**Vírusok, Számítógép-védelem**

A vírusok számítógépes programok, és céljuk a károkozás. A számítógépes vírusok működése hasonlít az élővilágban megfigyelhető vírus viselkedéséhez, mely az élő sejtekbe hatol be, hogy önmaga másolatait előállíthassa. Ha egy számítógépes vírus kerül egy másik programba, akkor ezt fertőződésnek nevezzük. Ez megtévesztő lehet a számítógép-felhasználók számára, mivel mára lecsökkent a szűkebb értelemben vett számítógépes vírusok gyakorisága, az egyéb rosszindulatú szoftverekhez képest, amivel sokszor összetévesztik őket.

Vírust a legegyszerűbben az interneten kaphatunk. Ez lehet bizonyos oldalakról és e-mailről is. Vírust még kaphatunk különböző adathordozókról is. (CD,DVD,Pendrive)

Ha már a gépen van a vírus, akkor lehetnek arra utaló jelek:

* Lelassul a gép
* Ok nélküli hibaüzenetek
* Elfogyó hely
* Sűrű lefagyás

Ezek ellen többféle módon tudunk védekezni:

* Vírusirtót telepítünk a gépre
* Körültekintő számítógép használat (Nem árt, ha sokkal óvatosabban használjuk az internetet)
* Biztonsági mentés készítése
* Tűzfal bekapcsolása

A rosszindulatú szoftvereknek (malware) számos fajtáját különböztetjük meg:

1. **Vírusok**
   1. Programvírusok: Sokszorosítja és terjeszti önmagát. Futtatható állományokat fertőz meg.
   2. Boot vírusok: Azokat a lemezterületeket használja fel önmaga terjesztésére, amiket a számítógép bekapcsoláskor automatikusan lefuttat.
   3. Makróvírusok:  Ezek a vírusok többnyire [szövegszerkesztők](https://hu.wikipedia.org/wiki/Sz%C3%B6vegszerkeszt%C5%91) által létrehozott dokumentumokkal terjednek.
2. **Férgek (Worm)**: Speciális fajta, melynek szaporodásához nincs szükség hordozóprogramra.
3. **Trójai programok**: Látszólag hasznosat vagy érdekeset csinál, de káros, nem kívánt mellékfunkciókat is végrehajt mellette.
4. **Kémprogramok (Spyware)**: Célja, hogy a felhasználó tudomása nélkül megszerezzék a megfertőzött számítógép felhasználójának adatait.
5. **Egyéb vírusok**
   1. Hoax vírus: Lánclevél útján terjed
   2. Spam: Kéretlen levelek, amik vírust tartalmaznak
   3. Phishing (Adathalászat): Egy internetes csaló oldal egy jól ismert cég hivatalos oldalának láttatja magát és megpróbál bizonyos személyes adatokat ellopni.

Hogyan tudunk védekezni ellenük?

**1.Biztonsági másolat**

Biztonsági másolatról beszélünk, ha egy adott állományról (mappáról) egy vele teljesen megegyező másolatot készítünk, melyet célszerűen másik fizikai egységen tárolunk. Adatvesztés esetén csak a másolat időpontjának megfelelő állapota állítható helyre.

**2.Archiválás**

Az adatok hosszú távú tárolásának céljából erre alkalmas külön eszközön történik, rendszerint nem szolgálja megsemmisülés esetén az adatok helyreállítását, inkább egyfajta adminisztratív eszköz.

**3. Biztonsági mentés**

Meghatározott eseményhez vagy időponthoz kötött, a rendszer egészéről, vagy annak egyes részeiről készített, tömörítési és egyéb (pl. titkosítási) eljárásokkal előállított kópia, mely lehetővé teszi az adatok ezen időpontnak megfelelő állapotban való helyreállítását.

Két fajta dologról tudunk biztonsági mentést készíteni a fájlokról, mappákról és rendszerállapot adatiról.

A biztonsági másolat az összes kijelölt fájlt átmásolja, de nem jelöli meg a fájlokat, hogy biztonsági mentés készült róluk (más szóval nem törli az archiválandó attribútumot).

Típusai:

* **Teljes mentés (Full Backup)**

A rendszer minden adata válogatás nélkül mentésre kerül. A mentési folyamat ezért egyszerű, ellenben sok ideig tart. Előnye az, hogy a visszaállítás viszonylag gyors. Teljes mentést célszerűen ritkán kell végrehajtani, a tárolandó hatalmas adatmennyiség miatt.

* **Napi biztonsági mentés (Daily Backup)**A napi mentések csak a biztonsági mentés napján módosult fájlokat archiválják. A napi mentés nem módosítja az archiválási bitet.
* **Különbségi (differenciális) biztonsági mentés (Differencial Backup)**

A különbségi biztonsági mentés a legutolsó normál vagy növekményes biztonsági mentés óta létrehozott vagy módosított fájlokról készít biztonsági másolatot. A normál és különbségi biztonsági mentés kombinációjának használatakor a fájlok és mappák visszaállításához egyaránt szükséges a legutolsó normál és a legutolsó különbségi biztonsági másolat.

* **Növekményes (inkrementális) biztonsági mentés (Incremental Backup)**

A növekményes biztonsági mentés csak a legutolsó normál vagy növekményes biztonsági mentés óta létrehozott vagy módosított fájlokról készít biztonsági mentést. A normál és a növekményes biztonsági mentés kombinációjának a használatakor az adatok helyreállításához egyaránt szükséges a legutolsó normál és az összes növekményes biztonsági mentés.

**Biztonsági mentések készítése lehet:**

* **Fájlokról, mappákról**

A biztonsági másolat az összes kijelölt fájlt átmásolja, de nem jelöli meg a fájlokat, hogy biztonsági mentés készült róluk (más szóval nem törli az archiválandó attribútumot). A másolás akkor hasznos, ha normál és növekményes biztonsági mentés között akar biztonsági mentést készíteni a fájlokról, mivel a másolás nem befolyásolja ezeket a biztonsági mentéseket.

* **Rendszerállapot adatokról**

A rendszerállapot adatok biztonsági mentésekor és visszaállításakor a rendszer a számítógéphez kapcsolódó összes rendszerállapot-adat biztonsági mentését vagy visszaállítását végrehajtja, a rendszerállapot-adatok különálló összetevőinek biztonsági mentése vagy visszaállítása nem hajtható végre.

Adatbiztonsági eszköznek számít még a **rendszervisszaállítási pont** is.

A rendszer-visszaállítási pontok visszaállítják az operációs rendszert egy, az időben előre meghatározott pontra. Néhány esetben, egy alkalmazás vagy egy hardver illesztőprogramjának telepítése instabilitást okozhat vagy váratlan változásokat idéz elő a számítógépen. A program vagy az illesztőprogram eltávolítása normális esetben kijavítja a problémát. Ha az eltávolítás nem oldja meg a problémát, meg kell próbálnunk visszaállítani az operációs rendszert egy korábbi időpontra, amikor a rendszer még megfelelően működött.

**A nulladik napi támadás (zero-day attack)** egy biztonsági fenyegetés, ami valamely számítógépes alkalmazás olyan sebezhetőségét használja ki, ami még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el azt foltozó biztonsági javítás. Zero-day exploitnak nevezik azt a tényleges kódot, amit a támadók használnak a sérülékenység kiaknázására, mielőtt a szoftver fejlesztője tudna arról.

**A nulladik napi védelem (zero-day protection)** a nulladik napi támadások elleni védekezés képessége. Ez azért is fontos lehet, mert a nulladik napi támadások sokáig észrevétlenül maradhatnak.

A nulladik napi támadások elkerülésének egyik módja, hogy csak bizonyos idő elteltével frissítenek a szoftverek új főverziójára (az 1.0 verzió problémájának elkerülése). Az új funkcionalitást tartalmazó termékekben általában új hibák is találhatók; az új főverzió hibáit viszont általában a szoftverfejlesztő gyorsan javítja, alverzió-frissítésekkel (1.1, 1.2 stb.). Bár ez a módszer védelmet ad az olyan nulladik napi támadásokkal szemben, amik a szoftverkiadás ciklusának nulladik napján jelennek meg, nem szabad elfelejteni, hogy a biztonsági réseket bármikor felfedezhetik. Ebben az esetben ez a módszer nem ad plusz védelmet.

**A vírusirtó** vagy antivírus program a számítástechnikában egy szoftveres vagy hardveres architektúra, amelynek célja annak biztosítása, hogy a hálózatba vagy egy adott számítógépbe ne juthasson be olyan állomány, mely károkozást, illetéktelen adatgyűjtést vagy bármely, a felhasználó által nem engedélyezett műveletet hajt végre.

A vírusirtó szoftverek két alapelven működnek:

* Az első az úgynevezett **reaktív védelem**. Ebben az esetben a vírusirtó szoftver egy adatbázisból azonosítja a kártevőket. Az adatbázist a vírusirtó szoftver gyártója rendszeresen frissíti, a frissítéseket a legtöbb vírusirtó szoftver automatikusan letölti az internetről.
* A második védelmi módszer az úgynevezett **heurisztikus védelem**. Ebben az esetben a vírusirtó a beépített analizáló algoritmusok segítségével azonosítja a vírusokat. A módszer azért nagyon fontos, mert sokszor több nap telik el egy új vírus megjelenésétől addig, amíg a vírusirtó program gyártója elkészíti az új vírus elleni védelmet és beépíti a vírusdefiníciós adatbázisba. A reaktív vírusirtó szoftvernek ilyenkor frissítenie kell magát az internetről, és csak ezután nyújt védelmet az új vírusok ellen. A modern vírusirtók viszont addig is védelmet nyújtanak a legtöbb kártevő ellen

Ezek a modern vírusirtók kombinálják a hagyományos (vírusdefiníciós adatbázison alapuló) védelmet a modern heurisztikus védelemmel, és így nagyobb biztonságot adnak a felhasználóknak.