3. tétel

Adatvédelem, adatbiztonság

Melyek az informatikában a védett adatok? Hogyan biztosítják az adatok védelmét a vállalati, illetve a magánszférában? Milyen védelmi mechanizmusok vannak egy helyi hálózatnál? Hogyan lehet megvédeni az adatokat a jogosulatlan hozzáféréstől? Milyen archiválási lehetőségek vannak?

A számítógépen tárolt információ, adat különböző okokból rongálódhat vagy semmisülhet meg pl.:

- Katasztrófa esetek (elemi károk, tűz, víz, villámcsapás stb.).
- Emberi hiba (gondatlanság, tájékozatlanság stb.).
- Szándékos rongálás, visszaélés (vírus stb.).
- Hardverhiba (géphiba, feszültség-kimaradás, -ingadozás stb.).
- Szoftverhiba (hibás program, rendszerösszeomlás stb.).

✓ 1 PONT

Az adatvédelem leggyakoribb megoldásai:

- Tűz- és vagyonvédelmi intézkedések.
- Képzés, jogosultságok finomítása.
- Adatok több példányban való tárolása, archiválás.
- Vírusmentesítés, tűzfal erősebbé tétele.
- Rendszeres karbantartás, szünetmentes tápegység használata stb.

- Lemeztükrözés, kettőzés, kiszolgáló-kettőzés.
- Programtesztelés.
- Állományok kódolása, titkosítása.
- Cserélhető merevlemezek páncélszekrényben történő őrzése.

✓ 2 PONT

Az adatok védelmét a **gépterembe való belépés ellenőrzésével** kezdhetjük (pl. egyedi kártya, vagy azonosító).
Tovább növeli a biztonságot ha a számítógépbe csak **felhasználói névvel és jelszóval lehet belépni.** A jelszót időnként célszerű cserélni, és jó ha nehezen megfejthető. A biztonsági jelszavakat ne tároljuk a gép környezetében pl. egy monitorra ragasztott cetlin!
Fokozza a védelmet az **azonosító hardverkulccsal, egyedi pendrive-val, ujjlenyomattal** vagy **retinaszkennerrel** való **beléptetés,** melyhez felhasználói név és jelszó is tartozik.

✓ 1 PONT

A harmadik védelmi vonal az lehet, ha **hálózati nevet és azonosítót** kérünk a hálózatra való belépéshez. A hálózati szoftverek többsége tárolja a felhasználók belépésének helyét, idejét, így ez további biztosítékot ad.

✓ 1 PONT

A negyedik védelmi vonalat a **felhasználók csoportosítása,** illetve a **felhasználói jogok adása** jelenti. Ilyen védelem kiépítésekor pl. egy átlagos felhasználó csak minimális jogokkal rendelkezik az általa használt szoftverekhez, a hálózati csoportadminisztrátorok már ellenőrzik a hozzájuk tartozó felhasználók tevékenységét, és szükség esetén be is tudnak avatkozni, végül a hálózati adminisztrátor (supervisor, admin) minden joggal rendelkezik az egész hálózatban.

✓ 1 PONT

A **megfelelő jogosultságokat** érdemes alaposan átgondolni és rendszeresen frissíteni a felmerült igények alapján. Pl. a céges fizetési jegyzék anyagát a raktáros ne olvassa, ugyanakkor a bérszámfejtő se nézhessen bele a raktárkészletbe.

✓ 1 PONT

A **szoftveres behatolók ellen** egy gyakran frissített, állandóan működő **vírusirtót** és egy jól záró **tűzfal**at kell alkalmazni. Általában **egy gépen csak egy vírusirtó** van, de ez nem zárja ki, hogy a hálózati szerveren egy másik vírusító ellenőrizze az átmenő forgalmat. A tűzfalból is lehet egy a számítógépen, és egy másik a helyi hálózati szerveren.

✓ 1 PONT

A sokoldalú védekezés ellenére a leggyakoribb hibalehetőség a felhasználói, illetve emberi hiba. Gyakori mulasztások:

- Nincs jelszó a gépen. (Magáncélú gépen igen gyakori.)

- Túl egyszerű a jelszó (pl. 1234 stb.).
- Könnyen feltörhető a jelszó (pl. a felhasználó gyerekének/kutyájának a neve stb.).
- A jelszó fel van írva a billentyűzet aljára vagy a monitor sarkára. (Vállalati számítógépeknél gyakori.)
- A felhasználó őrizetlenül hagyta a gépét, nyitott dokumentumokkal. Stb.

✓ 1 PONT

Helyi hálózat esetén a jogok helyes elosztásában segíthet a **hálózati szoftver** eleve adott jogokkal. Ilyen **jogosultságok** lehetnek pl.:

- R = read, olvasási jog.
- W = write, írási jog.
- O = open, megnyitási jog.
- X = executable, futtatási jog.
- C = create, létrehozási jog.

A felsorolt jogokat megadhatjuk akár egyetlen fájlra, akár egész könyvtárakra is, így minden felhasználó csak a saját adataihoz férhet hozzá, illetve a rendszeradminisztrátor hozzáférhet a szükséges adatokhoz.

✓ 1 PONT

Közösen használt számítógépnél célszerű **személyenkénti felhasználói nevet és jelszót létrehozni,** amellyel megteremthető, hogy mindenki csak a saját, személyes adataihoz férhessen hozzá. Magáncélú gépnél érdemes olyan **személyenkénti mappá**kat létrehozni, amelyhez csak az adott felhasználó férhet hozzá. Vállalati környezetben az egyes felhasználók adatait a szerveren is lehet tárolni (egyedi mappában), így a felhasználók bárhonnan láthatják a saját adataikat, melyet mások nem láthatnak. Vállalati környezetben célszerű egy „közös" mappát is létrehozni, amelyben a mindenkit érintő anyagok vannak.

Helyi hálózatoknál javasolt védelmi eljárások:

- bejelentkezési jelszavas védelem,
- hozzáférési védelem (érzékeny adatokhoz),
- jogosultságok átgondolt kiosztása,
- könyvtár és/vagy fájlvédelem,
- fájlok attribútumainak védelme,
- az érzékeny adatok tükrözése,
- a lényeges adatok rendszeres mentése hordozható HDD-re, majd azok páncélszekrényben tartása,
- több, párhozamosan működő kiszolgáló telepítése és használata,
- biztonsági mentés (szerverre, háttértárra, céges felhőbe stb.),

- a hálózati tevékenységek rendszeres adminisztrációja,
- hálózati forgalom figyelése,
- rendszeres szerver- és gépszintű karbantartás.

✓ 1 PONT

Archiválásra több lehetőség adódik:

- rendszeres, napi mentés (pendrive, külső HDD, felhő),
- a szerveren lévő adatok periódusonkénti mentése (pl. hetente) külső HDD-re, vagy streamerre,
- szünetmentes áramforrás alkalmazása (gépenként),
- belső szerver megerősítése (áramkimaradás esetén),
- vállalati megoldásoknál saját céges felhő alkalmazása a rendszeres mentésekre.

✓ 1 PONT

KIEGÉSZÍTŐ KÉRDÉSEK

- A számítógép ellopása ellen milyen védelem alkalmazható?
  - A számítógép újratelepítése ellen a legegyszerűbb módszer az alaplap BIOS jelszavas védelme, mely rongálás nélkül megakadályozhatja az újratelepítést. Egyes laptopokban és egyéb eszközökben van nyomkövetési védelem, így ha máshol jelentkeznek be vele, akkor jelez a tulajdonosának.
- Hogyan lehet védekezni a hibás program ellen?
  - Új programot vagy új verziót, ha van rá lehetőség, érdemes a valós felhasználás előtt tesztüzemben használni, mely során szembesülhetünk a legtöbb hibával. Erre egy virtuális gépen kerülhet sor, így ha ez a gép összeomlik, akkor nem sérül a valós gép, és kiderül, hogy hibás az új program vagy verzió.