11. tétel

Kártevők, vírusvédelem

Ismertesse a számítógépes vírus fogalmát! Milyen közös jellemzőjük van a számítógépes vírusoknak? Ismertesse és jellemezze a számítógép vírusok főbb osztályait! Milyen károkat okozhatnak a vírusok és hogyan védekezhetünk ellenük?

Gyakorlati feladat: A teremben lévő számítógépen hajtson végre egy gyors víruskeresést a telepített szoftverrel!

A számítógépek háttértárain található programok és adatok biztonságát olyan speciális programok veszélyeztetik, melyeket arra fejlesztettek, hogy tönkretegyék a fájlokat, vagy lekössék a számítógép erőforrásait (háttértár, memória, processzor-idő). Ezeket a kárt okozó kisebb-nagyobb kódrészleteket számítógépes vírusoknak, férgeknek vagy kártevőknek nevezik. ✓ 1 PONT

A számítógépes vírus egy olyan speciális program(részlet), amely képes saját példányát vagy annak egy változatát elhelyezni más programokban, tárhelyeken vagy adatbázisokban. A vírusok egy része csak szaporodik, mely által tárhelyet foglal el, de több olyan vírus is van, amely ennél súlyosabb károk okozására is képes. ✓ 1 PONT

Az **első vírus** az 1970-es évek elején **észlelt** Creeper vírus volt, melynek észlelésére és eltávolítására hozták létre a Reaper programot. Ettől kezdve tart a vírusok és a vírusirtók versenye. A számítógépes hálózatok elterjedése előtt a **kezdeti vírusok** az akkor használt adathordozókon, főleg az egyre olcsóbbá váló floppy lemezeken szaporodtak. Mivel akkoriban a felhasználók többsége nem ismerte a számítógépes vírust, ezért a terjedésüket gyakorlatilag nem akadályozta semmi. Egyes korai vírusok megfertőzték a futtatható fájlokat, az adatállományokat, de gyakori volt a **boot-szektort támadó** vírus is. Minden vírus közös jellemzője volt, hogy saját magát másolta minden lehetséges helyre. Az kezdeti vírusirtók **ritkán** (1–4 hetente) **frissültek,** a köztes időben az új vírusok szabadon rombolhattak. ✓ 1 PONT

A '90-es évek közepétől jelentek meg az ún. **makrovírusok**, melyek a Microsoft Word és Excel alatti script-nyelven megírt Office-segítségeket használták ki. Amióta az Apple gépeken is futnak a Microsoft Office programok, azóta az Apple Macintosh

gépein is lehetnek makrovírusok. Néhány évvel később a Linuxos gépekre is készült Windows-emulátor, így a Linuxos gépeken is lehetnek ilyen vírusok.

✓ 1 PONT

A 2000-es években az internet rohamos terjedése magával hozta a vírusfertőzések jelentős növekedését. A legtöbb vírus az ismerősöktől **e-mailben kapott** gyanútlanul **megnyitott mellékletek** útján terjedt. Számtalan olyan fertőzés is létezik, amely **megszerzi** a megtámadott gépen lévő **ismerősök e-mail-listáját,** és minden címre elküldi saját magát. A technika fejlődésével és a közösségi oldalak sikerével a vírusok terjedése is fokozódott. Napjainban egy jól megírt féreg 1-2 hónap helyett, akár 1-2 óra alatt is gépek százezreit fertőzheti meg. 2010 óta kifejezetten **mobiltelefonra írt vírusok** is léteznek, amelyek az okostelefonok (smartphone) felhasználóinak szabályait kerülik ki.

✓ 1 PONT

A vírusok főbb típusai:

- **Nem rezidens vírus:** azonnal keres másik megfertőzhető gépet, ahol terjesztheti magát.
- **Rezidens vírus:** nem keres azonnal másik megfertőzhető gépet, hanem végrehajtható állományként betölti önmagát a memóriába és átadja a vezérlést a fogadó programnak.
- **Gyorsan fertőző vírus:** arra tervezték, hogy minél hamarabb megfertőzze az összes lehetséges elérhető fájlt (pl. a magát vírusirtónak álcázó vírus). A fertőzés nagy CPU-használattal jár.
- **Lassan fertőző vírus:** csak ritkán aktivizálódó vírusfajta, mely titokban működik. Néhány lassan fertőző vírus csak akkor fertőz meg egy fájlt, amikor azt másolják.
- **Trójai vírus:** ártalmatlannak látszó program, mely a vírusmentes számítógépen aktivizálja magát.
- **Boot-vírus:** a gép bekapcsolásakor aktivizálódik és az egész gépet megfertőzi.
- **Makrovírus:** általában levélben kapott Office-fájlokhoz csatolt kártevő.
- **HTML/JS/VB-vírus:** weblapok kódjaiban megbújó kisebb-nagyobb kártevő.
- **Önálcázó vírus:** önmagát egy másik állománynak álcázza pl. picture.jpg.exe.
- **Polimorf vírus:** képes a saját kódját változtatni, így nagyon nehéz felismerni.

✓ 3 PONT

Védekezési módszerek:

- **Csak eredeti programot használjunk!** A szoftverfejlesztő cégek csak így garantálhatják a termékeik vírusmentes és stabil működését.
- **Mindig használjunk vírusirtót!** A megszokott, jól bevált vírusirtó mellett időnként érdemes egy másikkal is tesztelni a vírusmentességet.
- **Használjunk jó minőségű vírusirtót!** A kiválasztásnál ne az számítson, hogy fizetős vagy ingyenes a program, inkább az, hogy naponta vagy naponta többször is

frissítse az adatbázisát, és ne lassítsa le észrevehetően a számítógépet (pl. ESET NOD32, AVG, Avast, Symantech, ClamWin, Kaspersky, Vipre stb.)!

- Csak olyan vírusirtót használjunk, amely a megszokott fájl-ellenőrzés mellett felügyeli a ki- és bemenő forgalmat, valamint az érkező és a fogadott leveleket is! Választhatunk olyan védelmet is, amely egyesíti a hagyományos vírusirtót a **tűzfallal** és a kéretlen levelek szűrőjével **(spam/malware).** Az ilyen komplex védelmet nyújtó csomagokat (pl. Comodo, Panda, Kaspersky, Norton, AVG) Internet Security néven forgalmazzák.
- **Telepítsük az operációs rendszer frissítéseit!** A frissített programok legtöbbször éppen az időközben felfedezett biztonsági réseket szüntetik meg, és így védettebbé válhat a rendszer.
- **Ne látogassunk ellenőrizetlen** (pl. Torrent, illegális letöltő, pornó stb.) **oldalakra,** ahol rengeteg vírus fertőzheti meg a számítógépet!
- Az állandó vírusvédelem mellett rendszeres időközönként (hetente vagy kéthetente) **ellenőrizzük a gép háttértárolóit!**
- Ne használjunk ellenőrizetlen lemezt, pendrive-ot vagy egyéb adathordozót!
- A fontos adatokról, fájlokról és beállításokról **készítsünk biztonsági mentést!** Felelőtlenség pl. az összes családi fotót azon a munkára és internetezésre is használt laptopon tárolni, amely könnyen fertőződhet. A fontos adatokat, fájlokat stb. mentsük egy külső HDD-re vagy optikai tárolóra (DVD, BR stb.), melyeket rendszeresen frissítsünk!
- Az **illegális filmnéző oldalak**on a felugró reklámok megnézése után kezdhetjük el nézni a filmet. Ezalatt az oldalakról származó vírusok átvehetik a számítógépünk egyes részeinek irányítását, és olyan illegális műveletekre kényszeríthetik, mint pl. spam küldése vagy virtuális valuta bányászata.

✓ 3 PONT

Megjegyzés: A gyakorlati feladat végrehajtása további 1 pontot ér.

✓ 1 PONT

KIEGÉSZÍTŐ KÉRDÉSEK

- Mit tegyünk, ha ismerősünktől szokatlan e-mailt kapunk?
  - Ellenőrizni kell, hogy nem egy vírus postázta-e magát automatikusan.
- Mennyire megbízhatóak az ingyenes vírusirtók?
  - Az otthoni számítógépen bármelyik ismert ingyenes vírusírtó biztonságosan használható.
- Mikor nem elegendő a Windows 10 beépített tűzfala és vírusirtója?
  - Erősebb vírusvédelem akkor szükséges, ha intenzívebben használjuk a számítógépet, illetve ha olyan „érzékeny" (pl. személyes adatok, bankszámlaszámok stb.) adatokat tartalmaz, amelyek sérülése súlyos következményekkel járhat.