14. tétel
Vírusirtás, víruskeresés: ismertesse a számítógépes veszélyforrásokat, ismertesse a védekezés lehetőségeit. Hogyan lehet a védekezést hardveresen megoldani, és hogyan lehet szoftveresen? Mondjon példát, mikor lehet a számítógép működésében bekövetkező változások alapján vírustámadásra gyanakodni!
Milyen veszélyei vannak a közösségi oldalaknak, az on-line beszélgetéseknek?

A számítógépes veszélyforrások lehetnek:

- Külső behatolók
- Vírusok
- Adatvesztés

A védekezés lehetőségei:

- A külső behatolók ellen tűzfallal lehet védekezni.
- Ha a gépet illetéktelen indítás ellen akarjuk védeni, használjunk jelszót
- Fokozottan védett rendszereket szoftveresen felhasználónévvel és jelszóval, hardveresen pedig mágneskártyával, ujjlenyomat azonosítóval is védhetünk.
- Szünetmentes tápegység alkalmazása adatvesztés ellen.

AZ EGYIK LEGFONTOSABB VESZÉLYFORRÁS A VÍRUS!

Manapság naponta keletkeznek új vírusok, melyek egyre nagyobb károkat okoznak, és egyre ügyesebben rejtik el magukat a víruskereső programok elől. Az internet és a számítógépes hálózatok elterjedésével határok nélkül, egyre nagyobb területeken támadnak.

A vírusok egy része ártalmatlan, mindössze üzeneteket jelenít meg a képernyőn. A vírusok másik része azonban használhatatlanná teheti állományainkat, vagy letörölheti azokat, esetleg fizikailag is tönkreteheti a gépet.

Számítógépvírusnak olyan programokat nevezünk, amelyek a rendszerbe engedély nélkül lépnek be, önmaguk másolására, többszörözésére, és más programok megfertőzésére képesek.
A vírusok többsége ezenkívül valamilyen esemény hatására, vagy egy előre meghatározott időpontban aktiválódva más károkat is okozhat az állományainkban.

Vírusok leginkább négyféle módon kerülnek a számítógépekre

- a webböngészőn keresztül, böngészés közben,
- spameken keresztül (spamekben érkeznek)
- letöltött fájlokkal
- és fertőzött adathordozókkal.

A vírusok általános jellemzői

- Rosszindulatú szoftver
- Általában ártó szándékkal készítették őket;
- Zavaróak, túlterhelhetik a gép erőforrásait
- Szaporodik és fertőz
- Információt továbbíthatnak a gépünkről (spyware)
- Nagyon kis méret;
- Futtatható állományokat képesek megfertőzni;
- Gyakran akár válogatva, időzítve tönkretesznek más fájlokat;
- Rejtetten működnek, esetleg akkor fedik fel magukat, ha feladatukat elvégezték;
- Egyre fejlettebb intelligenciával rendelkeznek, pl. változtathatják saját kódjukat és aktivitásukat

Milyen kárt okoznak a vírusok?

- A számítógép lelassítása, a merevlemez szabad kapacitásának csökkentése, újraindítás, stb.
- Adatok továbbítása az interneten böngészési szokásainkról, kedvenc oldalainkról.
- Fájlok tartalmának megváltoztatása, törlése.
- Winchester megformázása

- A belső hálózat többi gépének megfertőzése.
- Jogosultságok megváltoztatása, védelmi rendszerek kiiktatása.
- A felhasználó dokumentumainak szétszórása az interneten.

Az informatika rohamos fejlődésével a vírusok is jelentős változáson mentek keresztül.

A vírusok csoportosítása

1. *A károkozás mértéke, típusa szerinti csoportosítás*

Reprezentatív vírus
Főleg a vírusok megjelenésének korai szakaszában volt jellemző. A program jelzi jelenlétét, de egyéb kárt nem okoz.

Szoftvert károsító vírus
Az ilyen programok az állományokat károsítják, és ezért az adatbázisainkban vagy az operációs rendszerben is kárt tehetnek.

2. *A támadás célpontja szerinti csoportosítás*

Boot vírusok
A boot vírusok az első vírusok közé tartoznak. Leggyakrabban akkor terjednek, ha fertőzött lemezzel indítjuk el a rendszert. Ebben az esetben a vírus a merevlemez boot szektorába ágyazódik be, így még az operációs rendszer betöltése előtt aktiválódik. Ennek hatására a fertőzött merevlemez az összes meghajtóba helyezett lemezt megfertőzi. A boot vírusok napjainkban a kevésbé elterjedt vírusfajták közé tartoznak.

Programvírusok
A programvírusok általában a .COM és .EXE kiterjesztésű fájlokba ágyazódnak. Amikor a fertőzött programot elindítjuk, a vírus a memóriába töltődik, és minden futtatott programra átterjed.

Makrovírusok
A makrovírusok gyakoriságát az internet elterjedése okozta. A makro nem más, mint névvel ellátott, automatikusan ismételhető utasítássorozat. A makrovírusok azt a lehetőséget használják ki, hogy például a szövegszerkesztőkben, táblázatkezelőkben a gyakran ismételt lépéssorozatokat makrókkal automatizálhatjuk. Terjedésükhöz egy fertőzött dokumentum megnyitása vagy egy dokumentum elmentése is elegendő.

Férgek és trójai programok
A vírusokkal kapcsolatban beszélhetünk még úgynevezett férgekről és trójai programokról. A férgek és a trójai programok hagyományos értelemben nem vírusok, de hatásukat tekintve igen hasonlítanak hozzájuk.

A férgek az operációs rendszerek védelmi hiányosságait, réseit kihasználva okoznak kárt. A férgek a vírusokhoz hasonlóan szaporodnak, de nem fájlokat fertőznek meg, hanem az interneten vagy a hálózaton magukat e-mailekhez csatolva gépről gépre terjednek. A férgek elsődleges célja, hogy egyetlen futtatással minél több számítógépre terjedjenek át.

A trójai programok olyan önálló alkalmazások, melyek első pillantásra hasznos alkalmazásnak tűnnek, azonban kártékony kódot tartalmaznak. Hatásukat csak az elindításuk után fejtik ki.

Kémprogramok (spyware)
Célja, hogy adatokat gyűjtsenek személyekről vagy szervezetekről azok tudta nélkül a számítógép-hálózatokon. Az információszerzés célja, lehet békésebb, például reklámanyagok eljuttatása a kikémlelt címekre, de ellophatják számláinkat jelszavainkat, vagy más személyes adatainkat rosszindulatú akciók céljából. A vírusokhoz hasonlóan lehet őket „beszerezni”.

Természetesen azok a programok, amelyek a felhasználó tudtával és beleegyezésével kérnek adatot, nem tekinthetők kémprogramoknak.

Vírusok jellemzői
A vírusok tulajdonságait tekintve minden vírus a következő két csoport valamelyikébe sorolható.

- A **lopakodó vírusok** úgy terjednek, hogy a fájlba ágyazódva bekerülnek a memóriába, és ott a fájlok eredeti hosszát mutatják, esetleg a fájl eredeti tartalmát szimulálják.
- A **polimorf vírusok** önmaguk titkosításával, állandó változtatásával terjednek, ami megnehezíti felismerésüket.

Vírusvédelem

A vírusok terjedésének megakadályozására az egyik legbiztosabb módszer a megelőzés. A vírusfertőzés során okozott károk mértéke csökkenthető:

- rendszeres mentéssel,
- a beérkező levelek, lemezen szállított adatok használat előtti ellenőrzésével,
- rezidens vírusellenőrző program telepítésével, amely a memóriában marad, és folyamatosan ellenőrzi a használt fájlokat,
- rendszeres biztonsági másolat készítésével,
- jogtiszta szoftverek használatával.
- Rendszeres vírusellenőrzés.
- Rendszeresen frissítsük vírusirtó programjainkat.
- Tűzfal használata

Vírusirtó programok (szoftvere védekezés)

Napjainkban egyre több vírusirtó programmal találkozhatunk. Ezek a programok hatékony védelmet nyújtanak az egyre nagyobb számban megjelenő károkozó vírusok ellen.

A legismertebb vírusirtó programok közé tartozik az AVG, ESET NOD 32, AVAST, stb.

A vírusirtó programok általában úgy működnek, hogy a már ismert vírusok kódjának jellegzetes részeit keresik az általunk kijelölt meghajtókon, fájlokban.

Ezt az adatbázist folyamatosan frissíteni kell, különben az újabb vírusokat nem ismerik fel.

A felismert vírusok a megfertőzött fájlokból nem mindig távolíthatók el, ilyenkor a vírusirtó azt átnevezi vagy törli.

Az ún. rezidens vírusirtó programok folyamatosan a memóriában tartózkodnak és valamennyi fájlműveletet ellenőriznek. Használatuk csak a különösen veszélyeztetett gépeken ajánlott, mert jelentősen visszafoghatják a számítógép teljesítményét.

Védelmi rendszerek (hardveres védekezés)

Gépünkön tárolt adataink biztonságát az interneten keresztül is számtalan veszély fenyegeti. Hackerek törhetik fel rendszerünket, ezáltal fontos és személyes adatainkat ellophatják, megrongálhatják. Adataink védelmére számos védelmi rendszert állíthatunk fel. A két leggyakrabban alkalmazott védelmi rendszer a **tűzfal** és a **proxy**.

Tűzfal (Firewall) alkalmazásával szabályozni lehet a be- és kimenő internetforgalmat, hogy kik, mikor, milyen szolgáltatásokat, milyen protokollon keresztül érhetnek el. A belső hálózat ezen az egy ponton keresztül csatlakozik a külvilághoz.

A **proxy** több feladatot ellátó segédszerver, mely magába foglalja a tűzfal szolgáltatásait. Figyeli és szűri a beérkező és kimenő kéréseket, valamint a felhasználók között megosztja az internet-hozzáférést. A HTML-oldalak gyorsabb eléréséhez letölti, és saját háttértárán tárolja a gyakran leolvasott oldalak tartalmát, így a felhasználók számára lényegesen gyorsítja a gyakran látogatott oldalak elérését.

Példa

Sorolja fel, hogy milyen fizikai veszélyforrások hathatnak egy informatikai rendszerre?

- Tűz
- Víz, nedvesség (csőrepedés, billentyűzetre ráömlő folyadék, páralecsapódás)
- Napsütés
- Por, füst
- Rengések (földrengés, járműforgalom)
- Villámlás, elektromos kisülések
- Elektronikus hálózat zavarai
- Statikus elektromosság
- Mechanikai sérülések
- Rágcsálók, ízeltlábúak