Előzmények

A történelem legelső vírusai csak elméleti alapon léteztek. Feladatuk ugyanis a Neumann Jánostól származó teóriának az igazolása volt, hogy mesterséges életet lehet létrehozni a bináris világban, azaz lehet olyan programot írni, amely az élet alapvető jellegzetességeit (vagy legalább részleteiben) megvalósítja. Az elmélet napjainkra kissé elfajult...

Ezenkívül egy másik fontos történet is szerepet játszott a vírusok kialakulásában: az 1980-as évek legelején a számítógépek már tudtak kommunikálni egymással telefonvonalakon keresztül és az amerikai telekommunikáció olcsósága miatt ez nem volt egyedi, ritka esemény. Eme számítógépes vonalakon keresztül cseréltek egymással adatokat, illetve információkat. Az információk között persze megbújtak egyes kisebb-nagyobb játékok. A számítógépek telefonszámaira persze amatőr felhasználók is rájöttek és szerették volna a nagygépeken lévő játékokat ellopni a saját kicsi gépeikre. Persze addig nem akarták használni a méregdrága távolsági hívásokat, így olyan speciális programocskákat írogattak, amik ezeket a játékokat megkeresik és elküldik az ő otthoni számítógépükre. A keresőprogram olyannyira profira sikeredett, hogy átment sok nagyszámítógépbe is és ott tovább kutakodott. Egy idő után az USA szinte valamennyi nagyszámítógépe csak ezt a keresőprogramot kutatta. A nagygépeken dolgozó profi programozók persze fejvesztve kutatták a keresőprogram megállításának, illetve kiirtásának ellenszerét. A keresőprogram olyannyira elfajult, hogy már az interkontinentális ballisztikus (nukleáris robbanófejjel felszerelt) rakéták indítókódját is majdnem feltörte. Ekkor sikerült az első ellen-programot megírni. Az ellenprogram olyannyira sikeres volt, hogy valamennyi nagygépen felrakták és így nem bénult le az USA teljes szuperszámítógép-parkja. A következő betörési kísérlet már a nagyprogramok speciális fajtáját akarta letörölni, és a gépeket használhatatlanná tenni. Ezt is sikerült kicselezni. A programok és az ellenprogramok párharca azóta is tart. A legkülönösebb dolog, hogy az eredeti keresőprogramot egy tinédzser írta.

Az idők folyamán természetesen sok minden megváltozott, így a vírusok támadási módja is. A hirtelen halált okozó vírusok kihalófélben vannak, a vírusok szülőatyjai ugyanis rájöttek, hogy a valódi járvány kialakulásához a vírusnak hosszú ideig kell észrevétlenül lappangania, és később, amikor már elterjedt, akkor kell aktivizálódnia. A vírusok osztályozását az operációs rendszertől való függés, illetve a terjedési metódus alapján végzik el. Az operációs rendszereket is két részre oszthatjuk: immunis és nem immunis. Előbbi kategóriába sorolhatók a különböző Unix-verziók, beleértve a Linuxot. Kifejezetten vírusra termett operációs rendszer a DOS, illetve a Windows különböző változatai. Az operációs rendszerek szerinti csoportosítás másik felét a platform - független vírusok jelentik. Ezek többségét a Microsoft által kifejlesztett, majdnem szinte minden platformon használt makrónyelveken írják. S ha már itt tartunk, a vírusok közé kell sorolnunk a com-objektumokat és az ActiveX-vezérlőket, amelyek a Windows világ mellett az egységesítés jegyében más rendszereken is megjelentek.

A legősibb vírusok a DOS-világban jelentek meg. Először a *.com kiterjesztésű programoknál, amelyekhez hozzákapcsolódva jöttek, láttak, és megfertőzték az egész világot. Később a lemez indítórekordját (boot sector), majd később a partíciós tábla programját vették célba, így akár üres lemez segítségével is terjedni tudtak. Így jelent meg egy új iparág: megszülettek azok a vállalkozások, amelyek a vírusirtásra alapozták jövőjüket. Ezekből a cégekből nőtt ki jó pár ma világhírű, milliárdos

forgalmú multinacionális vállalkozás: Symantec, McAfee Network Associates, Kaspersky Laboratorium.

Az antivírusprogramok legrégebbi technológiája a szekvenciális keresés, amit már a víruskorszak hajnalán alkalmaztak. Ilyenkor a program végigfut az állományokon, s a vírusok ismert és jellemző részleteit, a szekvenciasorokat igyekszik kimutatni azzal a felkiáltással, hogy a véletlenszerű egyezés nem valószínű. Ez így is van, ha a szakasz kellő hosszúságú, és több jellegzetes részletet tartalmaz. Van azonban egy kis probléma: a tömörített állományokban, adatbázisokban lévő vírus így nem ismerhető fel.

Vírusok

A számítógépes vírus olyan önsokszorosító program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Ez a működés 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. A vírus csupán egyike a rosszindulatú szoftverek számos típusának. Ez megtéveszthető lehet a számítógép felhasználók számára, mivel mára lecsökkent a szűkebb értelemben vett számítógépes vírusok gyakorisága, az egyéb rosszindulatú szoftverekhez, mint például a férgekhez képest. Bár a számítógépes vírusok lehetnek kártékonyak (pl. adatokat semmisítve meg), a vírusok bizonyos fajtái azonban csupán zavaróak. Némely vírus késleltetve fejti csak ki hatását, például csak egy bizonyos számú gazdaprogram megfertőzése után. A vírusok domináns kártékony hatása az ellenőrizetlen reprodukciójuk, mely túlterhelheti a számítógépes erőforrásokat. Napjainkban az Internet térhódításával vírusok már valamivel kevésbé gyakoriak, mint a hálózaton terjedő férgek. Az antivírus szoftverek, melyeket eredetileg a számítógépes vírusok elleni védelemre fejlesztettek ki, mára már képesek a férgek és más veszélyes szoftverek, mint pl. a spyware elleni védelemre is.

Gyakori jellemzőik:

A gazdaprogramok megfertőzése és az önsokszorosító viselkedés valamennyi vírusra jellemző. Ezen kívül gyakran rendelkeznek a következő tulajdonságokkal:

- nagyon kis méret;
- legtöbbjük a Microsoft Windows operációs rendszereken okoz gondokat;
- futtatható állományokat képesek megfertőzni;
- általában ártó szándékkal készítették őket;
- 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

Alaptípusaik:

- fájl-fertőző vírus
- boot szektor vírus
- makró-vírus
- e-mail vírus

- trójai-program

Férgek

A férgek történelmileg a nagygépes rendszereken alakultak ki, és létezésük a hálózathoz kötődik. A férgek is szaporodnak, de a vírusokkal ellentétben nem programokat fertőznek meg, hanem az a céljuk, hogy egyre újabb és újabb gépekbe jussanak be. Mivel manapság több olyan szerzemény jelent meg, mely vírusszerű és féregszerű tulajdonságokkal is rendelkezik, célszerű lenne e két csoportot egy kalap alá venni. Ez talán meg is tehető, ha a vírusok definícióját egy picit kitágítjuk, mondjuk így: ``A vírus egy olyan program vagy programtöredék, amely önhatalmúlag terjeszti magát."

Az első férget 1978-ban készítette el a Xerox PARC két kutatója.

Az önsokszorosításon kívül a féreg sokféle dologra beprogramozható, például a fájlok törlésére a gazdarendszeren, vagy önmaga elküldésére e-mailben. Az újabban megfigyelt férgek több végrehajtható állományt is visznek magukkal. Még valódi ártó szándékú kód nélkül is súlyos fennakadásokat okozhatnak, csupán azzal, hogy sokszorozódásuk kiugróan magas hálózati forgalmat generálhat. Például a Mydoom féreg terjedése csúcsán világszerte észrevehetően lelassította az Internetet.

Trójai programok

A trójai program szintén egy látszólag hasznos, vicces vagy egyéb módon érdeklődésre számot tartó program, amelybe azonban rejtett funkciót építettek. Előfordul, hogy egy teljesen új programot írnak e célra, de előfordul az is, hogy egy létező, jól ismert programot egészítenek ki, általában nem az eredeti szerzők. Ilyen esetekben például egy szép nagy verziószámot írnak rá, és a lelkes felhasználók máris terjeszteni kezdik a friss kiadást. A rejtett funkció lehet közvetlen károkozás, de gyakori még a vírustelepítés , a jelszólopás vagy egyéb titkos információk megszerzése, hátsó ajtó létrehozása. A trójai programok szándékosan károsítónak készülnek, tehát a rossz minőségű vagy hibás programok nem számítanak ebbe a csoportba. Egyes cikkekben trójai programnak nevezik a vírusfertőzött programot is. Az én szóhasználatomban a vírus által megfertőzött program nem trójai, de ha a program célja a vírustelepítés, akkor az.

A vírusok osztályozása

A vírusokat többféleképpen lehet csoportosítani. A csoportosítási módok általában egymástól függetlenek, de van, amikor az egyik fajta osztályozásban elfoglalt hely maga után vonja a másik fajta osztályozás egyik kategóriáját. A Java vírusok például mindig fájlvírusok.

Típus szerinti osztályozás:

- **fájlvírusok:** a vírusok klasszikusnak mondható fajtáját fájlvírusoknak nevezik. Ezek jellemzője, hogy a futtatható programhoz oly módon fűzik hozzá magukat, hogy a módosított program a vírus terjesztéséről (is) gondoskodjék.

- **boot vírusok:** a merevlemez boot szektorába fészkeli be magát és a számítógép elindulásakor onnan kezdve megfertőz mindent, amit a gépbe helyezünk vagy már csatlakoztatva van.
- **makrovírusok:** napjaink legnagyobb járványait a makrovírusok okozzák. Régen programokat csereberéltek az emberek, ma már inkább a dokumentumok csereberéje a gyakori. A makrovírusok valójában interpreteres vírusok, melyek arra utasítják a futtató alkalmazást, hogy végezze el nekik a piszkos munkát, új makrókat hoznak létre, így akár eredetileg makrómentes dokumentumokat is meg tudnak fertőzni.
- **polimorf vírusok:** gyakorlatilag bármelyik fenti vírustípus lehet polimorf. Jellemzőjük, hogy minden újabb fertőzéskor megváltoznak, ezért a kereső programok vírusdefiníciói többé nem ismerik fel.
- **retrovírus:** a retrovírusok a víruskereső alkalmazásokat támadják meg úgy, hogy megpróbálják törölni, vagy egyéb úton hatástalanítani a vírusirtó programfájlokat, vírusinformációkat. Az utóbbi időben nagy vihart kavart SirCam vírus nem csak e-mail útján terjed, hanem a belső számítógépes hálózat megosztott könyvtárain keresztül is fertőz. Ilyen vírus eddig nem létezett.
- **programvírusok:** ezek a vírusok COM és EXE fájlokba ágyazódnak. A fertőzés általában úgy történik, hogy a fertőzött program futtatásával a vírus a memóriába töltődik, és minden futtatott programra átterjed.

Platform szerinti osztályozás:

A vírus nagyon fontos tulajdonsága, hogy milyen rendszerek alatt képes működni. Ha egy vírust nem készítenek fel egy adott rendszerre, akkor nem is fog működni az alatt. A vírusplatformok száma egy új felhasználói program megjelenésével könnyen növekedhet.

- **DOS vírusok:** a DOS vírusok a DOS rendszerek fájlformátumait fertőzik meg, azaz a COM és EXE, esetleg SYS és egyéb fájlokat. Ehhez csak az adott fájlformátum tulajdonságait kell a vírusnak és írójának ismernie. A CEB vírusok a DOS-nak azt a tulajdonságát használják ki, hogy a COMMAND.COM a kiterjesztés nélkül megadott programokat a következő sorrendben keresi: *.com, *.exe, *.bat. Ha egy vírus az EXE vagy BAT fájlok mellett létrehoz egy COM állományt, akkor a futtatni kívánt program helyett a vírus indul el, majd az természetesen végrehajtja az eredeti programot is, hogy ne bukjon le.
- **Windows vírusok:** Két olyan EXE kiterjesztésű fájlformátum van, amit egy windowsos vírus célba vehet: a régebbi, 16 bites formátum a NewEXE (NE), az újabb, 32 bites a Portable EXE (PE). Hely hiányában itt nem tudok kitérni a fájlformátumok részleteire. A fájlformátumon kívül a vírusoknak csak a védett móddal kell megkűzdeniük. A vírusok szerencséjére Windows alatt (ha az NT-t nem számítjuk) ezt a fogalmat nem kell túl komolyan venni.
- **OS/2 vírusok:** a Windows mellett OS/2-re is jelentek meg vírusok. Talán azért, mert ez az operációs rendszer kevésbé elterjedt, az OS/2-es vírusok száma egy számjegyű. Természetesen a DOS-os vírusok futnak OS/2 alatt is.
- **Linux vírusok:** mint minden operációs rendszerre, Linuxra is lehet írni vírusokat. A vírusíró két megoldás közül választhat. Az egyik szerint kizárólag az operációs

rendszer számára legális műveleteket végez (beleértve ebbe az írható programok megfertőzését is), a másik megoldás szerint viszont egy vagy több biztonsági hibát kihasználva root jogosultságokat szerez, és átveszi a hatalmat a gép felett. Az első megoldás hátránya, hogy a vírus talán soha nem terjed el (a gyakorlatban eddig ez volt a helyzet), a másodiké pedig az, hogy a biztonsági hibákat hamar kijavítják, és a vírus többé nem tud működni. Talán a két megoldás kombinációja adhat valami esélyt a vírusnak, mert a biztonsági hiányosságokat kihasználva el tud terjedni annyira, hogy utána kevésbé eredményes módszerekkel is beérje.

- **Java vírusok:** a Java egy platform - független programozási nyelv, így a Java vírusok nagy előnye (a saját szempontjukból), hogy ők is platform - függetlenek lehetnek. Ezek a vírusok nem a Java appleteket, hanem a Java alkalmazói programokat szokták megfertőzni, melyek ugyanolyan programok, mint a winchesteren található összes többi, csak Java Virtuális Gép kell a futtatásukhoz. A böngészőprogramok írói azt ígérik, hogy az esetleges kártékony kód onnan nem szabadulhat el, de mivel egyik program sem tökéletes, semmiképpen sem szabad vakon bíznunk ezekben az ígéretekben. Ha rosszul állítjuk be a böngészőt, és kikapcsoljuk az alapértelmezés szerinti korlátozásokat (pl. az applet csak a saját szerverével létesíthet hálózati kapcsolatot, és nem férhet hozzá a helyi meghajtókhoz), akkor szintén kitesszük magunkat a támadásoknak.
- **HTML vírusok:** a HTML vírusok a valóságban valamilyen script vírusok, ugyanis a HTML-t magát nem lehet programozni. Létezik olyan VBScript vírus (pl. HTML/1nternal), amelyik saját kódját másolja be a winchesteren talált html állományokba. Ehhez azonban írási jogra van szükség a helyi meghajtókra. A Microsoft Internet Explorer egyes verzióiban van egy olyan hiba, amely lehetővé teszi, hogy egy túl hosszú URL hivatkozás megadásával az Internet zónába tartozó dokumentumok olyan jogosultságokkal fussanak, mintha azokat a helyi meghajtókról indítottuk volna.
- **Word, Excel, PowerPoint vírusok:** a Microsoft Word alatt futó vírusok platformja nem a szövegszerkesztőt futtató operációs rendszer , hanem a Word, mert a makrovírus az operációs rendszer típusától függetlenül képes futni. A Macintosh alatti Microsoft Word ugyanazokat a vírusokat képes futtatni, mint a windowsos, néhány kivételtől eltekintve. Ugyanez elmondható az egyéb makro-programozható alkalmazásokra is, például az Excelre.
- **emberi platform:** ide azok a vírusok tartoznak, melyeket az ember terjeszt. Nem a biológiai vírusokról, hanem azokról a lánclevelekről van szó, melyek valamilyen fontos cél elérése érdekében arra kérik az olvasót, hogy küldje tovább a leveleket minden ismerősének. Ezek a levelek általában álhíreket tartalmaznak rákbeteg gyerekekről, veszélyes vírusokról és hasonlókról. Sok olyan jellemzőjük van, mely a gyakorlottaknak rögtön feltűnik. Ilyen jellemző elsősorban az, hogy mindenkinek el kell küldenünk. Jellemző még egy befolyásos cég, vagy több cég emlegetése, nagybetűk és felkiáltójelek felesleges használata, tények hiánya.

Víruskeresők elleni technikák szerinti osztályozás

- **kódolt vírusok:** ezeknek a vírusoknak a fő része (teste) kódolt, és azt egy dekóder kódolja ki induláskor. A kódolás kulcsa általában minden példánynál más és más, véletlenszerű. Nyilván a kulcs is tárolódik a dekóderben , vagy egy adatterületen. Előnye a megoldásnak az, hogy rövidebb a szekvencia (maximum a

dekóder mérete), a kíváncsi ember számára nem láthatók a vírusba rejtett üzenetek, és a heurisztikus keresőknek is dekódolniuk kell a vírustestet, ha részletesebben meg akarják vizsgálni.

- **polimorf vírusok:** hasonlítanak a közönséges kódolt vírusokhoz, azzal a különbséggel, hogy a dekóderük is változik. Az alkalmazott technikák nagyon sokfélék, lehetséges az utasításokat kicserélni egy ugyanolyan eredményt adóra, lehetséges más regisztereket használni, utasításokat felcserélni, és a lényeget nem változtató utasításokat beszúrni. A jó polimorf kód ezt mind megcsinálja.
- **lopakodó vírusok:** a lopakodó vírusok célja, hogy a víruskereső hiába keresi a vírust, ne találja azt meg. A legtöbb lopakodó vírus a boot-vírusok között található. Annyi a dolguk, hogy ha bárki a boot-szektort (partíciós táblát) próbálja olvasni, akkor ne az igazit (a vírusosat), hanem az eredetit (vírusmenteset) olvassa be, és adja vissza. A lopakodó fájlvírusok a fájlkezelő DOS funkciókat irányítják magukra, és vagy mindig megkeresik a kért bájtok eredeti tartalmát, vagy egyszerűen a fájlok megnyitásakor kiirtják onnan magukat, zárásukkor pedig visszafertőzik azt. A lopakodásnak különböző fokozatai vannak, a One Half például nem mutatja az eredeti tartalmat, de a könyvtárlistában levonja a saját hosszát a fertőzött fájlok teljes hosszából.
- **visszafejtés elleni vírusok:** a visszafejtés elleni védelemnek több módszere létezik, ezek a módszerek megegyeznek a hagyományos programok hasonló célú védelmeivel. A disassemblálás megnehezítésére többszörös kódolásokat és összevissza ugrásokat helyeznek a kódba. Gyakori az olyan szubrutinhívás, amely sosem tér vissza a hívási helyre. A valós nyomkövetés megnehezítésére elsősorban a nyomkövető regiszterek és megszakítások átírása a megoldás. A vírus mérheti az utasítások közötti időt, átállíthatja a veremmutató értékét, miközben elvileg nem jöhet megszakítás, stb. Ha a vírus észreveszi, hogy nyomon követik, akkor elágazhat egy e célra készült ágra, amely jól beviszi az elemzőt az erdőbe.

Vírusok eltávolítása

Vírusok eltávolítására két módszert ajánlanak. Az első a biztonsági másolatról történő helyreállítás. Biztonsági másolat hiányában kénytelenek vagyunk a fertőzött állományt megtisztítani. Ilyenkor mindennek az ellenkezőjét kell tenni, és ellenkező sorrendben, mint ahogy a vírus csinálta. Ez például felülíró vírusok esetében lehetetlen. Általában azt lehet mondani, hogy ha egy program vírusosan működik, akkor abból ki lehet ölni úgy a vírust, hogy a program utána is működjön. A fertőtlenített állomány nem minden esetben lesz bitről bitre azonos az eredetivel, mert egyes vírusok eltűntethetnek információkat.

- **fájlvírusok eltávolítása:** bizonyos vírusok esetén nem kell mást tennünk, mint törölni az állományt. Ha például egy felülíró vírus teljes megsemmisítette az eredeti tartalmat, akkor nem tehetünk mást. Akkor is törölnünk kell, ha mondjuk egy companion vírusról van szó, és ez a fájl maga a vírus. Végül akkor is törlés a tennivaló, ha a fájl valójában nem vírus, hanem trójai program, vagy féreg.
- **boot-vírusok eltávolítása:** a boot-vírusok eltávolítása csak annyiban különbözik a fájlvírusok eltávolításától, hogy nem bájtokkal, hanem szektorokkal dolgozunk. A legegyszerűbb esetben, példa erre a Michelangelo , a vírus változatlanul elmenti

az eredeti szektort, nekünk csak ennek a helyét kell megtudni, és visszamásolni. Ízlés szerint a vírus által kitöltött szektorokat ki lehet nullázni. Bonyolultabb eset, amikor az eredeti boot-szektor nincs meg változatlan formában. Ekkor nincs mese, össze kell rakni a szektort darabokból. A darabok valahol meg kell legyenek, mert a vírus is egyberakja azokat, hogy az eredeti betöltési folyamat el tudjon indulni. Ha mégis egy olyan vírussal van dolgunk, mint a REX , amelyik saját rutinjával kiváltja az eredeti partíciós kódot, akkor vagy feladjuk a helyreállítást, vagy generálunk egy általános szektort.

- **makrovírusok eltávolítása:** itt az irtási procedúra is más, mint egy hagyományos fájlvírusnál. Itt a keresés és irtás makrók tartalmának ellenőrzését, és makrók törlését jelenti. Ha ezeket az alap funkciókat sikerül megvalósítanunk, akkor az új makrovírusok irtásának a programba építése már semmiség.

Vírusirtók

Nagyon sok ember használja a DOS és a Windows különböző változatait. Ezek az operációs rendszerek nem tudják megvédeni magukat és a felhasználókat a vírusoktól, így külön programra van szükség erre a feladatra. A UNIX rendszerek eddig elég jól tartották magukat, de elsősorban a Linux növekvő népszerűsége azt okozza, hogy a vírusírók kezdik felfedezni maguknak ezt a platformot. A kezdő felhasználók és a Linuxot windowsosító disztribúciók megjelenése csak növeli a támadható pontok számát. A windowsos irodai csomagok átültetése UNIX-ra pedig a makrovírusok számára nyitja meg az utat. Egy jó szerver feladata nemcsak a saját védelme, hanem a rajta tárolt állományok vírusellenőrzése is. E hagyományosabb feladat mellett a közelmúlt történései megerősítik, hogy a levelező szervernek is ellenőriznie kell a leveleket, és ki kell szűrnie a vírusokat.

A víruskereső három szintből áll. Minden szint az eggyel alatta levőre épül.

- **első szint** a vírusadatbázis, mely az egyes vírusok tulajdonságait tartalmazza. Többek között megadja, hogy a vírust milyen szekvenciával vagy milyen algoritmussal lehet megtalálni. Az irtás lépései is itt tárolódnak. Az algoritmusok egy virtuális gépen futnak, hogy az adatbázis gépfüggetlen lehessen. Így, ha egy új adatbázis jelenik meg, akkor minden ezt használó víruskereső rögtön ismerni fogja az új vírusokat, függetlenül attól, hogy milyen gépen futnak.
- **második szint** a hordozható vírusölő függvénykönyvtár, feladata a fájlokban való víruskeresés, a vírusok kiölése, könyvtárfákon való végighaladás, stb. Annak érdekében, hogy ez a rész is hordozható legyen a különböző géptípusok között, a könyvtár C-ben íródik. Filozófiája szerint minden vírus fájlvírus. Például a boot-vírus is. Ekkor a fájl a teljes winchester vagy a teljes partíció, a cilinderek, fejek és szektorok száma pedig attribútumként kérdezhető le.
- **harmadik szint**en található felhasználói programoknak nem kell törődniük a vírusok lelkivilágával, egyszerűen csak hívogatniuk kell a második szint rutinjait, és végezniük kell a saját dolgukat. Két fajta programot különböztethetünk meg: az első a víruskereső (-ölő), a másik az egyéb program. A víruskereső feladata a felhasználó kívánságait a függvénykönyvtárnak átadni, és viszont. A hagyományos víruskeresők esetében gyakran választanunk kell egy sokat tudó és egy kényelmes program között. Mivel a mi esetünkben a két jellemző két külön programba van szétosztva, nem kell megalkudnunk. Az egyéb programok

általában olyan szerverprogramok, melyek fájlokkal dolgoznak. Elég a programnak megmondania, hogy mit kell ellenőrizni, és rögtön visszakapja, hogy vírusmentes-e az adott fájl. Ha vírusos lenne, akkor megteheti például, hogy karanténba zárja, és levelet küld a rendszergazdának , és/vagy a fájl tuladjonosának. Ilyen módon rögtön ki lehet szűrni például a levélben érkező vagy a webről letöltött vírusokat. A felhasználók érdekében általános viselkedése kell legyen minden programnak, hogy csak kérésre változtat meg bármit, mert lehetséges, hogy egy, a program szerint nyilvánvaló hiba kijavítása után a helyreállítás sokkal több erőfeszítést igényel, ha egyáltalán lehetséges. Természetesen ez nem azt jelenti, hogy minden kérdést fel kell tenni, lehetséges mondjuk egy ``mindent kijavít'' opció.