jogosulatlan másolása

# Informatikai biztonság

* Az informatikai rendszer, az érintett számára kielégítő mértékű állapota, aminek védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása és a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

## Hogyan védhetjük informatikai rendszereinket?

* OS biztonsági szolgáltatásival, például naplózás, házirend kialakítása, felhasználó kezelés, hozzáférés-vezérlés.
* Titkosítás
* Tűzfalak, IDS/IPS alkalmazása
* Jelszókezelés jelentősége
* Vírusvédelem jelentősége
* Például oktatással, ha mondjuk van egy új gyakornok, akkor annak megtanítjuk, hogy hogyan használja az előírtaknak megfelelően, biztonságosan a rendszert.