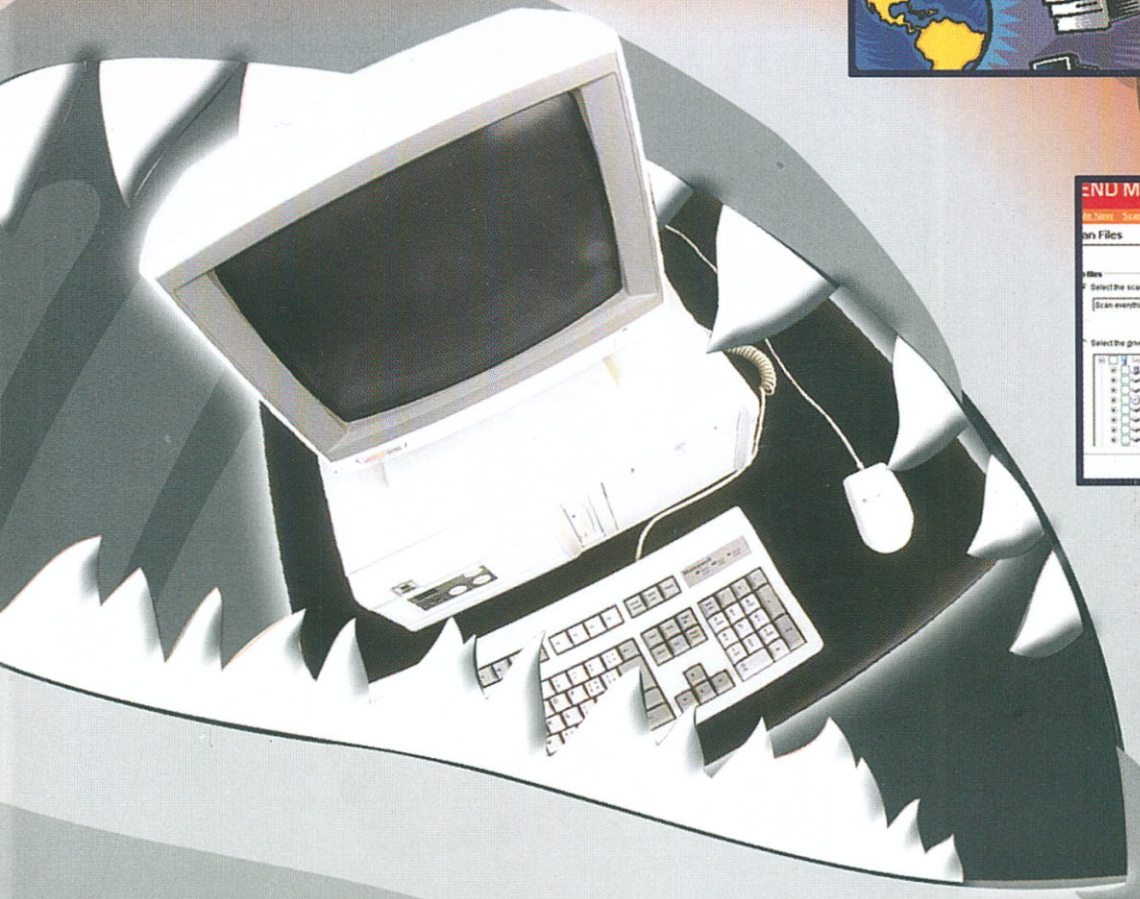
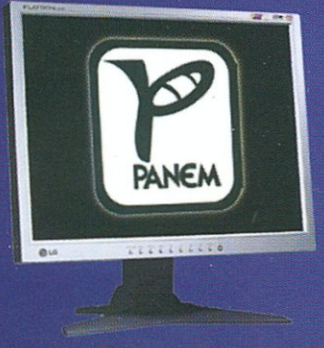
DREILINGER TÍMEA

VÍRUSVÉDELEM





PANEM
PRAKTIKUS
INFORMATIKA

DREILINGER TÍMEA

Vírusvédelem

Panem Praktikus Informatika

PANEM

ISBN 963 545 412 0

A kiadásért felel a Panem Kft. ügyvezetője
Lektorálta: Tarr Bence
Szerkesztette: Dávid Krisztina
Borítóterv: Tóth Attila
Tipográfia és tördelés: Székffy Tamás
panem@panem.hu
www.panem.hu

TARTALOMJEGYZÉK

ELŐSZÓ

„A számítógép senkivel nem bánik sehogyan sem! A számítógép matematikai eszköz, amelyet adatok tárolására és kezelésére hoztak létre. A felelősség azoké, akik beprogramozzák és kezelik…"

Isaac Asimov: A Hold tragédiája[1]

A „vírus" szót hallva az emberek többsége hajlamos – biológiai tanulmányaira támaszkodva – olyan mikroorganizmusokra gondolni, amelyek legyengítik a szervezetet, vagy akár halált is okozhatnak. Ugyanakkor a köztudatban lassan elterjed a szónak egy másik, informatikai értelmezése is. Mi is az a számítógépvírus? És miért kell vele foglalkoznunk?

Napjainkban a számítógépeken tárolt és feldolgozott adatok értéke több nagyságrenddel haladja meg a hardver és a gépeken futtatott szoftver pénzben kifejezhető együttes értékét. Fontos tehát, hogy súlyuknak megfelelően értékeljük és kezeljük a számítógépes adatbiztonsággal kapcsolatos feladatokat. Mindenkinek – akár otthonában, akár a munkahelyén használ vagy felügyel számítógépet – tisztában kell lennie a rendszereket fenyegető veszélyek természetével, komolyságával, valamint a megfelelő megelőző és helyreállító intézkedésekkel. Ha e fenyegetésekre megfelelően felkészülünk, egyrészt jó eséllyel előzhetjük meg a rendszerek összeomlását és az ezzel járó adatvesztést, másrészt a rendszeres adatmentéssel megteremtjük annak a lehetőségét, hogy – ha a baj mégis bekövetkezne – visszaállítható legyen a meghibásodás előtti állapot.

Megelőzhető-e a vírusfertőzés? Milyen eszközök állnak rendelkezésünkre a megelőzésben? Ezek milyen hatékonyságú védelmet biztosítanak számunkra? Mi történik akkor, ha vírust találtunk? Mi ekkor a teendő, és mit nem szabad tennünk? Van-e különbség aközött, hogy a vírusellenőrző program a kártevőt, a vírust a rendszerindítást végző merevlemezen, a memóriában vagy leveleink között fedezte fel? Mindezekre és a napi munkánk során felmerülő további, hasonlóan fontos kérdésekre keressük a választ ebben a könyvben.

Munkám során sokan segítettek és támogattak. Mindannyiuknak nagyon hálás vagyok.

Köszönet illeti édesanyámat, aki munkakörülményeim biztosítása mellett könyvem egyik fő kritikusa volt. Külön köszönet Markhot Attilának, aki emberileg és szakmailag is mindig a biztos hátteret jelenti számomra. Hálás vagyok Pesoldt Editnek, aki az ötletgazda és kritikusom is egyben. Továbbá köszönöm Fodor Péternek, Bahil Miklósnak és Kún Gergelynek, hogy a szakirodalom felkutatásában segítségemre voltak. Nélkülük ez a könyv nem készülhetett volna el.

A szerző

[1] Asimov, Isaac : *A Hold tragédiája.* Kozmosz Könyvek, 1979. ford.: Békés András.

I. A VÍRUSOK ÉS AZ ANTIVÍRUS-PROGRAMOK ÁTTEKINTÉSE

A könyv tematikailag két részre tagolódik. Az első részben a vírusokat és az antivírus-programokat tekintjük át. Megvizsgáljuk, hogy milyen esetekben kell vírusfertőzésre gyanakodnunk, a vírusokon kívül milyen digitális kártevők léteznek, hol keletkeznek a vírusok, és azt is, milyen „történelmi jelentőségű" kártevők érdemelnek említést. Ezt követően különféle szempontok – így a fertőzés módja, az operációs rendszer, a működési algoritmus, végül a károkozási képesség – szerint csoportosítjuk a vírusokat. A vírusok után a védelmi eszközöket kategorizáljuk: az antivírus-programokat soroljuk különféle szempontok szerint osztályokba. Az első rész végén áttekintjük, hogy milyen teendőink vannak a fertőzés észlelésekor.

Az első részt tehát egyfajta elméleti összefoglalónak szántuk, míg a második részben – ahol praktikus tanácsokat kaphatunk számítógépünk védelmével kapcsolatban – a gyakorlaté a főszerep.

1. BEVEZETÉS

„A vírusok azok vírusok!"
André Lwof[2]

Jelen fejezet az alapfogalmakat igyekszik tisztázni. Ehhez első lépésként megismerkedünk azokkal a jelenségekkel, amelyek arra utalhatnak, hogy a számítógépünkön valamilyen digitális kártevő garázdálkodik. Elkülönítjük a vírusokat, valamint a vírusrokon és vírusszerű programokat. Megismerkedünk azokkal, akik a vírusokat készítik, végül megvizsgáljuk a vírusok fejlődéstörténetét is.

1.1. Vírusra utaló jelenségek

Számítógépünk üzemeltetése során időnként furcsa, nem várt jelenségeket tapasztalhatunk. Ezek egy része a programok működésének eredménye, amikor valami olyan funkciót használunk, amelyet korábban nem ismertünk, esetleg a szoftverek nem megfelelő beállításának, paraméterezésének következtében lépnek fel. Más esetekben ezek a jelenségek programhibákra, esetleg vírusok jelenlétére utalhatnak. Melyek ezek a jelenségek?

- A korábban elegendő memória hirtelen kevéssé válik ahhoz, hogy a megszokott programjainkat lefuttassuk.
- A szabad lemezterület a vártnál gyorsabban fogy el.
- A korábban helyesen működő programjainkban látszólag ok és mindenféle ésszerű magyarázat nélkül programhibák lépnek fel, avagy egyes szoftverek működése lelassul, esetleg teljesen leáll.
- A képernyőn furcsa üzenetek, ábrák jelennek meg. A monitor nem a begépelt szöveget jeleníti meg.
- A számítógép időnként szokatlan hangeffektusokat produkál.
- Minden különösebb ok nélkül állományok és könyvtárak tűnnek el, vagy éppen ellenkezőleg, jelennek meg a lemezen. Megmagyarázhatatlan adatvesztések következnek be. Az állományok mérete rejtélyes módon megváltozik.
- Anélkül, hogy megnyomtuk volna a reset gombot, vagy erre bármi okot adtunk volna, a számítógép váratlan módon újraindul.

[2] André Lwof, Nobel-díjas francia biokémikus válasza a „mi is a vírus" kérdésre. Nagy Gábor: *Vírusvédelem a PC-n.* ComputerBooks, 1995.

- A vártnál nagyobb levélforgalmunk van.
- A háttérben futó vírusellenőrző program, avagy a rendszeresen, esetleg alkalmilag elindított víruskereső szoftver vírust jelez a lemezeken vagy a memóriában.

E jelenségek többségének észlelése önmagában nem egyértelmű bizonyíték a fertőzésre. Ugyanakkor, ha több tünet egyszerre is jelentkezik, akkor azok már nem a véletlen egybeesés következményei. Egyes esetekben csak közvetetten lehet vírusfertőzésre következtetni, ám a gyakorlottabbak azonnal észreveszik a nem várt „vendéget".

1.2. A digitális kártevők fajtái

Térjünk vissza az előszóban feltett kérdésre, nevezetesen hogy mi az a számítógépvírus? Azt mondhatjuk, hogy olyan, általában kisméretű program, amely más programokhoz valamilyen módon hozzákapcsolódva megsokszorozza önmagát. Önmagában életképtelen, csak megfelelő hardver- vagy szoftverkörnyezetben, más programokba beépülve működőképes. Készítője a vírust úgy alkotja meg, hogy jelenlétét lehetőleg ne vegyék addig észre, amíg a fertőzésre alkalmas alanyokat fel nem deríti és köztük kellően el nem terjed. A vírus egy beprogramozott jelre vagy adott feltételek teljesülésére vár, majd utána bizonyos mellékhatásokat produkál.

Ugyanakkor a fentebb összefoglalt jellemzők nem adják meg a számítógépvírus pontos definícióját. Ennek az a magyarázata, hogy nagyon keskeny az a határmezsgye, amely a vírusok és a vírusnak „látszó" programok között húzódik. Minden olyan tulajdonság, amely a vírusok sajátja – a szaporodás, a rejtőzködés és a károkozás képessége – megtalálható olyan programokban is, amelyek nem vírusok. Ugyanakkor vannak olyan vírusok is, amelyek a szaporodás képességét leszámítva egyetlen fenti jellemzővel sem rendelkeznek. Lássunk erre néhány példát!

Tekintsük az első feltételt, a szaporodás, a saját kód megsokszorozásának képességét! Saját kódját nemcsak a vírus képes másolni, elegendő, ha csupán napjaink telepítőprogramjaira gondolunk. Ugyanakkor ebben az esetben a szaporodási funkció nem teljesen automatikus, hanem a felhasználó tevőleges közreműködését, vagy legalábbis jóváhagyását igényli, és a legkevésbé sem rejtőzködve történik.

A másodikként említett kritérium a rejtőzködés volt. A lemeztitkosító, hozzáférést ellenőrző vagy akár a víruskereső programok is igyekeznek jelenlétüket leplezni, ám ezekben az esetekben a programok által ellátott feladatok követelik meg az ilyen rejtőzködést. Ezért e jellemzőt sem szabad túlértékelni.

A harmadik tulajdonság az adott feltételek teljesülésére való figyelés. Ez lehet például egy adott időpont vagy dátum elérése. De gondoljunk csak a Microsoft Office csomagban található Outlook program Naptár funkciójára, amely bizonyos beállítások esetén figyelmeztet bennünket a soron következő megbeszélésre vagy tennivalóinkra. (Természetesen az az állítás, hogy az Outlook program vírus lenne, egyáltalán nem állja meg a helyét.)

A negyedik kritérium a mellékhatások megléte. Tekintsük példának a Norton Disk Doctor régebbi változatait. Ha ezeket olyan lemezek esetén alkalmazzuk, amelyek hosszú fájlnevekkel rendelkező állományokat is tartalmaznak, akkor a program több

kárt tesz, mint amennyi hasznot hajt. Ha azonban az általunk észlelt mellékhatások semmilyen összefüggésben nincsenek a program eredeti feladatával, akkor joggal gyanakodhatunk vírusra. Ugyanakkor meg kell jegyeznünk, hogy a mellékhatások hiánya még nem zárja ki azt, hogy egy program vírus legyen.

Be kell tehát látnunk, hogy a feltett kérdésre nem adható tökéletes válasz – jelen pillanatban nem áll rendelkezésünkre olyan egzakt definíció, amely pontosan meghatározná a számítógépes vírus fogalmát.

Ha tehát a fenti meghatározást szó szerint vesszük, akkor nem tekinthetünk vírusnak néhány olyan speciális programtípust, amely a víruskritériumok közül egy vagy több pontnak nem tesz eleget. Ezáltal vírusszerű hatásaik ellenére szaporító rutin hiányában nem tekinthetők vírusnak a trójai falovak, a férgek, az időzített bombák, a memóriafaló vagy a tréfás programok. Vizsgáljuk meg ezeket sorban!

1.2.1. Trójai falovak

A trójai faló program (angol szakkifejezéssel trojan horse program) – a vírusok nagy részéhez hasonlóan – váratlan mellékhatásokat produkál. A közönséges vírusoktól abban különbözik, hogy nem tartalmaz önreprodukáló részeket.

Az internet szabványosításával foglalkozó szervezet, az IETF (Internet Engineering Task Force) az 1244-es sorszámú, Site Security Handbook[3] című ajánlásában a következőképpen írja le a trójai falovat: trójai lehet egy program, amely valami hasznosat vagy csak valami érdekeset tesz. Mindig valami váratlant tesz, például tudtunk nélkül jelszavakat lop, vagy állományokat másol. Másképpen fogalmazva a trójai faló egy meg nem engedett kódrész egy programon belül – azaz az eredeti program megváltoztatása. Különböző műveleteket hajt végre, amelyekről a fertőzött rendszer felhasználója mit sem tud.

1.2.2. Férgek

Az 1980-as években a programozók körében népszerűek voltak az olyan speciális életjáték-típusú programok, amelyek a saját kódjukat egymással versenyezve többszörözték meg. E programok kifejezetten romboló részeket nem tartalmaztak, csupán a memória vagy az erőforrások lefoglalásával okozhattak károkat. Ezekből a programokból fejlődtek ki az angol szakirodalomban wormnak nevezett kártevők. A wormok oly módon károsítanak, hogy addig másolják be magukat a fertőzött állományba, míg azok használhatatlanul hosszúvá válnak, vagy be nem telik a lemez.

[3] Holbrook, P.–Reynolds, J.: *Site Security Handbook.* IETF RFC 1244, 1991. július.

1.2.3. Időzített bombák

Előfordulhat, hogy valamelyik futtatandó programban rejtőzik valamilyen időzített bomba (angol szakkifejezéssel time bomb). Például a programozó „biztonsági rutint" építhet be a programjába, amely figyeli, hogy ő maga szerepel-e a cégtől eltávolítandók listájában, és ha igen, akkor az időzített bomba működésbe lépve kíméletlen pusztításba kezd. Az ilyen program azonban nem szaporodik, így nem tekinthető vírusnak.

1.2.4. Memóriafaló programok

Korábban a programozók szívesen foglalatoskodtak azzal, hogy memóriafaló programokat indítottak a számítógépeken, és e vetélkedés során az életképesebb program kiszorította a másikat a memóriából. Ezek a programok „csupán" a szabad memória mennyiségét csökkentik. Ugyanakkor ez nem lehet cél egy vírus esetén, amelyet készítője széles körben történő terjesztésre szán, hiszen ez egy gyorsan észlelhető meghibásodás, a vírus hamar „lebukik". Napjainkban pontosan azok a vírusok vannak előnyben, amelyek jól rejtőzködnek, észrevétlenül tevékenykednek.

1.2.5. Tréfás programok

Az emberi humor kimeríthetetlen. Minden bizonnyal találkoztunk már olyan tréfás programokkal, amelyek fejre állítják a képernyő képét, rezegtetik azt, vagy más, a vírusoknál tapasztalható jelenségeket okoznak, a vírusok mellékhatásai nélkül. Ezeket a programokat azért szükséges itt említenünk, mivel a romboló kódokat nem tartalmazó vírusokhoz hasonlóan ezek a tréfás programok is okozhatnak komoly hibákat, adatvesztéseket. Hiszen semmi másra nincs szükség, minthogy a számítógép a vírusjelenségekhez hasonló tüneteket produkáljon, és a halálra rémült felhasználó ijedtében esetleg meggondolatlanságot követ el, ezzel pedig nagyobb kárt okoz, mint akár a legpusztítóbb vírus.

1.3. Honnan jönnek a vírusok?

Az 1990-ben megjelent Víruslélektan című könyvben Buruzs Tamás a következőképpen határozza meg a számítógépvírust: *„A számítógépes vírus intelligencia, erkölcs és értelem nélkül. Intelligens, mert létrehozásához mély számítástechnikai ismeret szükséges. Erkölcstelen, mert alattomosan kihasználja a számítógépek sebezhetőségét. Értelmetlen, mert egy vírus terjedése, pusztítása mindössze öncélú erőfitogtatás... A vírusprogram valójában az élő anyag működését utánzó életképes modell. Olyan, mint a biológiai fegyver, mert miután kiengedték a laboratóriumból, még maga az alkotója is elveszíti az ellenőrzést felette."*[4]

Mivel a számítógépvírusok nem mások, mint programok, ezért nem a semmiből

[4] Farmosi István–Kis János–Szegedi Imre: *Víruslélektan*. Cédrus, 1990.

bukkannak elő, nem keletkezhetnek véletlenül, és nem szabadulhatnak el egy program sérülésekor. A vírusok tervszerű, tudatos fejlesztés eredményei. Ugyanakkor aki sikeres vírust tud írni, szaktudását ugyanúgy használhatja vírusvédelemre is – így lesz a rablóból pandúr. Lássuk, mely csoportosulások foglalkoznak vírusfejlesztéssel!

- **Egyetemi kutatólaboratóriumok:** az első vírusokat programozó matematikusok készítették, méghozzá kutatási célból. Be akarták bizonyítani, hogy lehetséges olyan intelligens programot készíteni, amely szaporodásra és mutációra képes. Napjainkban az egyetemi laboratóriumokban a vírusok terjedési, fertőzési mechanizmusait vizsgálják, szigorúan szabályozott keretek között. Ezért elhanyagolható annak valószínűsége, hogy egy új vírus egy egyetemi kutatólaboratóriumból kikerüljön.
- **Katonai kutatólaboratóriumok:** bár hivatalosan tagadják, és kézzelfogható bizonyítékunk sincs rá, mégis nagyon valószínű, hogy a katonai kutatólaboratóriumokban az ellenséges számítógépek tönkretételére szánt számítógépvírusok készülnek. Ezek a laboratóriumok rendkívül zártak, így ha onnan kiszabadul egy vírus, akkor biztosak lehetünk abban, hogy a kórokozót a készítők szándékosan engedték szabadon.
- **Elégedetlen programozók:** mivel napjainkra a cégek életében az informatikai részleg egyszerű szolgáltatóból kulcságazattá nőtte ki magát, így az itt dolgozó személyek felbecsülhetetlen értékű tudás birtokosaivá váltak. Ugyanakkor az ő pozíciójuk is pontosan annyira bizonytalan, mint bármely más dolgozóé. Ezért a programozók igyekeznek védeni kiemelt státuszukat, néhányan esetleg a felmondási idő alatt vírusírással és -telepítéssel próbálják megkeseríteni egykori munkaadójuk életét.
- **Felelőtlen programozók, szakképzetlen amatőrök:** sok programozó nemcsak eltávolítja a vírusokat, hanem kísérletekbe is kezd azokkal. Közben megfeledkeznek arról, hogy a vírus nem játékszer, és könnyen kiszabadulhat az ellenőrzésük alól. A vírust vagy a visszafejtett víruskódot gyakran továbbadják, ezzel megkezdődik az átiratok gyártása. Végeredményként könnyen előfordulhat, hogy magát a hóhért akasztják: az alappéldány készítője saját kreatúráját kapja vissza, de már olyan formában, hogy rá sem ismer, és hosszasan küzdhet a nem várt „vendég" eltávolításával. A szakképzetlen amatőrök néhány program átalakítása után szakembernek vélik magukat. Ugyanakkor nem képesek megteremteni azokat a feltételeket, amelyekkel a vírusok elszabadulását megakadályozhatják, esetleg meg is feledkeznek róla. A végeredmény: vírusmutánsok.

1.4. Crackerek, hackerek

A kereskedelmi forgalomban kapható programokat másolásvédelemmel látják el. Amíg van másolásvédelem, addig lesznek feltört programok is. E feltöréseket olyan személyek készítik, akik szemében az információ szabadsága minden másnál fontosabb. Ezeket a személyeket az angol szakirodalomban crackereknek nevezik. A crackerek célja nem a károkozás, „csupán" a korlátozások megszüntetése.

A másolásvédett programok mellett a számítógép-hálózatok, adatbázisok, zárt rendszerek is komoly kihívást jelentenek a programozók számára. Sokuk számára a

védett rendszerek feltörése, a gyenge pontok felderítése és a behatolásvédelmi intézkedések semlegesítése valamiféle sport. A védelmek ilyen feltörőit az angol szakirodalom hackereknek nevezi. A német nyelvű Hackerbibel[5] című kiadvány alapján a hackerek etikai kódexéből a következő pontok emelhetők ki:

- „A kommunikációs hálózatokat használd ki, derítsd fel! Szolgáltatást lopni nem bűn. De ne tedd tönkre ezeket a rendszereket, amelyek a te kényelmedet is szolgálják!
- A fizető adatbankokat ingyenesen nyisd meg magad és a mások számára! Információt lophatsz, de azokat a rendszerben módosítani és törölni tilos!
- Ha egy érzékeny rendszerbe sikerült bejutnod, ... a rendszerben elhelyezett információval hívd fel a gazdák figyelmét arra, hogy lyukas a védelmük."

Egy harmadik csoportról is kell beszélnünk. Sem a crackerek, sem a hackerek nem károkozási szándékkal tevékenykednek, így nekik köszönhetően a felhasználókat nem érheti adatvesztés. Azok, akik vírusokat telepítenek mások programjaiba, károkozási szándékkal tevékenykednek, ez pedig bűncselekmény. Aki szándékosan vírust telepít, vagy pedig telepítési szándékkal vírust fejleszt, bűnöző.

1.5. Vírustörténelem

Az 1960-as évek végén, az 1970-es évek elején bukkantak fel először a „nyulak". Ezek a programok az erőforrások lefoglalásával csökkentették a rendszer teljesítményét, de még nem voltak képesek továbbterjedni. Az első ilyen fertőzést a Pervading Animal nevű nyúl okozta, amely a futtatható állományok végéhez fűzte hozzá magát.

Az 1970-es évek első felében jelent meg a The Creeper nevet viselő kártevő, amely a számítógép-hálózatot felhasználva képes volt eljuttatni egy másolatot saját magáról egy távoli számítógépre. E kártevő megfékezésére fejlesztették ki a The Reeper programot, amely az első ismert antivírus volt.

Az 1980-as évek elején jelentek meg a trójai falovak. Fred Cohen, amerikai PhD-hallgató használta először (1983) a vírus fogalmát számítástechnikai vonatkozásban. Ekkor jelent meg az Apple II számítógépeket megfertőző Elk Cloner vírus is. 1986-ban bukkant fel az első IBM személyi számítógépekben kárt tevő vírus, a Brain, mely egyben az első lopakodó vírus is volt. Ettől a pillanattól kezdve a vírusok és az antivírusprogramok tábora robbanásszerűen bővül új tagokkal. Kis János és Szegedi Imre 1992-ben kiadott, Vírushatározó[6] című könyve már mintegy 220 oldalon keresztül sorolja fel az addig felfedezett vírusokat. A digitális kártevők szaporodása azóta sem állt meg, így az ellenük folytatott küzdelem is folyamatosan újabb erőfeszítéseket követel.

[5] *Die Hackerbibel I.* Werner Pieper Vlg., Löhrb. 1985.
[6] Kis János–Szegedi Imre: *Vírushatározó.* Cédrus, 1992.

2. A VÍRUSOK CSOPORTOSÍTÁSA, VÍRUSTÍPUSOK

Ismerd meg az ellenségedet!
(szólás)

A manapság ismert vírusok száma becslések szerint eléri a 70 ezret. Azért beszélhetünk csupán becslésekről, mivel gondot okoz annak megfogalmazása, hogy mi tekinthető önálló vírusnak és mi csupán kisebb variánsnak. Olvashatunk olyan meghatározást, amely alapján két vírust egy családba tartozónak – legfeljebb minor variánsnak – tekinthetünk, ha ezek azonos módszert alkalmazva ismerhetők fel és távolíthatók el a rendszerből. Ha a felismerés módja a két vírus esetén azonos, de az alkalmazandó eltávolítási módszer eltérő, akkor major variánsról beszélhetünk. Nem tekinthetjük külön változatnak vagy külön vírusnak azokat a kártevőket, amelyek két, egyébként azonos példányából az egyik egy adott típusú állományt fertőz meg, míg a másik egy más típusút.

A nagyszámú digitális kártevő könnyebb kezelhetősége érdekében a szakértők a vírusokat – az operációs rendszer, a működési algoritmus, a károkozási képesség és a fertőzés módja alapján – általában négy csoportba sorolják. Az osztályba sorolás nem kizárólagos, a csoportok nem különálló halmazokat alkotnak, lehetnek közös részeik, metszeteik is. Másképpen fogalmazva bizonyos vírusok egyszerre több csoportba is besorolhatók.

2.1. Csoportosítás a fertőzés módja alapján

A vírusok a fertőzés módja alapján rengeteg kategóriába sorolhatók. A könnyebb érthetőség és áttekinthetőség kedvéért ebből az alábbiakban öt főbb csoportot emelünk ki.

2.1.1. Bootvírusok

Ezek a kórokozók a rendszer bootszektorába vagy az úgynevezett Master Boot Recordba férkőznek be. Ezáltal a rendszer betöltésének normális folyamata a következőképpen módosul: fertőzés esetén a bootvírus a saját kódját helyezi annak a programkódnak a helyére, amely a rendszer indításakor kapja meg a vezérlést. A rendszer indítása után a vírus „rábírja" a rendszert, hogy az eredeti betöltőrutin helyett a vírus kódját olvassa be a memóriába, és átadja annak a vezérlést. Miután a vírus programkódjára kerül a vezérlés, a kártevő a következő dolgokat hajtja végre:

- Csökkenti a rendelkezésre álló memóriát.
- Bemásolja a saját kódját a felszabadított memóriaterületre.
- Rátelepszik a megszakításokra, ezt követően beolvassa az eredeti bootszektort is a memóriába, majd átadja annak a vezérlést.

A későbbiek során a bootvírus viselkedhet úgy, mint egy memóriarezidens fájlvírus: rátelepedhet a rendszerhívásokra, és minden lehetőséget kihasználhat a további fertőzésre. Léteznek olyan bootvírusok is, amelyek nem maradnak a memóriában: a számítógép indulásakor megfertőzik a merevlemezt, esetleg a floppymeghajtóban található lemezt, majd a vezérlést visszaadják az eredeti rendszerbetöltőnek, és tevékenységüket ezzel be is fejezik.

A bootvírusok tehát akkor fertőznek, ha a fertőzött lemezről indul a gép. Adatlemezeken is megtelepedhetnek, ahonnan rendszerint nem fertőznek, hiszen nem erről indítjuk a gépet, de egy véletlenül bekövetkező rendszer-újraindítás vagy áramszünet itt is sok nehézséget okozhat. Ezért az adatlemezeket is rendszeresen ellenőrizni kell!

Mivel a bootvírusok jelentős hányada a rendszer eredeti betöltőrutinjának adatait átmásolja, és felhasználja saját betöltőrutinjában, így az ilyen vírusok könnyedén törölhetők azáltal, hogy a bootszektorban és a Master Boot Recordban felülírjuk a rendszer betöltőrutinját. Ehhez mindössze egy „tiszta" rendszerlemezre van szükségünk, az operációs rendszerünknek adott megfelelő utasításokkal pedig felül kell írnunk a rendszer betöltőrutinját.

2.1.2. Fájlvírusok

A vírusok első nemzedékének tagjai a fájlvírusok. Ezek futtatható állományokat fertőznek meg, állományokról készítenek másolatot, avagy terjedésükhöz a különféle fájlrendszerekre jellemző adottságokat használják ki.

A fájlvírusok akkor fertőznek, ha fertőzött programot indítunk el. Kártékony tevékenységük két fő fázisból áll. Az első szakasz a szaporodás, amikor bemásolják önmagukat a programokba. Ez a folyamat a leggyakrabban megfelelő víruskereső és -irtó programokkal még megállítható. A második szakaszt valamilyen esemény bekövetkezte, például egy dátum vagy egy időpont elérése váltja ki. Ekkorra azonban az állományok súlyosan károsodtak, a pusztítás már sokkal nehezebben állítható helyre.

Az állományok megfertőzésének módját alapul véve a fájlvírusokat több csoportra oszthatjuk.

- **Paraziták:** minden olyan fájlvírus, amelynek terjedéséhez meg kell változtatni a gazdaállomány tartalmát (miközben a fájl részben vagy egészben még használható marad). A parazita lehet előrefurakodó (angol szakkifejezéssel prepending), ekkor a vírus a kódját a fájl elejére másolja, lehet hozzáfűző (appending), amikor a vírus a megfertőzött állomány végéhez csatolja magát, és lehet beszúró (inserting), amikor a fájl belsejébe másolja saját magát. A hozzáfűző vírusok által károsított állományok java része megfelelő antivírus-programok segítségével helyreállítható, mivel ezek a vírusok általában megőrzik a helyreállításhoz szükséges adatokat.

- **Felülíró vírusok:** a fertőzési módot tekintve talán ezek a legegyszerűbb vírusok. A kártevő a gazdaállományt egyszerűen felülírja saját kódjával, így elpusztítja annak tartalmát. Az ilyen módon megfertőzött programok és állományok nem állíthatók helyre, mivel azok többé nem működnek helyesen, és a vírus nem őrzi meg a felülírt részek adatait sem. Ilyenkor a legcélszerűbb megoldás a fertőzött fájlok letörlése és pótlása. A felülíró vírusok gyorsan felfedik magukat, mivel a rendszerbe kerülés után rövid időn belül mindent tönkretesznek.
- **Bizonytalan belépési pontú vírusok:** az ilyen módszereket alkalmazó kórokozók a saját kódjukra mutató vezérlésátadó utasítást elrejtik az eredeti fájl rutinjai közé. A vírus csak akkor lép működésbe, ha a vezérlés átadódik a gazdaállomány azon kódrészletének, amely a vírusra mutató ugróutasítást tartalmazza. Ily módon elképzelhető, hogy a kórokozó akár évekig is „lappanghat".
- **Társult vírusok:** angol szakkifejezéssel companion vírusnak nevezik. Ezek a kártevők nem változtatják meg a gazdaállományt, hanem arról másolatot készítenek. A futtatás során elsőként a vírussal fertőzött állomány indul el, majd meghívódik az eredeti fájl is.
- **Fájlférgek:** ezek a kártevők nem kapcsolódnak egyetlen futtatható állományhoz sem. Szaporodásuk során egyszerűen átmásolják magukat egy másik könyvtárba, és arra várakoznak, hogy egy felhasználó elindítsa a másolatok egyikét. A vírusok általában olyan nevet adnak a másolatnak, ami miatt a felhasználó elindítja azokat (például Install.exe).
- **Linkvírusok:** az ebbe a csoportba sorolt kórokozók nem változtatják meg a gazdaállomány fizikai összetevőit. Ha a felhasználó egy fertőzött állományt indít el, a vírus a fájlrendszer szükséges mezőinek módosításával éri el, hogy az operációs rendszer a vírus kódját futtassa le.

2.1.3. Makrovírusok

A makrovírusok körébe azok a makro nyelven megírt kártevők tartoznak, amelyek adatfeldolgozó rendszerekbe épülnek be. Tény, hogy leggyakrabban a Microsoft Office programcsomagjának állományait (elsősorban a Word- és Excel-fájlokat) fertőzik meg, de természetesen léteznek más programokat megtámadó kórokozók is.

A vezérlés akkor kerül a vírus kódjára, amikor egy fertőzött állományt megnyitnak, vagy bezárnak. Ekkor megfertőződik minden olyan fájl, amellyel a gazdaprogram bármilyen kapcsolatban állt. A vírus egészen addig fertőz, amíg a keretrendszer – például a szövegszerkesztő vagy a táblázatkezelő program – fut.

Mivel az Office-állományok szerkezete bonyolult, így a makrovírusok fájlokon belüli terjedésével kapcsolatban csak hozzávetőleges elképzelések vannak. Tovább nehezíti a vírusirtó programok készítőinek a helyzetét az a tény, hogy manapság már lehetőség van a makrók titkosítására is, így a kártevők akár titkosítva is szerepelhetnek a dokumentumokban.

Az Office állományait megtámadó makrovírusok nem csupán az asztali számítógépeken képesek terjedni. Ha a PC-n olyan program fut, amely teljes mértékben kompatibilis az Office valamely programjával (például a Microsoft Word for Macintosh), akkor a terjedésnek nincs semmi akadálya.

Az Office programcsomagot megfertőző makrovírusok zöme csak azzal a programverzióval kompatibilis, amelynek nyelve megegyezik a kártevő készítője által használt nyelvvel. Azaz egy magyar verzióra írt vírus nem biztos, hogy képes az angol programváltozat alatt is fertőzni. Ezt akár pozitív jellemzőnek is értékelhetjük, de nem szabad figyelmen kívül hagyni azt a tényt, hogy a vírus ennek ellenére aktív marad. Azaz, ha a hordozó állományt egy megfelelő programváltozatot futtató számítógépen nyitják meg, akkor a vírus továbbterjed.

A bevezetőben a vírusra utaló jelenségek között említettük az állomány méretének hirtelen megváltozását. Az Office-állományokkal – a benne szereplő redundáns adatblokkoknak köszönhetően – előfordulhat, hogy a fájl mérete például szöveg beszúrása után csökken, vagy éppen ellenkezőleg, növekszik, miután töröltünk valamit. Ez a makrovírus által történő fertőzés esetén is bekövetkezhet, így nehéz megjósolni, hogy az állomány méretének megváltozását mi okozta.

2.1.4. Hálózati vírusok

Az ebbe a csoportba sorolt kártevők a hálózati protokollokat, illetve a helyi és/vagy világméretű számítógép-hálózatokat kihasználva szaporodnak. Az ilyen vírusok működésének legfőbb jellemzője, hogy a hálózaton keresztül, külső beavatkozás nélkül képesek kódjukat egy távoli szerverre vagy munkaállomásra eljuttatni.

Fontos kiemelni, hogy nem minden, hálózaton keresztül terjedő vírust nevezhetünk hálózati vírusnak, mivel minden vírus képes a hálózaton keresztül fertőzni. Ahhoz, hogy a kórokozót hálózati vírusnak nevezzük, teljesülniük kell a következő feltételeknek: a kártevő a terjedéséhez a hálózati protokollokat használja fel, valamint ezt a folyamatot tudatosan, önállóan végzi.

Az internet széles körű elterjedése magával hozta az internetférgek egyre gyakoribb megjelenését is. Internetféregnek tekinthető például az elektronikus levelezésen keresztül terjedő vírus. A fertőzött levelek arról ismerhetők fel, hogy mindig tartalmaznak valamilyen csatolt állományt, amely a vírus kódját tartalmazza. Ha nem nyitjuk meg a mellékletet, akkor a vírus nem tud kárt okozni. (A gondot az okozhatja, ha a levelezőprogramunkban engedélyeztük a csatolt állományok automatikus futtatását. Ezt az opciót célszerű kikapcsolni!)

Az internetférgek általában önmaguknak egy – leggyakrabban változatlan – példányát küldik tovább, így a hordozó a terjedés során gyakorlatilag változatlan. Ez ugyan nem szokványos szaporodási mód, de ezt a hatást a felhasználó tudta nélkül fejtik ki. Az egyszerűbb változatok az aktiválódás után áttekintik a levelezőprogram címjegyzékét, majd az ott lévő minden címre egy e-mailhez csatolva elküldik önmagukat. Ennél kifinomultabb módszert alkalmaznak azok a vírusok, amelyek lecserélik az internetes kommunikációért felelős egyik meghajtóprogramot, majd helyére egy olyat állítanak be, amely az összes kimenő elektronikus levélhez hozzácsatolja a kártevőt.

Az internetférgek egyik nagy kárt okozó képviselője volt az 1999-ben megjelent Melissa nevű vírus, de ezek közé tartozott a 2000-ben felbukkant I love you és a SirCam is.

2.1.5. Polimorf, mutáló, öntitkosító vírusok

Sajnálatos módon léteznek olyan vírusok is, melyek képesek a kódjukat módosítani. Az ebbe a csoportba tartozó vírusok egy része minden fertőzéskor valamilyen titkosító algoritmust használva átkódolja saját programját, és az egymás után megfertőzött programokban csak a kibontást elindító néhány bájt marad azonos. Ezért ezeket a vírusokat nem vagy csak komoly nehézségek árán lehet – a statikus kóddal rendelkező kártevőknél megszokott – mintaillesztéssel felismerni. Szerencsére azonban több olyan módszer is létezik, amelyekkel ezeket a kártevőket nem csak észlelhetjük, de el is távolíthatjuk, sőt, a terjedést, a további fertőzést is megakadályozhatjuk.

2.2. Csoportosítás az operációs rendszerek alapján

Minden vírushoz, amely egy bizonyos állományt vagy hálózattípust fertőz meg, egy adott operációs rendszer (például a Windows különböző verziói, Unix stb.) kapcsolható. Tehát minden operációs rendszerhez hozzárendelhetők az annak állományait megfertőzni képes kártevők is.

Ha a makrovírusokat vizsgáljuk, akkor ezek nem kimondottan az operációs rendszer, hanem a tevékenységi környezet alapján sorolhatók osztályba. Ilyen módon beszélhetünk Word-, Excel- vagy például Access-vírusokról.

A bootvírusok leggyakrabban csupán egyetlen operációs rendszer állományaiban képesek kárt tenni, ilyen módon külön-külön sorolhatók csoportba.

2.3. Csoportosítás a működési algoritmus szerint

Mivel a működési algoritmus szempontjából nagyszámú víruscsoportot hozhatunk létre, ezért ezek közül emeljünk ki kettőt!

A memóriarezidens vírusok egyes részeiket a memóriában helyezik el. Ezek a részek bizonyos rendszerhívásokhoz (például írás az állományba) kapcsolódnak, és így találnak újabb áldozatot. A makrovírusok memóriarezidens vírusnak tekinthetők, hiszen mindaddig a memóriában maradnak, amíg az általuk megfertőzött gazdaprogram (például a Word) fut.

Különféle rejtőzködési és titkosítási technikák használatosak. A rejtőzködési technikák használata teszi lehetővé, hogy a vírusok részben vagy teljes egészében leplezzék jelenlétüket. A legkedveltebb rejtőzködési módszer például a fertőzött állományokra irányuló rendszerhívások figyelemmel kísérése. A titkosítás és a polimorfizmus segítségével a vírusok jelenlétének felfedezése válik nehézzé. Az úgynevezett polimorf vírusokat azért nehéz felismerni, mert nem tartalmaznak csak rájuk jellemző és a szaporodás folyamán állandó kódrészletet.

2.4. Csoportosítás a károkozási képesség szerint

A károkozási képesség szerint a vírusok az alábbi négy csoportba sorolhatók:

- **Szinte ártalmatlannak** nevezik a szakemberek azokat a vírusokat, amelyek terjedésük során csökkentik a szabad kapacitást (memóriamennyiséget vagy lemezterületet). Fontos hangsúlyozni, hogy ártalmatlan vírus nincsen! Még ha elsődleges romboló hatásuk nincs is, programokat tehetnek használhatatlanná. Helyet foglalnak a szabad memóriából, amely memóriaigényes alkalmazások futtatása esetén lehetetlenné teheti programok futtatását, vagy adatvesztéseket okozhat. Ha nem memóriarezidens vírusról van szó, akkor is foglalja a lemez szabad kapacitását. Ez önmagában nem biztos, hogy nagy veszteség, de Murphy törvénye alapján mindig pont az a néhány bájt hiányzik, amelyet épp a vírus foglal el.
- **Veszélytelennek** tekintik a szakemberek azokat a kártevőket, amelyek – a szabad lemezterület és memóriakapacitás csökkentésén túl – valamilyen grafika vagy hanghatás segítségével tudatják jelenlétüket. Ilyen módon ismételten károsodás éri a rendszert, mivel a gazdaprogram képernyőkimenete elromlik. A pánikba esett felhasználó például a gép kikapcsolásával adatok elvesztését okozhatja, így komolyabb kárt tehet, mint amire a vírus önmagában képes lett volna.
- **Veszélyesnek** minősülnek azok a vírusok, amelyek komolyan akadályozzák a számítógépet a feladatai végrehajtásában.
- **Fokozottan veszélyesnek** nevezik azokat a vírusokat, amelyekbe a készítők olyan rutinokat helyeznek el, amelyek alkalmasak arra, hogy adatvesztést, sérülést, a rendszer működéséhez szükséges alapvető információk törlését vagy hardverelemek mozgó alkatrészeinek meghibásodását idézzék elő.

3. ANTIVÍRUS-PROGRAMOK

„Még szerencse, hogy a gombokat a tudományos háttér ismeretének a hiányában is könnyű kezelni!"
Isaac Asimov: A Hajnal bolygó robotjai[7]

A vírusok elleni küzdelemben a leghatásosabb fegyvert az antivírus-programok jelentik. Ezek a szoftverek – típusuktól függően – képesek detektálni a vírusok jelenlétét, megakadályozni a vírusfertőzések kialakulását, a felfedezett kártevőket el tudják távolítani, vagy legalább arra alkalmasak, hogy a fertőzött állományokat elkülönítsék, karanténba zárják. Ugyanakkor le kell szögeznünk, hogy nem létezik olyan program, amely tökéletes védelmet nyújtana a digitális kártevőkkel szemben. Ennek oka az, hogy a víruspopuláció nem statikus, hanem dinamikus – azaz a vírusok alkotói mindig új és új célpontokat, támadási felületeket keresnek és találnak. (Dr. Fred Cohen matematikailag is bebizonyította, hogy nincsen tökéletes antivírus-program.) Szerencsére az antivírus-programok fejlesztői folyamatosan lépést tartanak a kártevők fejlődésével.

Ebben a fejezetben azt tekintjük át, hogy a vírus ellen védő programok milyen módszerekkel dolgozhatnak, milyen eszközöket használhatnak. A fejezet végén pedig megvizsgáljuk, hogy milyen jellemzőkkel kell(ene) rendelkeznie egy jó antivírus-programnak.

3.1. Víruskereső programok

A víruskereső szoftverek működésük közben az állományokban, a lemez szektoraiban, illetve a rendszer memóriájában kutatnak a keresőprogram számára ismert és ismeretlen vírusok után.

3.1.1. Vírusazonosító mintákat használó keresőprogramok

Ezek a szoftverek a keresés során vírusmintákat használnak. A vírusminta olyan kódsorozat, amely csak az adott vírusra jellemző. Ez a módszer a természetéből adódóan követő jellegű, azaz nem képes megelőzni a vírusfejlesztőket. A vírusmintákat használó programok hatékonyságát korlátozza, hogy a keresőprogramok, illetve az azokban található kódsorozatok tanulmányozásával a vírusok fejlesztői úgy módosíthatják saját kártevői-

[7] Asimov, Isaac : *A Hajnal bolygó robotjai.* Galaktika, 1992. ford.: Hajdu Gábor.

ket, hogy azok a víruskereső programok által már ismert kódrészleteket ne tartalmazzák. Ezeknek a programoknak további korlátja, hogy csak a már ismert vírusok detektálására képes, az ismeretlen vírusokkal azonban nem boldogul, azokat nem észleli.

A vírusmintát használó eljárások viszonylag elfogadható pontossággal jelzik és azonosítják a kártevőket. Előfordul azonban, hogy egy rosszul megválasztott vírusminta miatt a program „üldözési mániába" esik, szaknyelven megfogalmazva gyakorivá válnak a vakriasztások. Ez azt jelenti, hogy a víruskereső szoftver olyan objektumokban talál fertőzést, amelyben valójában nincs is vírus. Ez elsősorban akkor okoz problémát, ha többféle vírusvédelmet alkalmazunk egyszerre, mivel ez a vakriasztások sorozatához vezethet. Ez legegyszerűbben úgy akadályozható meg, ha áttérünk egy másik, hasonlóan hatékony, de vakriasztást nem produkáló antivírus-programra.

Létezik olyan vírustípus, amelynél a vírusminta alapján történő keresés eleve hatástalan. Ez a már korábban említett polimorf, mutáló, öntitkosító vírusok csoportja. Ezekre a kártevőkre az a jellemző, hogy nincs két egyforma víruspéldányuk, minden egyes fertőzés során más lesz a beépülő víruskód. Ekkor a szakemberek kénytelenek más módszerekhez folyamodni a kórokozó azonosítása érdekében. Az egyik módszer például az, ha egy algoritmus segítségével leírják a vírus által használt összes lehetséges kódszekvenciát, amelyek közül az egyik biztosan alkalmas lesz az éppen vizsgált fertőzés esetén használt víruskód azonosítására.

3.1.2. Heurisztikus keresést alkalmazó víruskereső programok

Nagyon sok program rendelkezik a heurisztikus keresés képességével. Ez a fogalom annyit jelent, hogy a program nem vírusminták segítségével keresi a vírusokat, hanem a programkódban található, a vírusfunkciókra jellemző utasítás-szekvenciákat vizsgálja át, és ezekről statisztikákat készít. A fertőzés tényének eldöntését a vírus előfordulásának valószínűségi tényezőire alapozzák. Azaz, ha a program elegendő számú, a vírusfunkcióra jellemző utasítás-szekvenciát talál, akkor a vizsgált állományt fertőzöttnek nyilvánítja, míg ha csak kevés szokatlan jelet ismer fel, akkor a fájlt gyanúsnak minősíti.

A vírusok terjedésében és pusztításában nagy szerepet játszanak a nem dokumentált utasítások. Ugyanis számos hardvervezérlő, operációs rendszer és felhasználói program értelmez, illetve hajt végre olyan utasításokat, amelyek semmilyen hivatalos dokumentációban nem szerepelnek. A vírusok készítői azonban ismerik, és ki is használják ezeket a kiskapukat. A heurisztikus keresést alkalmazó víruskereső programok ezeknek a nem dokumentált utasításoknak a jelenlétét is vizsgálják. Ha ilyen utasításokra bukkannak egy állományban, akkor abban nagy valószínűséggel vírus található.

A heurisztikus keresést alkalmazó víruskereső programok komoly előnye a már említett, vírusazonosító mintákat használó keresőprogramokkal szemben, hogy nem vírusspecifikusak. Azaz nemcsak a már ismert és feltérképezett, hanem az ismeretlen vírusokat is képesek időben észlelni.

3.1.3. Általános, illetve specializált víruskereső programok

A víruskereső programokat a vizsgált célterület alapján két csoportra oszthatjuk: beszélhetünk általános célú, illetve specializált víruskeresőkről. Az általános célú keresőket arra tervezték, hogy megtalálják, illetve eltávolítsák az összes olyan kártevőt, amely például a víruskereső által védelmezni kívánt operációs rendszer alatt fertőzhet. A keresők másik csoportjába tartozó programok csak bizonyos számú vagy adott típusú vírus detektálására, illetve eltávolítására képesek. Például a makrovírusok felkutatására specializált programok kényelmes vírusvédelmi megoldást nyújtanak az irodai munkavégzés során, de más kártevők felismerésére nem alkalmasak.

3.1.4. Eseti vírusellenőrző és memóriarezidens programok

A tisztán szoftveres vírusellenőrzést a végrehajtás módját tekintve két fő csoportra oszthatjuk. Az első csoportba az eseti ellenőrzések sorolhatók. Ekkor a keresőprogramot a megfelelő módszerek segítségével elindítjuk, az az ellenőrzés elvégzése után kilép a memóriából, és visszaadja a vezérlést az operációs rendszernek. Szintén ebbe a csoportba sorolhatjuk azokat a programokat, amelyeket valamely időzítő indít el az előre beállított időpontokban.

A másik csoportba a memóriarezidens programok segítségével megvalósított, háttérben futó vírusellenőrzők sorolhatók. Ezek a szoftverek az elindításuk után – általában egészen a számítógép kikapcsolásáig – folyamatosan ellenőrzik a rendszer különböző objektumait. A memóriarezidens vírusellenőrző programok kifejlesztése során fontos szempont volt, hogy a program saját céljaira minél kevesebbet foglaljon le a rendelkezésre álló memóriaterületből, és eközben a lehető legtöbb vírus jelenlétét észlelje. A kompromisszum eredménye, hogy az ilyen programok bár észlelik a vírus jelenlétét, általában nem képesek a kártevők teljes eltávolítására.

Fel kell hívnunk a figyelmet arra, hogy a memóriarezidens vírusellenőrző szoftverek néha problémát okozhatnak, például összeakadhatnak más memóriarezidens programokkal. Ugyanakkor védelmükben felhozható, hogy jobb vírusvédelmet biztosítanak, mint az eseti ellenőrző programok, mivel fertőzés esetén azonnal képesek a beavatkozásra, míg utóbbiak csak elindításuk után nyújtanak védelmet.

3.2. Változásdetektorok alkalmazása

A vírusazonosító mintákat használó keresőprogramok mellett a legrégebben alkalmazott módszer a változásdetektorok használata. Ezek nem vírusspecifikusak, azaz a változás tényét képesek észlelni, de arról már nem tudnak információt adni, hogy mi okozta a változást.

A módszer hatékonysága nem függ a programozó, és így az antivírus-program vírusismeretétől. Ez két előnyhöz is vezet: a szoftver nem igényel rendszeres frissítést, valamint ismeretlen vírusok jelenlétére is fel tudja hívni a figyelmet. Ugyanakkor az

önmagukba visszaíró vagy gyakran frissített állományok sorozatos vakriasztásokhoz vezethetnek, ami a módszer komoly hátulütője.

Meg kell jegyezni, hogy ha egy vírus bekerült a memóriába, a változásdetekción alapuló antivírus-programokat „lóvá tudja tenni": az ellenőrzéskor nem a valódi, hanem a fertőzés előtti állapotnak megfelelő értéket szolgáltatja.

3.3. Immunizálás

Az immunizáló programok működésük során vagy vírusok jelenlétére figyelmeztetnek, vagy egy víruscsoport rendszerbe jutásának megakadályozására törekszenek. Az első csoportba tartozó immunizálók – a fájlvírusokhoz hasonlóan – a megóvni kívánt állományok végéhez fűzik magukat, és az állomány minden indításakor módosítások után kutatnak a fájlban. Az ilyen programok komoly hátránya, hogy nem képesek felfedezni a rejtőzködő technikákat használó vírusokat.

A második csoportba tartozó immunizálók megpróbálják megakadályozni egy adott vírus vagy egy bizonyos víruscsoport bejutását a rendszerbe. Ezek a szoftverek az állományokat úgy módosítják, hogy a kártevők az állományokat fertőzöttnek vélik, így a víruskódot nem fűzik hozzájuk. A memóriarezidens vírusok elleni immunizálók azt a módszert alkalmazzák, hogy egy kis memóriarezidens programot indítanak el, és amikor a vírus terjedés közben megpróbál beférkőzni a memóriába, a rendszert már fertőzöttnek véli, ezért nem próbál szaporodni.

A módszer hátránya, hogy nem lehet az összes vírus által alkalmazott terjedési módszerre felkészülni, és ezekkel szemben ellenállóvá tenni az állományokat.

3.4. Ellenőrző összegek alkalmazása

Az immunizálás és a változásdetekció kombinációjából született meg az ellenőrző összeges védelem. Már kezdetben két irányzat alakult ki. Az egyik esetében az ellenőrző összegek magukba az ellenőrzött állományokba kerültek, míg a másik módszer használata esetén az adatok egy központi állományban tárolódtak el.

Az első megoldás egészen addig megfelelő volt, amíg meg nem jelentek az önellenőrző programok. Ezek futása lehetetlenné vált, amint a programkód megváltozott. Ezzel a módszerrel tehát nem védhetők, nem ellenőrizhetők a másolásvédett, saját épségüket megőrző, az önmagukba visszaíró, valamint a programkód mögött közvetlenül elhelyezkedő memóriaterületet használó programok.

A gyűjtőállományok alkalmazása nagyon hasznos, de méretük a lemezen tárolt állományok darabszámának megfelelően változik, így a keresés ezzel arányosan lelassul. A CRC ellenőrző programok (CRC – Cyclical Redundancy Checking, ciklikus redundancia-ellenőrzés) ellenőrző összegeket készítenek a merevlemez állományrendszerének aktuális tartalmáról, majd ezeket minden más szükséges adattal együtt elmentik az antivírus-program adatbázisába. A CRC ellenőrző programok minden futás alkalmával az adatbázis tartalmát összehasonlítják az újonnan képzett értékekkel. Elté-

rés esetén a szoftver tájékoztatja a felhasználót erről a tényről, és figyelmeztet, hogy ezt a változást vírusfertőzés is előidézhette.

A rejtőzködő vírusokat felderíteni képes CRC ellenőrző programok használatával elméletileg a vírusfertőzések 100%-a röviddel a rendszerbe kerülés után felderíthető. Ugyanakkor nagy hátrányuk ezeknek a szoftvereknek, hogy a kártevőt nem rögtön a rendszerbe bekerülésekor, hanem csak bizonyos idő elteltével képesek felfedezni. Ez azt jelenti, hogy a CRC ellenőrző programok nem képesek az újonnan érkezett programokban detektálni a vírust, mert az adatbázisuk nem tartalmazza az erre vonatkozó bejegyzéseket. Ez a késlekedés pedig elegendő lehet ahhoz, hogy a vírus ezalatt az egész számítógépet megfertőzze.

3.5. Viselkedésgátlók

Annak érdekében, hogy a vírusvédelem az ismeretlen vírusokra is kiterjeszthető legyen, a fejlesztők számba vették azokat a műveleteket, amelyek csak a vírusokban fordulhatnak elő. Ha ezeket sikerül blokkolniuk, akkor a vírusvédelem biztosítható.

A viselkedésgátlók tehát olyan antivírus-programok, amelyek a rendszerben végbemenő eseményeket figyelik, és azokat elemezve figyelmeztetnek vírusok jelenlétére. (Vírus jelenlétére utalhat például a futtatható állományok módosítására irányuló rendszerhívás vagy minden olyan művelet, amely a vírusok terjedését lehetővé teszi.)

A viselkedésgátlókat gyakran a BIOS-ban tárolják (lásd az 5.1.1. alfejezetet), hogy hatásukat a rendszer indításának pillanatától kezdve kifejthessék. Sajnos ezeket egy kis szakértelemmel könnyedén félre lehet vezetni, és eközben egy olyan egyszerű program használatával, mint például az FDISK, vakriasztást idézhetünk elő.

A viselkedésgátlók azzal az előnyös tulajdonsággal rendelkeznek, hogy képesek a fertőzés első szakaszában felfedezni a vírust, és meggátolni annak tevékenységét. Ezek a szoftverek a felhasználók körében mégsem örvendenek nagy népszerűségnek, aminek több oka van. Egyrészt ha olyan programot futtatunk, amely a védett lemezterületet közvetlenül kívánja használni, akkor a viselkedésgátló szinte minden lépés végrehajtásához a felhasználó jóváhagyását kéri. Ez egy laikus számára, aki esetleg az üzenetek java részét nem is érti, felettébb zavaró lehet, és előbb-utóbb ki fogja kapcsolni a védelmet. A viselkedésgátlók további hátránya, hogy sok figyelmeztetésük tévesnek bizonyul, és igen népes az olyan módszerek tábora, melyekkel a védelmük kijátszható.

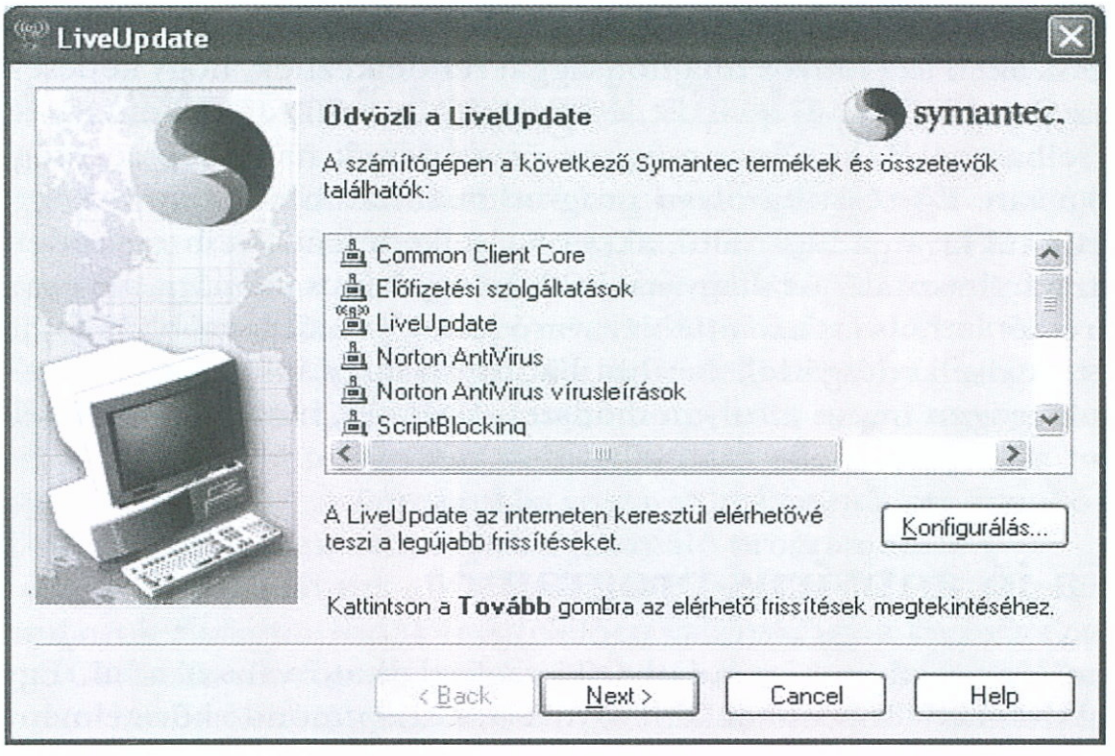
3.6. Milyen a jó antivírus-program?

A kérdésre nem lehet egyszerű, egy mondatban összefoglalható választ adni. Egy antivírus-programmal szemben több, esetenként egymásnak ellentmondó követelmény támasztható.

- **Legyen megbízható.** Ez alapvető kritérium, hiszen ha a program nem képes befejezni a vírusellenőrzést vagy -irtást (mert például működés közben lefagy), és marad

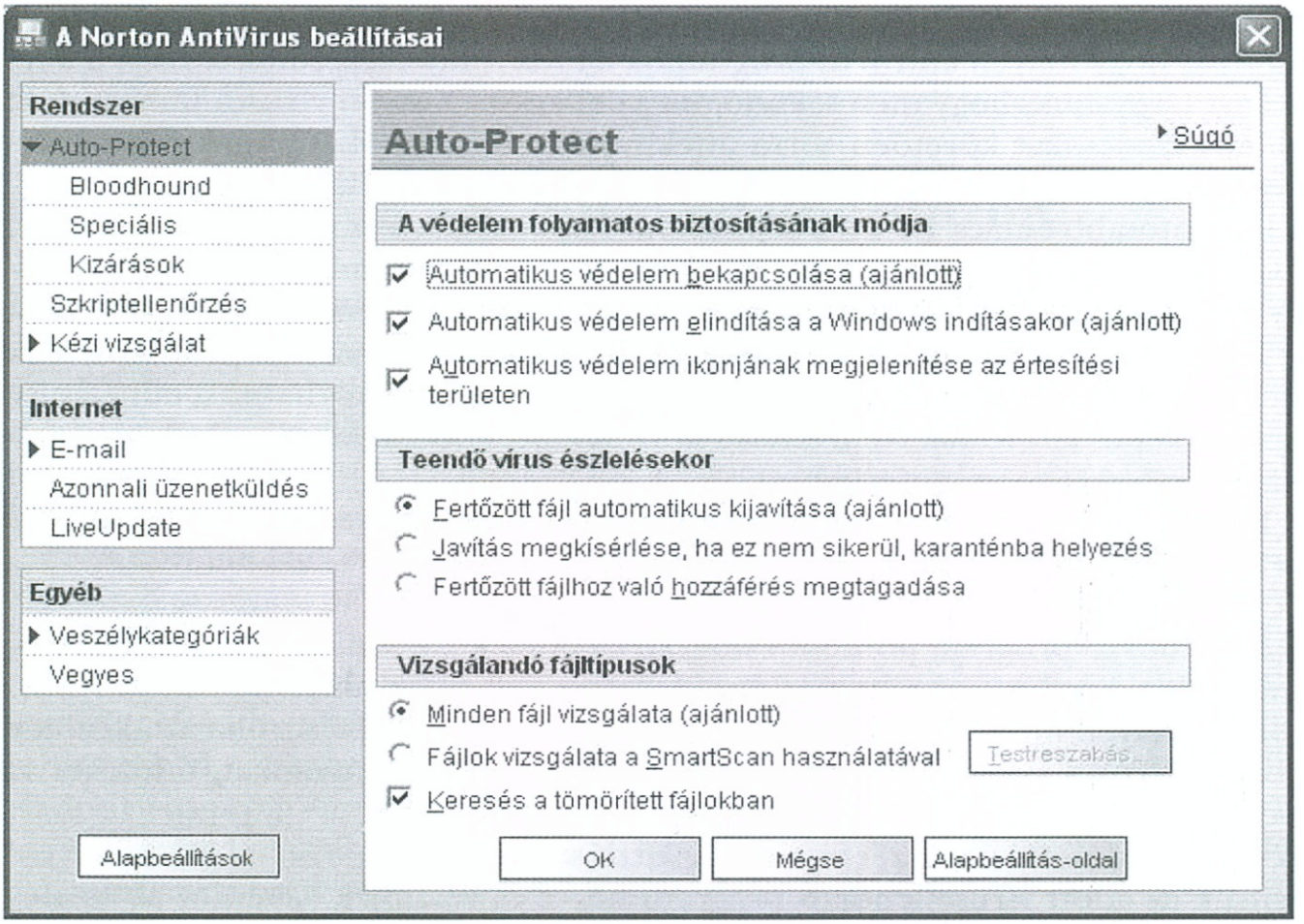
ellenőrizetlen terület, akkor a tökéletes vírusmintakészletet használó szoftver is legfeljebb arra jó, hogy segítségével a szabad tárterületet csökkentsük.

- **Legyen alkalmas minél többfajta kártevő azonosítására.** Alapvető elvárás, hogy képes legyen az előző fejezetben ismertetett főbb víruscsoportokba tartozó kártevők azonosítására. Ezt a felderítést mindenféle fájlban (futtatható és tömörített állományokban, dokumentumokban, az e-mailek mellékleteiben stb.) legyen képes elvégezni, és e tevékenység közben a vakriasztások száma a lehető legkevesebb legyen. Az egyes antivírus-programok minősítéséhez támpontot nyújt a segítségükkel felismerhető és eltávolítható kórokozók darabszáma, valamint ezek felsorolása. Ebben a listában a vírusszám növelése céljából sok olyan kártevő szerepelhet, amelyek a kutatólaboratóriumokból soha ki nem kerültek, vagy csak bizonyos helyeken, sok évvel ezelőtt bukkantak fel. Ezért ezt a felsorolást a megfelelő körültekintéssel tanácsos kezelni.
- **Legyen alkalmas a kártevő eltávolítására.** Elvárható, hogy a szoftver a megtalált kártevőt távolítsa el, állítsa helyre a fertőzött állományokat, vagy ha ez nem lehetséges, akkor legalább különítse el, helyezze karanténba azokat.
- **Álljon rendelkezésre rendszeres frissítés.** Ugyanis lényeges, hogy a vírusinformációs adatbázist minél gyakrabban frissítsük, továbbá a programhoz kiadott szoftverfrissítéseket is azonnal telepítsük, amint azokat megkapjuk. Az 1. ábra azt mutatja, amint éppen a Norton AntiVirus program frissítése töltődik le. Célszerű, ha a programhoz felhasználói támogatás, úgynevezett help desk szolgáltatás is a rendelkezésünkre áll. Ez bizalmi szolgáltatás, ezért fontos, ha az új vírusok felbukkanásakor nem csupán a soron következő frissítést kapjuk meg, hanem szaktanácsokkal is hozzásegítenek bennünket a program minél hatékonyabb felhasználásához.



1. ÁBRA • A Norton AntiVirus program frissítése

- **Legyen képes folyamatos ellenőrzésre.** Fontos, hogy a számítógép működése (pontosabban az antivírus-program futása) során állandóan figyelje a kórokozók tevékenységét, ezt ne csak felhasználói utasításra tegye meg.
- **Legyen elfogadható a futási sebesség.** Nem hagyhatjuk figyelmen kívül azt a szempontot sem, hogy a program működési sebessége elfogadható legyen. Ha a teljes rendszer átvizsgálásához több órára van szükség, akkor valószínűtlen, hogy a programot a felhasználók túl gyakran fogják elindítani.
- **Használata legyen kényelmes.** Nem elhanyagolható, hogy olyan felhasználók is képesek legyenek futtatni a programot, akik nem rendelkeznek megfelelő szakképesítéssel. Például a Norton AntiVirus program konfigurálása nagyon egyszerű – ezt szemlélteti a 2. ábra.



2. ÁBRA • A Norton AntiVirus konfigurálása

A vírusvédelem hatékonysága növelhető, ha vírusellenőrzés céljából nem csupán egyetlen programot alkalmazunk. Ezek megválasztása során fontos arra ügyelnünk, hogy például ne egyszerre kétféle memóriarezidens programot telepítsünk, hiszen ennek semmi értelme, és ezek működés közben „össze is akadhatnak". Ugyanakkor az időszakos és eseti ellenőrzések hatékonyságát növelhetjük, ha legalább két, különböző fejlesztőtől származó, eltérő vírusadatbázison alapuló rendszert működtetünk, egymás kiegészítéseképpen.

4. MIT TEGYÜNK, HA FERTŐZÉST ÉSZLELÜNK?

„Ne ess pánikba!"
Douglas Adams: Galaxis Útikalauz stopposoknak[8]

Az előző részekben megismerkedtünk a különféle digitális kártevőkkel, vírusokkal, és áttekintettük, hogy milyen antivírus-programok állnak rendelkezésünkre. Ebben a fejezetben azt tárgyaljuk, hogy mi a teendő, ha az ellenőrzés során vírusra bukkanunk. Az általános tanácsokat követően sorra áttekintjük a tennivalókat annak függvényében, hogy a vírusellenőrző program hol és milyenfajta kártevőt talált.

A legfontosabb tanács: **ne essünk pánikba!** Ha a hibát a számítógépünk kijelezte, ez azt bizonyítja, hogy még nem pusztult el teljesen a merevlemez. Ez biztató jel, hiszen így reménykedhetünk abban, hogy nem olyan súlyos a rendszer sérülése, amit még ne lehetne helyreállítani. De a pánik és a meggondolatlan javítási próbálkozások oda vezethetnek, hogy a jó szándékú igyekezetünkkel több kárt okozhatunk, mint amire maga a vírus képes lett volna. Nem szabad körültekintés nélkül kikapcsolni a számítógépet vagy újraformázni a merevlemezt!

A legelső tennivaló a rendszerparaméterek rögzítése. Jegyezzük fel a következő ismérveket:

- A vírusellenőrző program pontosan hogyan és hol jelezte a vírust (merevlemezen, memóriában, hordozható adattárolón, hálózati meghajtón stb.).
- A szoftver milyen néven azonosította a kártevőt, milyen típusba sorolta azt, közölt-e további, a vírusra vonatkozó adatokat, és esetleg adott-e tanácsokat, ötleteket az eltávolítással kapcsolatban.
- Írjuk fel az operációs rendszer típusát és verziószámát.
- Rögzítsük az adott vírusellenőrző program nevét és verzióját, valamint az esetleg alkalmazott további vírusvédelmi intézkedéseket (például rendelkezünk-e hardveres vírusvédelmi eszközökkel).

Ezekre az adatokra feltétlenül szükségünk lesz, ha a vírusmentesítés során szakértő segítségét kívánjuk igénybe venni. A szakember ugyanezeket az adatokat fogja bekérni. Ezért így egyrészt elébe megyünk a megválaszolandó kérdéseknek, másrészt ezeknek a jellemzőknek az összegyűjtése során mi magunk is megnyugszunk kissé, elkerülhető a pánikszerű kapkodás és az ily módon történő károkozás.

[8] Adams, Douglas: *Galaxis Útikalauz stopposoknak.* Gabo, 2003. ford.: Molnár István.

A veszély mértéke a fertőzés jellegétől, mértékétől, előrehaladottságától, kiterjedtségétől, valamint a fülön csípett kártevő típusától, jellemzőitől függ. A helyzet súlyosságát az is befolyásolja, hogy mi magunk mennyire értünk a vírusmentesítéshez, avagy – ha mi magunk nem boldogulunk a kártevő eltávolításával – kaphatunk-e segítséget közvetlen környezetünktől, munkatársainktól, esetleg az általunk alkalmazott vírusellenőrző szoftver forgalmazója nyújt-e támogatást a vírusmentesítés során.

A fertőzést vizsgálva a veszély következő fokozatait különböztethetjük meg:

- A kártevő csak az éppen ellenőrzött külső adathordozón (például floppylemezen) található, még nem került be sem a memóriába, sem a merevlemezre, és nem kapott még vezérlést.
- A merevlemezen található egyik állományban fedeztük fel a kártevőt, de az még nem került bele a memóriába, és nem kapott még vezérlést.
- A vírusellenőrző a memóriában fedezte fel a kártevőt.
- A hálózatba kapcsolt számítógépünkön az egyik hálózati meghajtó fertőződött meg.

4.1. Vírus van egy külső adathordozón!

Tekintsük azt az esetet, amikor a vírusellenőrző program vírus jelenlétére utaló jelet észlelt, például a floppymeghajtó ellenőrzésekor. Ez lehet egyértelmű vírusazonosítás, de akár megalapozatlan gyanú, vakriasztás is. Ha a vírusellenőrző program egyértelműen azonosította a kártevőt, akkor ne használjuk a fertőzött adathordozót, ne másoljunk onnan állományokat a merevlemezre, mert ezzel csak felesleges munkát okozunk saját magunknak!

A korábbi fejezetben ismertetett vírusbesorolás alapján azt mondhatjuk, hogy az ellenőrző program például egy floppylemezen bootvírusra és/vagy fájlvírusra bukkanhat. A fájlvírusok észlelésekor arra kell ügyelnünk, hogy a vírus ne vehesse át az uralmat a számítógépünk felett, azaz ne jusson vezérléshez. Ha ezt elértük – például a fertőzött dokumentumállományt nem nyitottuk ki, vagy a fertőzött programot nem indítottuk el –, akkor gondolhatunk a vírus eltávolítására és a károk helyreállítására. Az antivírus-programok java része lehetővé teszi a vírusok eltávolítását, de teljesen biztos eredményt csak akkor érhetünk el, ha a fertőzött és sérült állományokat letöröljük, valamint az érintett programokat újratelepítjük.

Ha a vírusellenőrző program „csak" bootvírust talált a külső adathordozón, akkor a floppyn található programok és adatállományok még biztonságosan elindíthatók, illetve átmásolhatók a merevlemezre. *Ezt természetesen csak akkor tehetjük meg, ha a vírusellenőrző nem talált fájlvírust a floppyn!* Ügyelnünk kell még arra is, hogy a fertőzött lemez bootterületén található víruskód ne kapja meg a vezérlést. Ezt elérhetjük annak megadásával, hogy a rendszer indításakor a betöltendő operációs rendszert először a merevlemezen kell keresni, és csak ezután lehet bármilyen más meghajtóhoz fordulni. Ezen túlmenően tanácsos ügyelni arra, hogy a gép újraindításakor (történjen ez bármilyen módon és okból) ne legyen lemez a külső adathordozó meghajtójában. A bootvírusok a külső adathordozóról annak megformázásával egyszerűen eltávolíthatók.

4.2. Vírus van a merevlemezen!

Ha az ellenőrzés során a merevlemezen találtunk vírust, akkor annak eltávolítása és az eredeti állapot helyreállítása komoly feladat, amelyhez egy sor speciális program áll rendelkezésre. Néhány vírusellenőrző nemcsak felismeri a kártevőt, de bizonyos kórokozókat képes el is távolítani. A programtól függ, hogy a fertőzés észlelésekor azonnal biztosít-e lehetőséget a vírus eltávolítására, vagy a felhasználónak külön el kell indítania egy megfelelő víruseltávolító célprogramot. Ha valaki ezt a feladatot valamilyen okból nem képes saját maga elvégezni, feltétlenül kérje szakember segítségét, ugyanis a merevlemez állományai között megbúvó víruskód előbb vagy utóbb biztosan vezérlést fog kapni, és működésbe lép. Ezt pedig mindenképpen meg kell előznünk!

4.3. Vírus van a memóriában!

Ha a vírusellenőrző program a számítógép memóriáját találta fertőzöttnek, ez a lehető legveszélyesebb és emiatt a legsürgősebb beavatkozást igénylő helyzet. A veszély abban rejlik, hogy a memóriában lapuló kórokozó a vírusellenőrző program közvetítésével megfertőzheti az összes vizsgált programot. Szerencsére a víruskereső szoftvereket felkészítik erre az esetre, amelyek bizonyos műveleteket végrehajtva meg tudják előzni a továbbfertőzést.

Egyes vírusellenőrző programok felkínálják azt a lehetőséget, hogy kitörlik a memóriából az ott megbúvó vírust. Lehetőségünk van elfogadni ezt az opciót, de a legbiztonságosabb az, ha – a fertőzést okozó vírus paramétereinek feljegyzése után – kikapcsoljuk a számítógépet, majd egy fertőzésmentes bootlemezről újraindítva a rendszert, onnan keressük meg, és számoljuk fel a fertőzést.

4.4. Vírus van a hálózaton!

Napjainkban a munkahelyeken a számítógépek jelentős része nem önmagában áll, nem „szóló gép", hanem hálózatba kapcsolt. Ilyen módon egyszerűbben hozzáférhetők mások munkái, a személyek közötti együttműködés könnyebbé válik. Ezzel együtt azonban a fertőzésveszély is megnő.

A hálózati meghajtókról történő víruseltávolítás több okból is a szokásosnál nagyobb szakértelmet és körültekintést igényel. Egyrészt ezekben az esetekben a vírus által a rendszerben közvetlenül vagy közvetetten okozott kár sokkal nagyobb lehet, mint egyetlen asztali gép esetén. Másrészt a számítógép-hálózatok hozzáférési hierarchiája – megfelelő gondossággal kialakított rendszerek esetében – olyan mértékben szabályozott, hogy a vírusirtást csak megfelelő jogosultság és szakértelem birtokában lehet elvégezni. Ezért, ha a víruskereső szoftverünk egy olyan állományban jelez vírust, amely egy hálózati meghajtón található (továbbá esetleg nincs is jogosultságunk e meghajtó állományait módosítani vagy törölni), akkor ne is próbálkozzunk a vírus eltávolításával! Jegyezzük fel, hogy melyik víruskereső programot használtuk, az hol és

milyen vírust talált, valamint célszerű azt is rögzíteni, hogy korábban mit dolgoztunk az adott hálózati meghajtón. Végül ezeket az információkat továbbítsuk a számítógép tulajdonosának vagy a rendszergazdának.

4.5. Vírus van a ... vagy nincs is vírus?!

Csak az nem követ el hibát, aki nem dolgozik – tartja a mondás. Hasonlóképpen igaz ez a vírusellenőrzésre is: ha nem vizsgáljuk kellő alapossággal és gyakorisággal a rendszerünket, akkor nem is kerülhetünk szembe vakriasztásokkal. Ugyanakkor nem szabad elfelednünk azt, hogy inkább célszerű – esetleg akár többször is – vállalni a vakriasztások kockázatát, semmint egyszer is megfertőződjön a számítógépünk.

Mi okozhat vakriasztásokat? Az ismertetett antivírus-programcsoportok definícióit felhasználva elmondhatjuk, hogy vírusazonosító mintákat használó keresőprogramok esetén téves riasztáshoz vezethet egy rosszul megválasztott minta. Ha az antivírusprogram heurisztikus keresést alkalmaz, akkor egy túlságosan érzékeny elemzés eredménye lehet a vakriasztás. Bizonyos esetekben téves figyelmeztetést okoz az is, ha egyszerre több, különböző fejlesztőktől származó vírusellenőrző programot használunk.

Nagyobb gyakorisággal adnak vakriasztást a vírusellenőrző programok az önellenőrző és másolásvédett szoftverek esetén, valamint azoknak a programoknak a vizsgálata során, amelyeknek kódjába a programozók a visszafejtést megnehezítő (angol szaknyelven anti-debug) kódot építettek. A téves riasztások számát gyarapíthatják a tömörítőprogramok is, mivel ezekben a legújabb, gyakran először éppen a vírusok esetén alkalmazott programozási módszereket használják.

A vakriasztások kiszűrésére adható néhány általános tanács. Téves riasztásra gyanakodhatunk, ha a vírusellenőrző program nem végrehajtható állományokban (például szöveges fájlban) véli felfedezni a kórokozót. Vakriasztásra utalhat az is, ha egy ismert vírust egy olyan állományban talál a keresőprogram, amelynek mérete kisebb, mint az adott kórokozó irodalmi hivatkozásokban megtalálható variánsainak mérete. Téves figyelmeztetésnek gondolhatjuk azt is, ha egy újonnan telepített vírusellenőrző program a nap mint nap használt programjainkat hiszi fertőzöttnek. Tovább erősíti a vakriasztás gyanúját az, ha az antivírus-szoftver csak ezt az egy programot véli fertőzöttnek, hiszen a vírusok alapvető célkitűzése a szaporodás.

4.6. Ki és hogyan irtson?

A fertőzés észlelésekor ki végezze, ki végezheti el a vírus eltávolítását? A kérdés nagyon fontos, hiszen a számítógépben meglapuló kórokozó előbb vagy utóbb komoly pusztítást tud végezni. Ezért a legbiztonságosabb megoldás az, ha a fertőtlenítést hozzáértő szakemberre bízzuk. Ez természetesen nem kevés költséggel jár, viszont ilyen módon megszabadulunk a hibás vírusirtás kockázatától. Ha mi magunk szeretnénk elvégezni a vírusok eltávolítását, fel kell készülnünk az esetleg felmerülő nehézségekre, kockázatokra és azok kiküszöbölésére.

Az első és legfontosabb szabály, hogy a vírusokat teljes mértékben el kell távolítani a számítógépről. Azaz a többszörös fertőzés esetén a kártevő felszámolása csak akkor mondható sikeresnek, ha minden vírust eltávolítottunk, az ismételt ellenőrzés során a programok vírusmentesnek bizonyulnak, és a programfunkciók is helyesen működnek. Fontos, hogy mielőtt a fertőzésmentesített programot ismételten elindítjuk, a vírusellenőrzést ismételjük meg! Ezt azért kell megtennünk, mert a víruseltávolító programok általában egy lépésben csak egyetlen vírust tudnak eltávolítani. Ha többszörös fertőzés fordult elő, akkor a program ismételt elindítása biztosan újrafertőzéshez vezet, hacsak a vírusellenőrzést a fertőzés eltávolítása után nem ismételjük meg.

A vírusok leggyakrabban a végrehajtható fájlokat támadják meg, ugyanakkor beépülhetnek egyéb állományokba és károsíthatják adatainkat is. Ha a vírus eltávolítása során csupán a víruskódot irtjuk ki, akkor nem lehetünk biztosak abban, hogy az érintett programok helyesen fognak működni. Ekkor a kártevő eltávolításával teljes mértékben nem értünk célt, mivel fontos adataink veszhettek el, válhattak használhatatlanná vagy elérhetetlenné. Tehát ha fertőzést észleltünk, önmagában nem elegendő a víruskód eltávolítása, érdemes a lehető legnagyobb érzékenységgel az elérhető összes állományban további fertőzések után kutatni.

Az összetettebb fertőzések eltávolítása nehéz feladat, mivel ha a fertőtlenítés során nem tudjuk sikeresen helyreállítani a károsodott programrészleteket, akkor végeredményként lesz egy vírusmentes, de hibás, nem működő programunk. Rosszabb esetben a program a vírus eltávolítását követően működőképes lesz, de a benne maradt sérülések a későbbi futtatások során komoly károsodásokat okozhatnak. Ezért nem tanácsos a vírusmentesített programokat ellenőrzés nélkül futtatni.

Az önmagunk által elvégzett vírusmentesítés további kockázata, ha „felülünk" egy vakriasztásnak, és a vírusirtó programmal egy teljesen tiszta állományból távolítunk el a működéshez elengedhetetlen részeket.

Végezetül ejtsünk néhány szót arról, hogy mit kell tennünk a memóriába bekerült vírusokkal. Ez nagyon komoly kockázati tényező: ha egy vírus, amelyet valamilyen okból nem észlelünk időben, bekerül a gép memóriájába, és rezidens módon bent is marad, akkor az nem csupán az elindított és futó programokat, de a megnyitott programállományokat is megfertőzheti. Ez a program pedig lehet akár maga a vírusmentesítő szoftver is! Ha tehát a víruskereső program elindításakor a memóriában vírus található, akkor jobb esetben az erre felkészült vírusellenőrző szoftver leblokkol. Sokkal rosszabb a helyzet, ha a programunk erre nincs felkészítve. Ekkor a vírusirtó program, amint víruseltávolítás céljából hozzányúl egy állományhoz, azonnal meg is fertőzi azt a memóriarezidens vírussal. Tehát a vírusmentesítés során mi magunk fertőzzük meg a rendszerünket. Ezért a vírusok eltávolításának alapszabálya: víruseltávolítást csak úgy szabad végezni, ha a rendszer memóriája garantáltan vírusmentes. A legkisebb gyanú esetén a rendszert egy vírusmentes rendszerlemezről kell újraindítani, és a vírusmentesítést innen kell elvégezni.

II. ÓVINTÉZKEDÉSEK – MIT TEGYÜNK, HOGY NE FERTŐZŐDJÜNK MEG?

A vírusokkal szemben nagy biztonságot nyújtó védelmet csak a teljesen zárt rendszerektől várhatunk el, ahol a bemenő adatokat mi magunk visszük be a billentyűzetről, és a kimenet a monitoron vagy a nyomtatón jelenik meg. Semmilyen más esetben nem zárhatjuk ki teljesen a fertőzés lehetőségét, ezért meg kell ismernünk azokat a megelőző intézkedéseket, amelyekkel csökkenthetjük a megfertőződés kockázatát és a keletkező kár mértékét. Tekintsük át azokat az óvintézkedéseket, amelyek betartásával a veszély mérsékelhető!

- Legalább a fontos, kritikus adatokról és programokról tároljunk biztonsági másolatot. Természetesen az a legmegfelelőbb, ha időnként a számítógép teljes (vírusmentes!) tartalmát külső adathordozóra mentjük.
- Alakítsunk ki olyan munkakörnyezetet, amelyben a kártevők gyorsan felismerhetők. Dolgozzuk ki azt a munkafolyamatot, amelyet a vírus felismerésekor végre kell hajtanunk. Legyünk tisztában azzal, hogy miként kell a vírust eltávolítani, valamint hogyan lehet „életre kelteni" a megfertőződött rendszert.
- Bizonyos időközönként ellenőrizzük a teljes rendszert, így megállapíthatók annak gyenge pontjai és felfedezhetők az esetlegesen bejutott vírusok.
- Ügyeljünk a hálózati kommunikációra, ideértve az elektronikus levelezést, böngészést és csevegést is. Vizsgáljuk meg a leveleink mellékletét, ne nyissuk meg azonnal azokat, és különösen ügyeljünk az üzenetekhez csatolt futtatható állományokra.

Ha cégünk számítógépeit kívánjuk megóvni a kártevőktől, az alábbi intézkedések követésével csökkenthetjük a fertőzés kockázatát.

- A biztonságtechnikai oktatás legyen a számítógépes munka alapfeltétele.
- Hozzunk létre olyan szakértői csoportot, amelynek tagjai a vírusokkal összefüggésben álló problémákat kezelni tudják. (Ez lehet a vállalat vagy vállalkozás egy szervezetileg is különálló egysége, de ennek a feladatnak az ellátásával megbízhatunk egy külső céget is.)
- Bizonyosodjunk meg afelől, hogy minden egyes munkatársunk tisztában van a tennivalókkal, ha vírusfertőzés gyanúja merül fel. Veszély esetére dolgozzunk ki munkatervet.

A könyv hátralevő részében azokat a pontokat tekintjük át, amelyeken keresztül a számítógépünk megtámadható. Ezt követően megvizsgáljuk, hogy milyen védelmi intézkedések segítségével tudjuk ezeket a támadási pontokat lezárni.

5. AZ OPERÁCIÓS RENDSZER VÉDELME

„Futura praevia minoris sunt timoris, com praesentia fuerint."
Gregorius[9]

A számítógép védelmének a bekapcsolással kell elkezdődnie, mivel az operációs rendszer az indításkor még nem készült fel a kártevők támadására. Fontos, hogy ebben a szakaszban is körültekintően viselkedjünk. Ebben a fejezetben azt vizsgáljuk meg, miként kell az operációs rendszerünket megvédeni, melyek a rendszer kritikus pontjai, és hogyan lehet rendszerünket megfelelően karbantartani. A továbbiakban – elterjedtségükből kifolyólag – kizárólag Windows-rendszerekkel foglalkozunk.

5.1. A rendszer indítása

5.1.1. A BIOS

A számítógép bekapcsolásakor elsőként a BIOS töltődik be. A BIOS (Basic Input/Output System – alap be- és kiviteli rendszer) az alaplapba égetett program, amely megadja a rendszer indításával kapcsolatos beállításokat. A BIOS rendszerállományok után kutatva, előre megadott sorrendben átvizsgálja a számítógép meghajtóit. Ha ezt a sorrendet úgy adtuk meg, hogy először a floppymeghajtón, majd a merevlemezen keressen rendszerállományokat, akkor bármilyen hiba esetén egy rendszerfájlokat tartalmazó indítólemezről a Windows mindig működésre bírható. (A Windows telepítésekor a Varázsló már felkínálta az indítólemez elkészítését. Ha ekkor igent mondtunk, nincs okunk az aggodalomra. Ellenkező esetben tanácsoljuk, hogy minél hamarabb készítsük el ezt a lemezt!) Ennek a megoldásnak az a hátránya, hogy ha véletlenül egy bootvírussal fertőzött floppylemezt hagyunk a meghajtóban, és a rendszert bekapcsoljuk vagy újraindítjuk, akkor a kórokozó megfertőzi a számítógépünket.

Ha a bootolási sorrendet fordítva adtuk meg, azaz először a merevlemezt kell megvizsgálni, majd csak ezt követően kell a floppy- (esetleg CD-) meghajtóhoz fordulni, akkor ezt a fajta támadási lehetőséget kizártuk. Ugyanakkor, ha bármilyen rendszerindítási hiba merül fel, akkor a gépet floppylemezről (CD-ről) kellene újraindíta-

[9] „A jövő, míg be nem következik, kevésbé ijesztő, mint amikor már jelenné lett." *Latin mondások 2.* Lazi Bt., 2003. ford.: Nagyillés János.

nunk, de a BIOS a merevlemezen kutat, a rendszer pedig nem indul el. Ezért fontos, hogy a különböző kockázati tényezők megfelelő mérlegelése után döntsük el a bootolási sorrendet, és szükség esetén a BIOS-ban változtassuk azt meg.

5.1.2. A BIOS jelszavas védelme

Ezt követően vizsgáljuk meg, hogy a rendszerindítás szakaszában miként nehezíthetjük meg az illetéktelen behatolók dolgát! A fentieket áttekintve leszögezhetjük, hogy a BIOS betöltése létfontosságú, enélkül el sem indul a rendszer. A számítógépek védelmének egyik módja a BIOS-jelszó beállítása, amelyet a felhasználónak a számítógép minden indításakor, a grafikus felhasználói felület megjelenése előtt be kell írnia. Jelszó hiányában a gép el sem indul.

De mi történik, ha elfelejtettük a BIOS-hoz rendelt jelszót? Ha nem kívánunk elmélyülni a számítógép „lelki világának" elemzésében, akkor az a legcélszerűbb, ha szakemberhez fordulunk, vagy visszavisszük a gépet ahhoz, akitől vásároltuk. Bizonyos számítógépeknél lehetőség van arra, hogy egy kapcsoló segítségével visszatöltsük a BIOS alapbeállításait, avagy hozzáférjünk a jelszóhoz. Az, hogy a mi gépünknél ezt megtehetjük-e, a számítógéphez mellékelt kézikönyvből deríthető ki.

A fenti kérdést másképpen is megfogalmazhatjuk: megtámadható-e a BIOS-jelszóval védett rendszer? Sajnos azt kell mondanunk, hogy minél öregebb egy számítógép, és vele együtt a BIOS, annál könnyebb kikerülni, illetve feltörni ezt a védelmet. Ennek a feltörésnek háromféle módja különböztethető meg:

- **Általános jelszó használata:** a különböző BIOS-verziók gyártói kiadnak egy általános vagy alapértelmezett jelszót arra az esetre, ha a felhasználó elfelejtené a jelszavát. Ezen alapértelmezett jelszavakkal a számítógépet az utoljára használt és mentett jelszótól függetlenül el lehet indítani. Ezeket a jelszavakat az internet számos oldaláról le lehet tölteni, és mi magunk is alkalmazhatjuk ezt a módszert, ha elfelejtettük jelszavunkat.
- **Jelszó megszerzése a memóriából:** ez feltételezi, hogy a rendszer már valamilyen módon elindult. Ekkor az egyes BIOS-verziókhoz tartozó különböző, a világhálóról letölthető segédprogramok alkalmazásával elérhető a memóriában tárolt jelszó.
- **A CMOS** (Complementary Metal-Oxide Semiconductor – kiegészítő fémoxid félvezető) **törlése:** szintén a rendszer elindulása után lehetőség van a BIOS, és vele együtt a jelszó törlésére is. Ehhez szintén speciális segédprogram áll rendelkezésünkre, amely a BIOS-szal együtt az összes rendszerbeállítást is letörli.

5.2. A rendszer kritikus pontjai, rendszerfájlok

A tájékozottabb internetfelhasználók néha azt gondolják, hogy a rendszert csak a világhálóról érhetik támadások, és ez ellen egy megfelelő módon beállított tűzfallal teljes mértékben meg is védhetik számítógépüket. De mi történik akkor, ha valaki az ebédszünetben fizikailag is hozzáfér gépünkhöz? Hogyan védekezzünk ebben az eset-

ben? Mi a teendő akkor, ha bizonyos korlátozásokkal másoknak is engedélyezni szeretnénk rendszerünk használatát?

- **Rejtsük el a rendszerindító menüt!** Ezt a menüt bizonyos típusú Windows-rendszerek (például Windows 98) esetén lehet elérni olyan módon, hogy a gép bekapcsolása után, a memória-ellenőrzéskor lenyomjuk az F8 billentyűt. Ha a menüt el szeretnénk rejteni, akkor az Msdos.sys állományban, az [Options] szövegrészbe írjuk be a BootKeys=0 parancsot. (Ne felejtsük el, hogy az Msdos.sys írásvédett fájl! Az írás megkezdése előtt ezt a beállítást törölnünk kell.) Így a rendszerindító menühöz senki nem férhet hozzá egészen addig, amíg ezt a sort ki nem töröljük.
- **Rejtsük el a rendszerállományokat!** Mivel ezek nélkül a számítógép nem működőképes, ezért a legcélszerűbb, ha elrejtjük ezeket, nehogy más felhasználók módosíthassák azokat. Ezt a Sajátgépből vagy az Intézőből tudjuk megoldani.
- **Készítsünk biztonsági másolatot a legfontosabb rendszerállományokról!** Javasolt, hogy a Config.sys, Msdos.sys, Autoexec.bat, Io.sys, Winboot.sys, Progman.ini, Win.ini, Protocol.ini és System.ini állományokat másoljuk floppylemezre, így a rendszer összeomlása vagy más katasztrófa esetén sincs minden elveszve.
- **Nyomtassuk ki a rendszer beállításait!** Ha valamilyen okból újra kell telepítenünk az operációs rendszert, a legnagyobb nehézséget a különböző eszközök ismételt beállítása okozza. Ezért érdemes kinyomtatni a rendszer adatait. Mivel ez nem túl gyakran használt feladat, ismertetjük a végrehajtását: a Sajátgép Tulajdonságok pontján belül válasszuk az Eszközkezelő fület. Ezen a lapon belül kattintsunk a Nyomtatás gombra, és a Jelentés típusa kereten belül jelöljük meg a Minden eszköz és a rendszer áttekintése rádiógombot.
- **Megfelelő időközönként ellenőrizzük a rendszerállományokat!** Windows 98 esetén erre a Rendszereszközök Rendszerinformáció pontján belül, az eszközök menü Rendszerfájl-ellenőrző pontjának kiválasztásával nyílik lehetőségünk. Ha a Megváltozott fájlokat keresni lehetőséget választjuk, akkor egy párbeszédablak jelenik meg, amelynek a különböző lapjain végezhetjük el a kívánt beállításokat.

5.3. A rendszer karbantartása

Merevlemezes meghajtóinkon hatalmas mennyiségű adat található. A lemez kapacitásának bizonyos részét elhasználják a fájlrendszer struktúráját tároló táblázatok. Ha ezeknek az információknak csak egy része is megsérül, akkor elveszhet a merevlemezen tárolt összes adatunk, holott maguk a tárolt anyagok nem sérültek, csupán nem tudunk hozzájuk férni. Ezért tanácsos az összes merevlemezes meghajtón rendszeresen ellenőrizni a fájlrendszer szerkezetének épségét.

Más probléma merül fel akkor, ha gyakran törlünk és hozunk létre új állományokat a meghajtónkon. Ugyanis ekkor az állományok beolvasása egyre több időt vesz igénybe, és egy bizonyos szint felett a rendszerünk érzékelhetően lelassul.

Ezeket a nehézségeket rendszeres karbantartással lehet kezelni. Ebben a részben a későbbiekben lesz erről szó.

5.3.1. Lemezellenőrzés

Windows XP-rendszerek esetén a ChkDsk (Check Disk, lemezellenőrzés), Windows 98 esetén a ScanDisk program képes diagnosztizálni és kijavítani a számos különféle eszközön, például a merevlemezen, a hajlékonylemezen vagy a cserélhető adathordozón felfedezett hibákat. Ezek a programok egyrészt ellenőrzik a lemezmeghajtók felszínének épségét, és lehetőség szerint megpróbálják visszanyerni a hibák miatt elvesztett adatokat, másrészt megvizsgálják az állományallokációs táblázatot (FAT – File Allocation Table, állománykiosztási táblázat), a könyvtárszerkezetet és a hosszú állományneveket, amelyek több fájlhoz vannak hozzárendelve.

Ha a Windows lefagy, vagy nem a Start menü Kikapcsolás gombjával állítottuk le, akkor a legközelebbi indításkor a ScanDisk általában lefut, hogy a váratlan leállás miatt előforduló esetleges hibákat ki lehessen javítani.

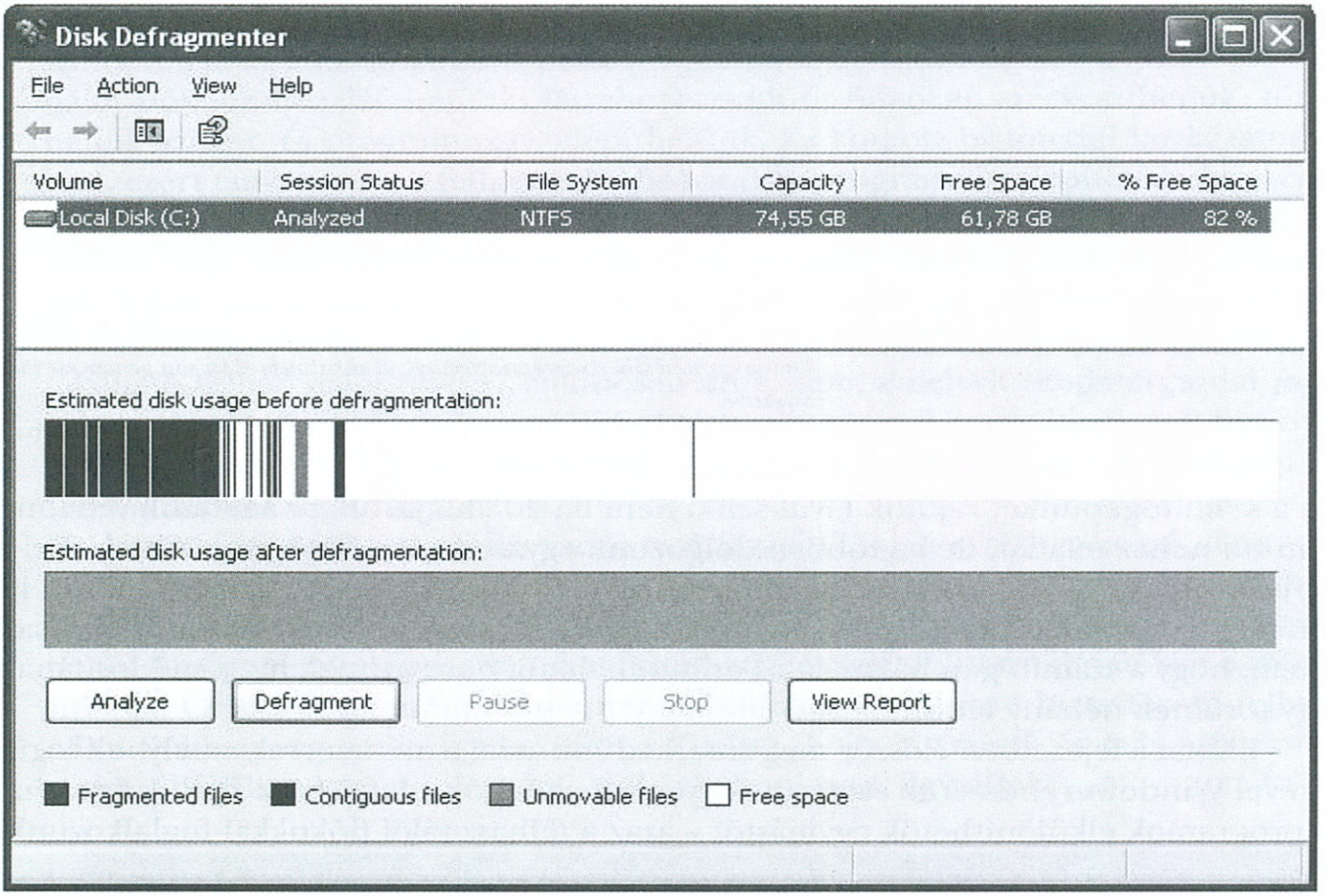
Bizonyos feladatok elvégzése – például a lemezhibák kijavítása vagy az elveszett szektorok visszaállítása – nem lehetséges a Windows futása közben, mert a javítások addig nem végezhetők el, amíg megnyitott állományok is vannak a rendszerben. Így, ha elindítjuk a ScanDisket, a Windows valószínűleg csak beütemezi a feladat végrehajtását, a program pedig csak a legközelebbi rendszerinduláskor fog lefutni.

5.3.2. Töredezettségmentesítés

A merevlemezen akkor léphet fel töredezettség, ha törlünk, majd elmentünk állományokat. Egy fájl törlésekor az operációs rendszer az addig elfoglalt szektorokat szabad területnek jelöli, így egy állomány elmentésekor azokat már használni is tudja. Ha a felszabadult helynél az új, elmentendő állomány nagyobb méretű, akkor annak egy része erre a helyre kerül, míg a maradék a lemez más szabad helyére mentődik el. Az állományok folyamatos törlése és írása miatt a meghajtó egyre töredezettebb lesz, azaz a tárolt fájlok a lemez több, nem összefüggő részén lesznek megtalálhatók.

Ha a töredezettség bizonyos mértéket meghalad, érzékelhetővé válik, hogy az állományok hozzáférési ideje megnő, a számítógép teljesítménye romlik. Minél kisebb részekre van szabdalva egy állomány, annál hosszabb időt vesz igénybe, míg az operációs rendszer hozzá tud férni.

Szerencsére rendelkezésünkre áll a Windows töredezettségmentesítő programja, amely az állományok szétdarabolt részeit egymást követő szektorokba rendezi. A program működését a 3. ábra mutatja. (Bár ez a program adatokat másol a merevlemez egyik helyéről a másikra, mégsem állományok és mappák mozognak, ezért ne gondoljuk azt, hogy ha például egyik mappánkat a másikba mozgatjuk, akkor annak fizikai elhelyezkedése megváltozik a meghajtón.) A töredezettségmentesítő program futtatását csak akkor kezdeményezzük, ha számítógépünket hosszabb ideig biztosan nem akarjuk használni, mivel a művelet végrehajtása akár néhány órát is igénybe vehet. Ha eközben megváltoztatunk egy állományt, akkor kezdhetjük elölről a folyamatot.



3. ÁBRA • Töredezettségmentesítés

6. ADATAINK VÉDELME

„Omne animal sibi commendatum est, et se salvum et in sou genere ese vult incolume."

Cicero[10]

Ha a számítógépünket rajtunk kívül senki nem használhatja, akkor adataink védelme nem túl nehéz feladat, de ha többen dolgozunk egyazon számítógépen, akkor a helyzet bonyolulttá válhat. Ez nemcsak a munkahelyen okozhat gondot, hanem otthon is, ahol a gép közelében mindig megtaláljuk a családtagjainkat. Nem lehetünk biztosak abban, hogy a számítógép használata során véletlenül nem nyitnak meg, módosítanak vagy törölnek néhány létfontosságú állományt.

Ebben a fejezetben először megismerkedünk azzal a módszerrel, amelynek segítségével Windows-rendszerek esetén az egyes felhasználók adatai és az általuk futtatható programok elkülöníthetők egymástól – azaz a felhasználói fiókokkal foglalkozunk. Majd részletesen megvizsgáljuk, miként dolgozhatunk „nyom nélkül" a számítógépen, és hogyan rejthetjük el mások elől bizalmas adatainkat. Végül pedig áttekintjük a biztonsági másolatok készítésének módjait.

6.1. Felhasználói fiókok

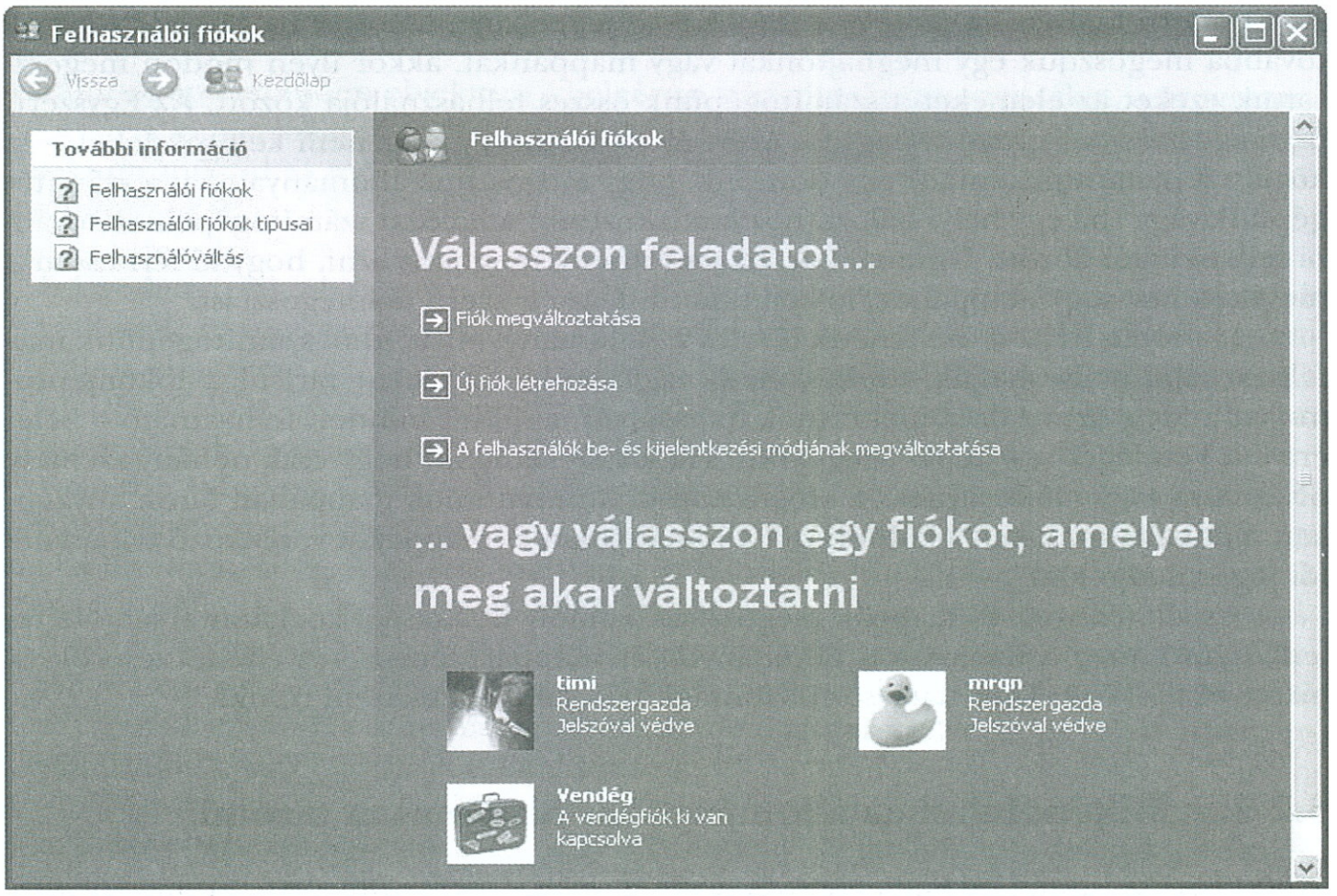
A Windows 95 vagy a Windows 98 szinte semmilyen beépített védelmi rendszert nem tartalmazott, azaz szinte semmilyen módon nem biztosította, hogy az egyik felhasználó ne olvashassa a másik állományait.

Amikor több felhasználó osztozik egyetlen számítógépen, a helyi felhasználói fiókok teszik lehetővé, hogy mindenki személyre szabhassa a felhasználói felületét, anélkül hogy másoknak ezzel kényelmetlenséget okozna. A felhasználói fiókok jelszóval védettek, így az egyes felhasználók nem léphetnek be más felhasználói fiókokba. A korábbi rendszerekkel szemben a Windows XP esetén már kötelező a felhasználói név és a jelszó megadása. Lehetőség van a gyors felhasználóváltásra is, így egyidejűleg több felhasználó is bejelentkezhet a rendszerbe, továbbá programokat is futtathat. Az Egyszerű fájlmegosztás megkönnyíti az állományokhoz és mappákhoz történő hozzáférés megosztását a számítógépet használó személyek között.

Tekintsük át, hogy milyen típusú felhasználói fiókok hozhatók létre, és ezekhez milyen jogosultsági szintek tartoznak!

[10] „Minden élőlény magára van utalva, célja saját épsége, s saját nemében való sérthetetlenségének biztosítása." *Latin mondások 2.* Lazi Bt., 2003. ford.: Nagyillés János.

- **Adminisztrátor:** legalább egy ilyen típusú felhasználói fióknak kell lennie a rendszerben. Ha az adminisztrátori fiókba vagyunk bejelentkezve, bármely más felhasználói fiókhoz hozzáférhetünk: létrehozhatunk új fiókokat, szerkeszthetjük, törölhetjük azokat, és programokat telepíthetünk. Ez komoly biztonsági kockázatot jelent, ezért tanácsos ezt a felhasználói fiókot csak programok telepítésére és a rendszer karbantartására használni. A veszélyt a vírusok tovább növelik: ha adminisztrátorként bejelentkezve fertőződik meg a számítógép, elképzelhető, hogy az összes más felhasználói fiók is fertőzött lesz. Tanácsos továbbá az adminisztrátori felhasználói fiók átnevezése, mivel a rendszer feltörése nehezebb, ha nem ismertek az ott található felhasználói fiókok, különösen azok nem, amelyek rendszergazdai jogosultságokkal bírnak! (A felhasználói fiókok beállításainak megváltoztatását bizonyos jellemzők esetén a Felhasználói fiókok ablakban, más elemeknél a Számítógép-kezelés ablakban végezhetjük el.)
- **Korlátozott hozzáférés:** a felhasználó csak a saját fiókjához férhet hozzá, nem telepíthet programokat, nem nyithatja meg a más felhasználók Dokumentumok mappájában található állományokat, valamint nem változtathatja meg a rendszer beállításait. A már telepített programokat futtathatja, és saját felhasználói fiókját is módosíthatja. Célszerű, ha a mindennapi munkánkat a korlátozott hozzáférésű felhasználói fiókban végezzük, így kevésbé valószínű, hogy a vírusok és más programok megpróbálják magukat telepíteni, miközben mi nem figyelünk.



4. ÁBRA • Felhasználói fiókok

- **Vendégfiók:** ekkor nem változtathatjuk meg a további felhasználói fiókokat, nem nyithatjuk meg a más felhasználók Dokumentumok mappájában található állományokat, valamint nem telepíthetünk programokat, csak a már telepített programokhoz van hozzáférésünk.

A felhasználói fiókok különféle típusainak egy lehetséges felhasználását szemlélteti a 4. ábra.

6.2. Bizalmas adatok kezelése

Miután áttekintettük, hogy milyen típusú felhasználói fiókok állnak rendelkezésünkre, valamint megtudtuk, hogy lehetőség van a számunkra megfelelő munkakörnyezet kialakítására, meg kell állapítanunk, hogy mindez nem elegendő, ha bizalmas adatainkat nem látjuk el megfelelő védelemmel. Hogyan óvjuk bizalmas adatainkat? Most erre keressük a választ.

6.2.1. Hogyan férhet hozzá más felhasználó a mi állományainkhoz?

Az Egyszerű fájlmegosztás a Windows XP új jellemzője, amelyet ha engedélyezünk, továbbá megosztjuk egy meghajtónkat vagy mappánkat, akkor ilyen módon megosztottuk ezeket az elemeket a számítógépünk összes felhasználója között. Az Egyszerű fájlmegosztás bekapcsolva hagyása azért előnyös, mert ekkor nem kell sok lehetőség közül választanunk, amikor úgy döntünk, hogy megosztjuk állományainkat a számítógépünk vagy (ha egy helyi hálózathoz csatlakozunk) a hálózat számítógépeinek további felhasználói között. Ugyanakkor, ha szeretnénk meghatározni, hogy ki férhessen a meghajtóhoz vagy mappához, le kell tiltanunk az egyszerű fájlmegosztást.

Ha olyan helyen szeretnénk tárolni az állományainkat, ahol számítógépünk más felhasználói is olvashatják, szerkeszthetik vagy törölhetik azokat, tartsuk a dokumentumokat a Megosztott dokumentumok mappában, amelyet minden felhasználó – beleértve a Vendéget is – képes megnyitni. Ha azt szeretnénk, hogy csak néhány személy olvashassa vagy módosíthassa a Megosztott dokumentumok mappában tárolt anyagokat, módosítanunk kell a különböző, állományokra és mappákra vonatkozó felhasználói jogosultságokat.

Az állományok és mappák megosztása komoly biztonsági kockázattal jár. Ne feledkezzünk meg a megosztott állományok és mappák rendszeres ellenőrzéséről, és bizonyos időközönként tanácsos biztonsági másolatot is készíteni róluk!

6.2.2. Miként lehet az állományokat bizalmasan tárolni?

A Windows korábbi változatai (Windows 95, Windows 98 és Millennium Edition) nem biztosítják, hogy a felhasználók bizalmasan kezelhessék adataikat. A Windows NT, Win-

dows 2000 és Windows XP Professional már képes ezt garantálni, ha teljesülnek a következő kritériumok:

- Az állományokat tároló lemezt NTFS fájlrendszerre formáztuk. (Ha a lemez NTFS helyett FAT32 formátumú, létrehozhatunk helyi felhasználói fiókokat és csoportokat, de az állományokat vagy mappákat nem tudjuk bizalmasan tárolni.)
- Az Egyszerű fájlmegosztás nem engedélyezett.

Minden felhasználói fiók rendelkezik a C:\Documents and Settings mappában található Dokumentumok könyvtárral, amelyben a felhasználó az állományokat tárolhatja. Amikor a felhasználói fiókhoz tartozó jelszót létrehozzuk, megadhatjuk, hogy a dokumentumainkat bizalmasan kívánjuk kezelni. Ekkor a Dokumentumok mappát csak mi magunk és a rendszergazda tekintheti meg, ellenkező esetben viszont bármely felhasználó megnyithatja.

Ha a fentebb ismertetett Egyszerű fájlmegosztás használatát letiltottuk számítógépünkről, a mappáink egy NTFS formátumú meghajtón vagy partíción tárolódnak, továbbá ha Windows XP Professionalt használunk, megtekinthetjük és beállíthatjuk, hogy kinek van jogosultsága állományainkat vagy mappáinkat megnyitni. Ezt az adott állományhoz vagy mappához tartozó Tulajdonságok párbeszédablakban tehetjük meg.

6.2.3. Írásvédett, rejtett és titkosított állományok

A számítógépen minden objektum – beleértve a hardverkomponenseket, a programokat és az állományokat is – tulajdonságokkal rendelkezik, amelyek meghatározzák az objektum működési módját. Tekintsük át az állományokra és mappákra vonatkozó attribútumokat!

- **Írásvédett** (csak olvasható): ennek az állománynak vagy mappának a tartalmát olvashatjuk és szerkeszthetjük, de a változtatásokat az eredeti állományba már nem tudjuk elmenteni, azt csak egy másik fájlba helyezhetjük el. Ha megpróbáljuk a csak olvasható állományt vagy mappát letörölni, a Windows figyelmeztet bennünket arra, hogy az csak olvasható, de ha ragaszkodunk hozzá, letörli.
- **Rejtett:** a Windows számos olyan állományt tartalmaz, amelyet nem lenne jó véletlenül letörölni vagy megváltoztatni. Ezek az állományok rejtettek, ami azt jelenti, hogy alapértelmezésben nem jelennek meg a Windows Intézőben, és nem nyithatjuk meg, törölhetjük vagy módosíthatjuk azokat, hacsak nem tesszük ezeket láthatóvá. A rejtett állományok és mappák az átlagos számítógép-felhasználó mindennapi életében nem játszanak jelentős szerepet. Ezért tanácsos, hogy ezeket az állományokat és mappákat hagyjuk rejtetten, így csökkenthető annak esélye, hogy véletlenül megváltoztatunk vagy letörlünk valami fontosat.

  Fontos, hogy a rejtett állományok vagy mappák nem tekinthetők biztonságosnak, mivel a Keresés parancs segítségével nemcsak megtalálhatók, de bárki, aki megtalálja azokat, közvetlenül meg is nyithatja a Keresés ablakból. Ezért ha mások is

használják a számítógépünket, célszerű titkosítani, majd a Dokumentumok könyvtárban tárolni az érintett állományokat.

- **Titkosított:** az állomány titkosított (kódolt), így azt a későbbiekben csak a létrehozója tudja megnyitni. A titkosítás opcióját csak NTFS partíción tárolt állományok és mappák esetén láthatjuk (és módosíthatjuk).

Mint ismeretes, a Vezérlőpult segítségével a Windows számos fontos beállításához hozzáférhetünk. Ha nem szeretnénk, hogy ezeket bárki módosíthassa, el kell rejtenünk a Vezérlőpultot is.

Léteznek olyan elemek, amelyekhez a felhasználók más módon is hozzáférhetnek, például az állományok jellemzőinek leírására szolgáló Tulajdonságok menüpont, így ezeket is célszerű elrejteni. Ehhez a Rendszerleíró adatbázis (Registry) tartalmát kell módosítanunk. (Fontos, hogy mielőtt belekezdenénk a módosításba, mindenképpen készítsünk róla biztonsági másolatot, mivel ez a rendszer egyik kritikus eleme!)

6.2.4. Hogyan tüntessük el nyomainkat?

A számítógéppel végzett munka során rengeteg nyomot hagyunk magunk után. Ezek segítségével más felhasználók gyorsan kideríthetik, hogy például mely fájlokat használtuk, vagy milyen mappákat hoztunk létre. Bizalmas adatok esetén ezeket a jeleket célszerű rendszeres időközönként eltüntetni mások elől.

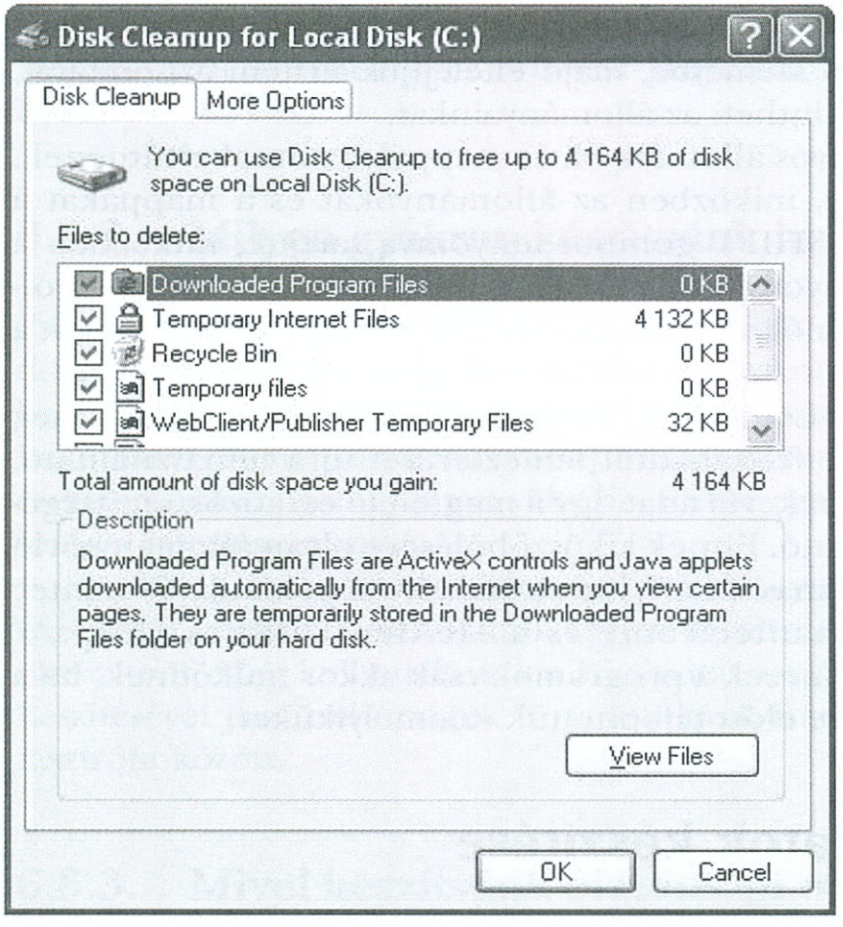
Ideiglenes állományok törlése

Ilyen árulkodó nyom lehet egy ideiglenes állomány, amelyet néhány program működése közben létrehoz, és a program használatának befejeződésekor nem töröl. Ha egy program váratlanul kilép (lefagy), akkor szintén megmaradhatnak az ideiglenes állományok a merevlemezen.

A Windows a legtöbb ideiglenes állományt a C:\Documents and Settings*felhasználónév*\Local Settings\Temp, illetve a C:\Windows\Temp mappában tárolja. Ezeknek az állományoknak az időről időre történő összegyűjtése és törlése felettébb hasznos, mivel azon túlmenően, hogy megmutatják, mivel dolgoztunk utoljára, feleslegesen foglalják a helyet a merevlemezen, továbbá jelenlétükkel zavarhatják az ezeket létrehozó programokat (különösen akkor, ha egy lefagyás után maradtak ott).

A Windows XP Lemezkarbantartó programjának segítségével törölhetjük a merevlemezen felgyülemlett felesleges ideiglenes állományokat (lásd 5. ábra). A Lemezkarbantartó használatával azonban bánjunk óvatosan, ugyanis esetenként törlésre jelöl olyan állományokat, amelyeket hónapok óta nem használtunk. Ezért mielőtt automatikusan töröltetjük vele az összegyűjtött állományokat, nézzük át a felsorolást!

A Lemezkarbantartó programot használhatjuk esetileg, de megadhatjuk a Windowsnak, hogy a programot rendszeres időközönként futtassa automatikusan. Utóbbi esetben először indítsuk el mi magunk is a programot, hogy beállíthassuk, mely típusú állományok törlődjenek.



5. ÁBRA • Lemezkarbantartó

Dokumentumok menü

A Start menü Dokumentumok (Windows XP esetén a Legutóbbi dokumentumok) pontja általában az utolsó 15 megnyitott, módosított és elmentett állomány nevét tartalmazza. Ezért ha nem szeretnénk, hogy más is megtekintse munkánkat, a bizalmas adatokat tartalmazó állományok nevét mindenképpen töröljük a menüből!

A Dokumentumok menü tartalmát többféleképpen is eltávolíthatjuk. Egyrészt törölhetjük azáltal, hogy a benne szereplő hivatkozásokat töröljük. (A Windows ezen hivatkozásokat a C:\Documents and Settings*felhasználónév*\Recent mappában tárolja.) Másrészt módunkban áll a Klasszikus Start menü testreszabása párbeszédablakot használni, ahol egy gomb áll rendelkezésünkre, hogy a legutóbb használt dokumentumokat, programokat és webhelyek listáját eltávolítsuk.

Adattörlés biztonságosan

Régebben bármilyen adat, amelyet letöröltünk, örökre elveszett. Ma már a merevlemezről letörölt állományok és mappák nem tűnnek el automatikusan, legalábbis nem azonnal – megmaradnak a Lomtárban. (Fontos megjegyezni, hogy a Lomtár csak a merevlemezről törölt állományokat tárolja, a külső adathordozókról vagy a hálózatról törölt fájlok nem kerülnek ide.) Onnan visszaállíthatjuk azokat abba a mappába, ahon-

nan letöröltük, vagy átmozgathatjuk bármely más mappába. Ezzel az a probléma, hogy ha bizalmas állományokat dobunk a szemétbe, majd elfelejtjük üríteni a Lomtárat, akkor bárki visszaállíthatja és megtekintheti az állományainkat.

Ha azt szeretnénk, hogy bizonyos állományok és mappák azonnal eltűnjenek, tartsuk lenyomva a SHIFT gombot, miközben az állományokat és a mappákat a Lomtár ikonjára vonszoljuk. Ha a SHIFT gombot lenyomva tartjuk, miközben a Törlés gombra kattintunk, vagy lenyomjuk a DELETE billentyűt, az előző megoldáshoz hasonlóan az objektumok valóban törlődnek, és nem csupán bekerülnek a Lomtárba.

Ugyanakkor még az állomány Lomtárból történő törlése sem semmisíti meg azonnal az információt. A törléskor felszabadult lemezterület újra felhasználható, de oda csak a következő mentés során kerül adat. Így a megfelelő eszközök segítségével a törölt információ még elolvasható. Ennek kiküszöbölésére olyan állománytörlő programra van szükségünk, amely nem része a Windowsnak. Ilyen például a Symantec Norton Utilities (http://www.symantec.com) és a McAfee Utilities (http://www.mcafee.com). Sajnálatos módon ezek a programok csak akkor működnek, ha a helyreállítani kívánt állomány törlése előtt telepítettük valamelyiküket.

6.3. Biztonsági másolatok készítése

Adataink védelmével kapcsolatosan a legfontosabb: készítsünk biztonsági másolatot az állományainkról! De melyekről, milyen gyakran és milyen eszköz felhasználásával készítsünk biztonsági másolatot? Ebben a fejezetben ezeket a témákat tekintjük át.

6.3.1. Miről készüljön biztonsági másolat?

Célszerű mindenről biztonsági másolatot készíteni, a teljes biztonsági másolat elkészítése azonban sok időt vehet igénybe. Ezért javasolt legalább egyszer egy teljes biztonsági másolatot létrehozni, amelyből a későbbiekben dolgozhatunk, és amelyet frissíthetünk. A biztonsági másolat frissítése ugyanis lényegesen kevesebb időt vesz igénybe. Tanácsos a rendszer alábbi részeiről gyakrabban másolatot készíteni:

- azok a dokumentumok, amelyeken dolgozunk;
- olyan adatbázisok, amelyekhez rendszeresen hozzáadunk adatokat;
- levelezés, különösen az e-mail állományok.

A programok nem szerepelnek a fenti felsorolásban, mivel feltételezhető, hogy rendelkezünk azokkal a CD-kkel, amelyeket a program első telepítésekor használtunk. Ne feledkezzünk meg azokról a programokról sem, melyeket az internetről töltöttünk le: készítsünk ezekről is olyan biztonsági másolatot, amely a letöltött telepítőállományokat tartalmazza.

Ha valamilyen okból újra kell telepítenünk a programjainkat, a legnagyobb nehézséget a különböző eszközök beállításai okozzák, hiszen ezeket az értékeket a prog-

ram telepítésekor adtuk meg, és nem szokás észben tartani ezeket. Ezért munkánk megkönnyítése érdekében célszerű kinyomtatni vagy külön elmenteni a rendszer adatait.

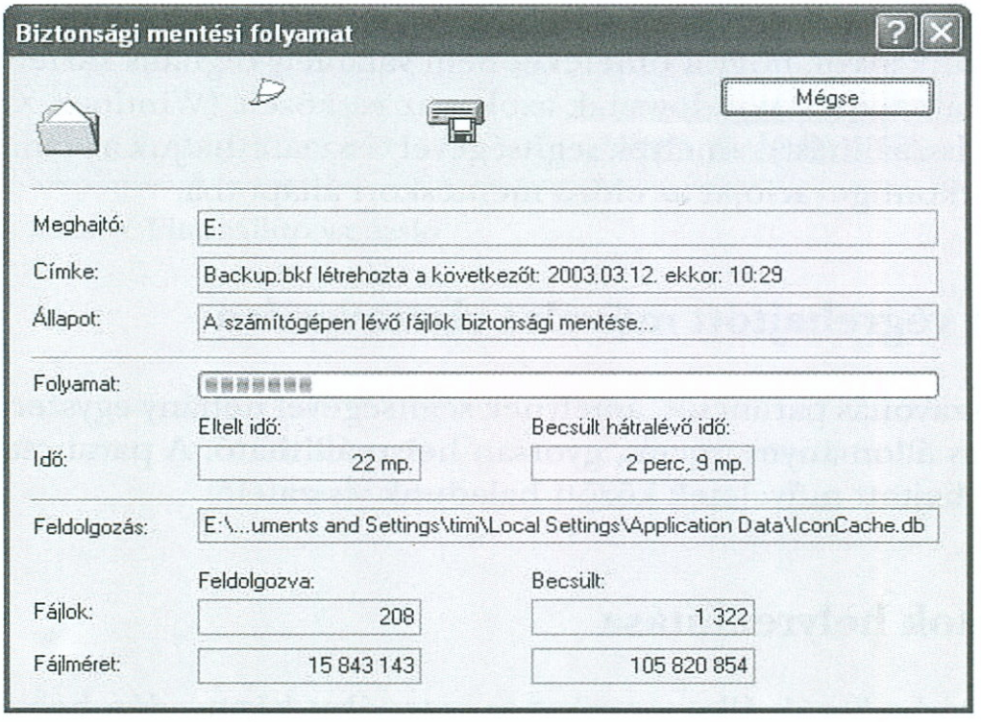
6.3.2. Milyen gyakran készítsünk biztonsági másolatot?

Erre a kérdésre nem adható egyértelmű válasz. Ha egy dokumentumon minden nap dolgozunk, egyetlen napi munka elvesztése komoly problémát okozhat. Ezzel szemben a rendszerállományok csupán akkor változnak, ha a beállításokat módosítjuk, vagy ha új hardvert, illetve szoftvert telepítünk. Csak mi magunk tudhatjuk, hogy mely rendszerelemünk milyen gyakran változik, illetve egy adott anyag elvesztése mekkora veszteséget jelent számunkra.

Általános tanácsként elmondható, hogy rögtön azután készítsünk biztonsági másolatot, miután létrehoztunk vagy megváltoztattunk valamit, amit nem szeretnénk elveszíteni. Meg kell találnunk a középutat az állományok biztonsági másolatának elkészítésével járó nehézségek és a munkánk ismételt elvégzésével járó lehetséges katasztrófa között.

6.3.3. Mivel készítsünk biztonsági másolatot?

A Windows 95 és Windows 98 esetén a Microsoft Backup program áll rendelkezésünkre. A Windows XP operációs rendszerben található Biztonsági másolat segédprogram (lásd 6. ábra) a Windows 2000 részét képező Windows Backup program továbbfejlesztett változata.



6. ÁBRA • A Biztonsági másolat segédprogram

A biztonsági másolatot elkészítő segédprogram feladata, hogy az állományainkról gyorsan és hatékonyan elkészítse a biztonsági másolatot, valamint a fájlok helyreállításában is részt tudjon venni. Ahhoz, hogy a biztonsági másolat tárolása a lehető legkisebb helyet foglalja el, a program tömörítést használ. Képes arra, hogy a másolat hosszabb állományait több floppylemezen vagy eltávolítható médiumon tárolja. A számítógépet folyamatosan használhatjuk a biztonsági másolat elkészítési ideje alatt is. A Biztonsági másolat segédprogram képes minden, Windows-kompatibilis partícióról (NTFS, FAT32, FAT) biztonsági másolatot készíteni.

Nem szabad megfeledkeznünk arról, hogy a Biztonsági másolat segédprogram a másolatokat speciális formátumban tárolja. Így a helyreállításhoz is ezt a segédprogramot kell használnunk, az állományokat nem másolhatjuk egyszerűen oda, ahol használni szeretnénk azokat. Fontos az is, hogy biztonsági másolatainkat csak azon az operációs rendszeren használjuk, amelyen készítettük, mivel az operációs rendszerek újabb és újabb változatainak megjelenésével a biztonsági másolatot elkészítő segédprogram is folyamatosan változik.

6.4. Hibajavítás

A leggyakorlottabb számítógép-kezelőkkel is előfordul, hogy egy rossz mozdulat után döbbenten merednek a képernyőre, és azt kívánják, bárcsak egy perccel vissza lehetne forgatni az időt. Szerencsére számos olyan eszköz áll rendelkezésre, amelyek segítségével a véletlenül elkövetett hibák java része helyrehozható.

6.4.1. Komoly hibák orvoslása

Ahogyan már korábban is szóltunk róla, bizonyos esetekben a számítógép furcsán tud viselkedni. Ha meggyőződtünk arról, hogy a tüneteket nem valamely digitális kártevő okozza, akkor bátran használhatjuk a Windowsnak azokat az eszközeit (Windows XP esetén például a Rendszer-visszaállítást), amelyek segítségével visszaállíthatjuk a számítógép hardver- vagy szoftverkonfigurációját az előző mentéskori állapotba.

6.4.2. Az utoljára végrehajtott művelet visszavonása

Az Intéző tartalmazza a Visszavonás parancsot, amelynek segítségével néhány egyszerű hiba, mint például egy téves állománymozgatás, gyorsan helyreállítható. A parancsot ismételve a korábban végrehajtott műveletek között haladunk visszafelé.

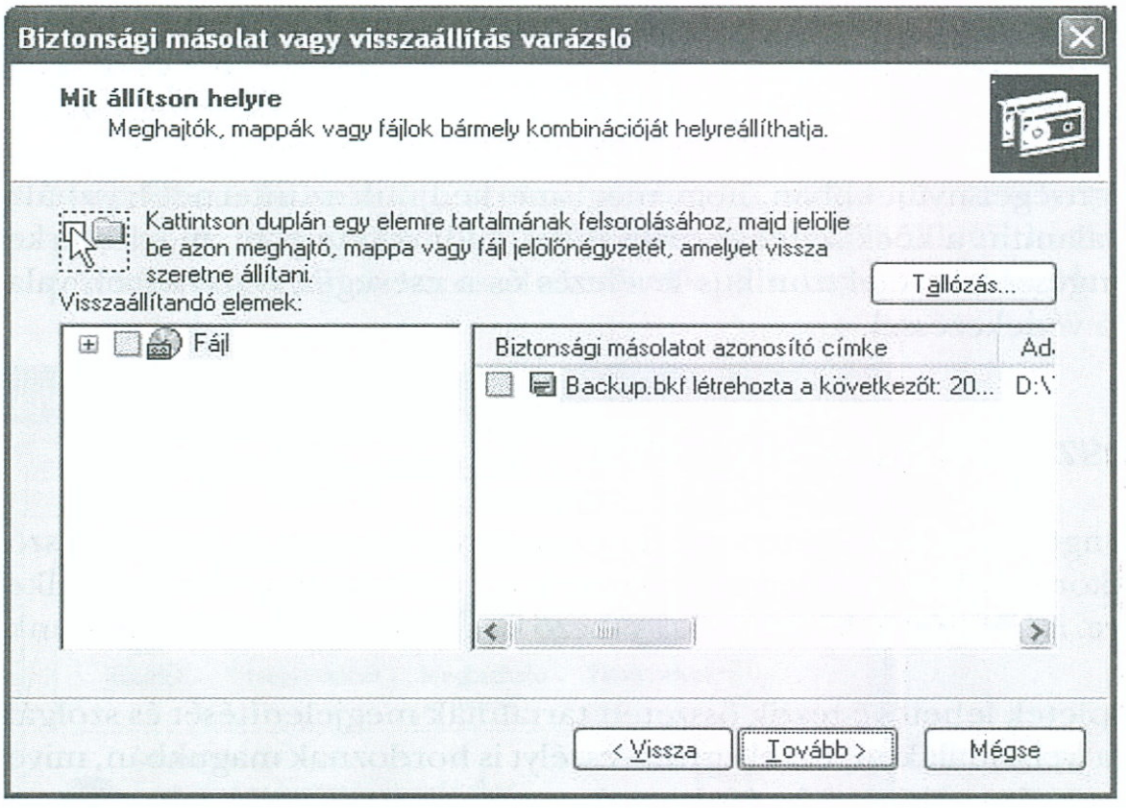
6.4.3. Törölt adatok helyreállítása

A tévedésből letörölt, Lomtárba került állományokat és mappákat könnyedén helyre tudjuk állítani – feltéve, hogy azokat a merevlemezről töröltük, a Lomtárba kerültek,

és a Lomtárat közben nem ürítettük. Ehhez nyissuk meg a Lomtárat, és válasszuk a Fájl menü Helyreállítás parancsát.

Használhatjuk erre a célra a korábban említett Symantec Norton Utilities és McAfee Utilities segédprogramokat is. Használatuk különösen indokolt olyan esetben, ha a Lomtárat már ürítettük.

A biztonsági másolatot azért készítettük, hogy probléma esetén adatainkat könnyedén visszaállíthassuk. Ezért, ha olyan állományokat szeretnénk helyreállítani, amelyekről például Windows XP esetén a Biztonsági másolat segédprogrammal készítettünk másolatot, ezt szinte automatikusan megtehetjük a Visszaállító varázsló (lásd 7. ábra) segítségével, vagy mi magunk is megszabhatjuk a helyreállítás során alkalmazott opciókat, de Windows XP Professional esetén igénybe vehetjük az Automatikus rendszerhelyreállítást (ASR, Automatic System Recovery) is.



7. ÁBRA • Visszaállító varázsló

7. VÉDELEM AZ INTERNETES TÁMADÁSOK ELLEN

„Nihil est pro certo futurum, quod possit aliqua procuratione accidere, ne fiat."
Cicero[11]

Az internet felhasználóinak száma folyamatosan növekszik, eközben újabb és újabb szolgáltatásokat kínálnak számukra, és a tartalmak is mind vonzóbbá válnak. A legtöbb ember életéből már nem maradhat ki ez a médium. Az internetelérés megvalósulásával azonban fokozódnak azok a veszélyek, amelyeknek a felhasználó gépe vagy akár a számítógép-hálózat ki van téve.

Ez a fejezet segítséget nyújt abban, hogy megismerkedjünk az internet használatának veszélyeivel, valamint a kockázatokat reálisabban tudjuk felmérni, megismerkedünk továbbá a böngészés, az elektronikus levelezés és a csevegés veszélyeivel, valamint az ellenük való védekezéssel.

7.1. Böngészés biztonságosan

Sokan szeretünk böngészni az interneten, mert az rendkívül hasznos és felettébb szórakoztató. Ugyanakkor tisztában kell lennünk azzal, hogy ott rengeteg veszély leselkedik számítógépünkre. A böngészés közben a következő kockázatokkal kell számolnunk:

- A szkriptek és appletek lehetővé teszik összetett tartalmak megjelenítését és szolgáltatások nyújtását a weboldalakon. Ezzel együtt veszélyt is hordoznak magukban, mivel hackerek és vírusok támadási eszközei lehetnek.
- Egyes weboldalak információkat gyűjthetnek rólunk és böngészési szokásainkról azáltal, hogy kis állományokat, úgynevezett cookie-kat helyeznek el számítógépünkön.

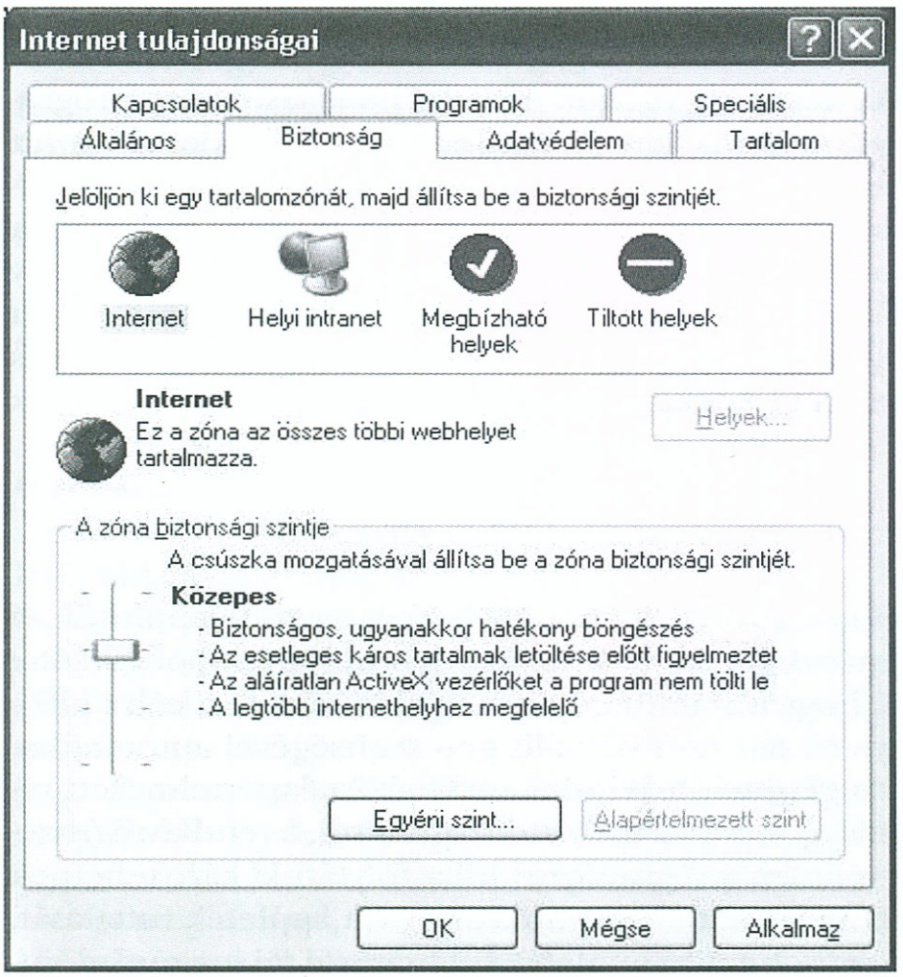
A szkriptekről, appletekről és cookie-król a fejezet későbbi részeiben bővebben olvashatunk. Ebben a fejezetben megismerkedünk a böngészőprogramok, azon belül is az Internet Explorer védelmi beállításaival, melyek használata nélkül veszélyes és felelőtlen vállalkozás az internetre merészkedni.

[11] „Semmi sem biztos a jövőben, aminek bekövetkezte némi gondoskodással elkerülhető." *Latin mondások 2.* Lazi Bt., 2003. ford.: Nagyillés János.

7.1.1. Biztonsági zónák az Internet Explorerben

Az Internet Explorer a világot négy zónába sorolja. Mind a négy zónára megadhatunk magas, közepes, közepesen alacsony és alacsony biztonsági szinteket. Ezen túlmenően lehetőségünk van minden zónához egyéni beállításokat tenni, melyekkel pontosan megadhatjuk, hogy a különféle távoli parancsokra számítógépünk hogyan reagáljon. Tekintsük át ezeket a biztonsági zónákat és főbb jellemzőiket!

- **Internet:** ide sorolható az összes olyan webhely, amely nem a számítógépen vagy a helyi belső hálózaton található, illetve amelyet még nem rendeltünk más zónához. Az ebből a zónából érkező objektumok általában közepes biztonsági szint szerint kezeltek.
- **Helyi intranet:** ez a csoport azokat a helyeket tartalmazza, amelyek például munkahelyünk belső hálózatából vagy saját webkiszolgálójából helyben elérhető. Ezeket a webhelyeket általában a rendszergazda állítja be, amikor a hálózatot telepíti. Az ilyen helyeket rendszerint megbízhatónak tekinthetjük, és az innen érkező objektumoknak közepes biztonsági szintű hozzáférés van engedélyezve.
- **Megbízható helyek:** ide azok a webhelyek tartoznak, amelyekről mi magunk úgy gondoljuk, hogy az itt fellelhető állományok anélkül letölthetők, hogy a számítógépünkön tárolt fájlok károsodnának. Alapértelmezés szerint ide sorolódnak be azok



8. ÁBRA • Az Internetbeállítások párbeszédablak Biztonság füle

a helyek, amelyeket a Microsoft megbízhatónak tekint. Az innen érkező objektumok alacsony biztonsági szint szerint kezeltek, azaz széles körben hozzáférnek számítógépünkhöz.

- **Tiltott helyek:** azok a webhelyek tartoznak ide, amelyekről nem tudjuk teljes bizonyossággal eldönteni, hogy az itt található adatok nem károsítják-e számítógépünk állományait. Ezeket megbízhatatlannak jelöljük, az innen letöltött objektumok számítógépünkhöz csak igen kevéssé férnek hozzá, vagyis a legmagasabb biztonsági szint szerint kezeltek.

Lehetőségünk van arra, hogy webhelyet adjunk a Helyi intranet, Megbízható helyek vagy a Tiltott helyek zónáihoz, mivel a megbízható és tiltott helyek zónái eredetileg üresek. Ugyanígy módunkban áll bizonyos helyek törlése is. Ezt az Internet Explorerben az Internetbeállítások párbeszédablak Biztonság fülének segítségével tehetjük meg (lásd 8. ábra).

Tanácsos megkövetelnünk, hogy a Megbízható helyek listába felvett összes webhely rendelkezzen ellenőrzött titkosított kapcsolattal. Ily módon elkerülhetjük, hogy véletlenül olyan webhelyeket adjunk ehhez a zónához, amelyek nem támogatják a biztonságos kapcsolatot. (A biztonságos és titkosított kapcsolatokról bővebb információt a Titkosítás és tanúsítványok című alfejezetben találunk.)

7.1.2. Szkriptek, appletek és ActiveX-vezérlők

Napjainkban a weboldalak interaktivitását oly módon növelik, hogy kisméretű programokat helyeznek el rajtuk, amelyek az oldal meglátogatásakor a weboldallal együtt letöltődnek. Ezek a folyamatok rendszerint számunkra észrevétlenül, mindenféle figyelemfelhívás nélkül játszódnak le. Bizonyos szempontból ezek a programocskák igen hasznosak lehetnek, de könnyen okozhatnak biztonsági problémákat is: pédául ha egy weboldal figyelmeztetésünk nélkül telepíthet egy programot számítógépünkre, és azt le is tudja futtatni, akkor ugyanilyen egyszerűen más, veszélyes szoftverek, vírusok is felkerülhetnek gépünkre. Az ilyenfajta kockázatokat ki kell küszöbölnünk. Ennek megoldását tekintjük át ebben a fejezetben.

Java, JavaScript, VBScript

A Java programozási nyelven íródott rövid alkalmazások, úgynevezett appletek az interneten használatosak, de futtatásukhoz nem szükséges semmilyen, a böngészőbe beépített modul. Ennek az az oka, hogy a számítógépünk egy külön erre a célra kifejlesztett értelmezőprogram, az úgynevezett Java virtuális gép segítségével automatikusan futtatja azokat. (A Java virtuális gép már a Windows 98-nak is alapértelmezett része.) Bár a Java készítői megpróbáltak gondoskodni biztonságunkról, a rendkívül összetetté váló alkalmazások akár egy véletlen programozói hiba folytán is kárt tehetnek rendszerünkben. Ezért célszerű letiltani számítógépünkről a Java appletek futtatását, vagy legalább úgy beállítani a rendszert, hogy az appletek futtatásáról mi magunk dönthessünk.

A HTML (HyperText Markup Language) képességeit kibővítő JavaScript parancsnyelv nem keverendő össze a Java programozási nyelvvel. A JavaScript nyelven készült, weboldalakba beépülő kis programokat, az úgynevezett szkripteket számítógépünk nem képes automatikusan futtatni, azok csak a böngésző segítségével hajthatók végre.

A VBScript leginkább a Microsoft Visual Basic nyelvre hasonlít. Szkriptje az Internet Explorerben megjelenített oldalakhoz adható hozzá, és a JavaScripttel azonos képességekkel rendelkezik. A JavaScriptek és VBScriptek futtatását is tanácsos letiltani, avagy beállítani, hogy mi magunk dönthessünk a futtatásról, ha a megjelenő párbeszédablakban a megfelelő gombra kattintunk.

ActiveX-vezérlők

Az ActiveX a Microsoft „válasza" a Java programnyelvre. A weboldalakon fellelhető ActiveX-vezérlők bináris állományok, amelyeket közvetlenül a processzor futtat. Ily módon kijelenthető, hogy használatukkal a weboldalak a számítógépünknek túlságosan sok erőforrása felett kapnak irányítást. Ha egyszer véletlenül letöltünk egy ActiveX-vezérlőt, az utána szabadon tevékenykedhet számítógépünkön: tudtunk nélkül további ActiveX-vezérlőket tölthet le, amelyek a továbbiakban már szerves részeit képezik szoftverkörnyezetünknek, így szinte lehetetlen követni, hogy pontosan mi is történik számítógépünkkel.

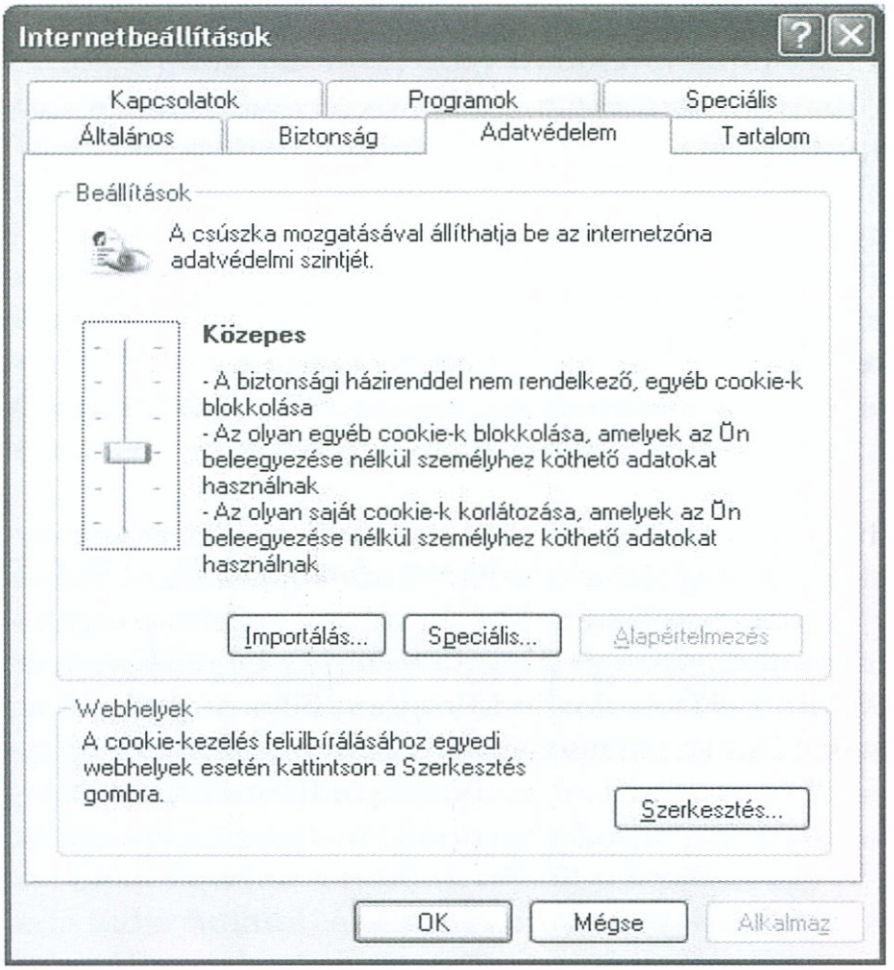
Mivel ezek veszélyt is jelenthetnek számítógépünkre, tanácsos az ActiveX-vezérlőket minden zónában letiltani, kivéve a Megbízható helyet. Ennek a félmegoldásnak az az oka, hogy ha gyakran látogatjuk a Microsoft weboldalait, számos csábító szolgáltatásról maradhatunk le, ha nem kapcsoljuk vissza az ActiveX-vezérlők engedélyezését. (A letöltött ActiveX-vezérlők a C:\Windows\Downloaded Program Files mappában találhatók. Ha Internet Explorert használunk, tanácsos gyakran ellenőrizni ezt a mappát.)

7.1.3. Cookie-k

A cookie (süti) egy kisméretű állomány, amelyet egyes weboldalak helyeznek el számítógépünkön, és elérési útvonalunkat, a megnyitott oldalakat vagy az általunk megadott személyes információkat tartalmazhatják. A cookie-k használatával a webkiszolgálón lévő oldalakat személyre szabhatjuk, hogy legközelebbi látogatásunkkor a korábban beállított környezet fogadjon minket. A tartalmat elvileg csak a cookie-t létrehozó weboldal olvashatja el, és csak az általunk megadott információkhoz biztosít hozzáférést. Mivel a cookie-k potenciális veszélyforrások, ezért megfelelően kell kezelnünk azokat.

Nem szabad elfeledkeznünk arról, hogy a világhálón keresztül igénybe vehető szolgáltatások jelentős része nem működik a cookie-k nélkül, ezért nem célszerű az összes cookie blokkolása. Az sem kényelmes, ha az Internet Explorer minden cookie esetén megkérdezi, hogy az adott weblaptól elfogadhatja-e a cookie-t, vagy sem. Ezért különbséget kell tennünk a belső és a külső cookie-k között. A két típus között abban van eltérés, hogy milyen webkiszolgálótól érkezik: a belső cookie-k közvetlenül arról a

weboldalról érkeznek, amellyel kapcsolatban vagyunk, azaz amelyet a böngészőablakban látunk. A külső cookie-k azok, amelyek olyan webkiszolgálóktól érkeznek, amelyekkel a kapcsolatot rendszerint észre sem vesszük, azaz szinte kivétel nélkül reklámcégektől származnak. Ezért tanácsos elfogadni az összes belső cookie-t, és blokkolni az összes külsőt. Megjegyezzük, hogy a Netscape esetén sokkal rugalmasabb a cookie-k kezelése, mint az Internet Explorernél. Az Internet Explorer adatvédelmi beállításait szemlélteti a 9. ábra.



9. ÁBRA • Az Internet Explorer adatvédelmi beállításai

7.1.4. Titkosítás és tanúsítványok

Böngészés közben gyakran előfordul, hogy a letöltött weboldal személyes adatokat kér be tőlünk. Ilyenkor a böngésző megadja a weboldal nevét és a kért információkat, mi pedig eldönthetjük, hogy megadjuk-e a kért adatokat. Ebben a döntésben a tanúsítványok segíthetnek bennünket. A tanúsítványok a korszerű böngészők által kínált lehetőségek, amelyekkel biztonságosabbá tehető a böngészés. Ezek olyan titkosított adatok, amelyekkel azonosíthatóvá válik számítógépünk távoli gépek számára és fordítva. Tanúsítványokat csak hitelesítési szervezetek adhatnak ki, és a cégek mindegyike egymástól különböző, saját tanúsítványt használ. Az Internet Explorer mintegy harminc

hitelesítési szervezetet ismer, ennek köszönhetően a távoli számítógépek által küldött hitelesítések jelentős része ellenőrizhető.

Az említett biztonságos kapcsolat létrehozásához az Internet Explorerben az SSL-t (Secure Sockets Layer, biztonsági alréteg) kell használnunk. Ez a szabványos http-protokoll kiterjesztése, melyet gyakran https-nek neveznek, míg azokat a webkiszolgálókat, amelyek képesek a https használatára, biztonságos szervereknek (angolul secure server). Az SSL leggyakrabban észrevétlenül működik, a biztonsági azonosítás automatikusan zajlik.

Mi magunk is kaphatunk személyes tanúsítványokat. Ezeket saját magunk azonosítására használhatjuk, amikor az Internet Explorer vagy a Navigator segítségével biztonságos kommunikációt igénylő weblapokat látogatunk meg. A legismertebb hitelesítési szervezet, amely személyes tanúsítványokat is kiad, a VeriSign (http://www.verisign.com) és a Thawte (http://www.thawte.com). A tanúsítványokról további információkat kérdés-felelet formában az RSA Adatbiztonság honlapján (http://www.rsasecurity.com/rsalabs/faq) találunk.

7.1.5. Böngészés névtelenül

Amennyiben felhasználói fiókunkat többen is használhatják, nem szerencsés, ha internetes böngészésünk nyitott könyv mások számára. Legyünk óvatosak, mivel a Címsor, az Előzmények és a Vissza menü magánjellegű bejegyzéseket is tartalmazhat. Ezek segítségével más könnyen megtudhatja, milyen weblapokat látogattunk meg. (Természetesen ez fordítva is igaz: mi magunk is nyomon követhetjük, hogy a mi gépünket használva mások merrefelé szörföztek a világhálón.) Tekintsük át ezeknek az eszközöknek a kezelését!

Ideiglenes állományok és gyorstárak

A gyorstárak, illetve az ideiglenes állományok átmeneti tárolók, amelyek segítségével a böngészéskor megnyitott összes weboldal a merevlemezünkre mentődik. (A gyorstár, angol szakkifejezéssel élve a cache, a Netscape esetén használatos terminológia. Internet Explorer esetén ezt Ideiglenes internetfájloknak nevezzük.) Itt a weboldalak tartalma külön állományokra szétbontva tárolódik, így letöltésük legközelebb sokkal gyorsabb lesz, hiszen a tartalom jelentős része már a merevlemezünkön található. Ez roppant hasznos, ugyanakkor ilyen módon bárki könnyedén meg tudja állapítani, hogy az utóbbi időben milyen oldalakat tekintettünk meg. Ezért célszerű ezeket az átmeneti tárolókat rendszeresen kiüríteni. Ezen túlmenően módunkban áll megadni azt is, hogy miként kerüljenek ide fájlok, vagy mennyi tárhelyet engedélyezünk a merevlemezen az ideiglenes állományok számára.

Az Előzmények használata

Az Internet Explorer az összes korábban meglátogatott weblapot az Előzmények mappában, internetes parancsikonként eltárolja. A mappa helye a C:\Documents and

Settings*felhasználói név*\Local Settings\History, mivel minden felhasználói fiók előzményei, a saját beállításokkal együtt külön tárolódnak. Az Előzmények mappában több almappa található: az elmúlt 20 napból az adott hétre eső napoknak külön mappájuk van, míg az előző hétre eső napok közös mappán osztoznak. Minden nap mappája további almappákat tartalmaz, melyek egy-egy meglátogatott webhelyhez tartoznak. Ezeken a mappákon belül az adott helyen meglátogatott összes weblap parancsikonja megtalálható.

Az előzmények működését kikapcsolhatjuk, belőle alkalmanként elemeket törölhetünk, mellyel egyes weblapok hivatkozásait távolíthatjuk el az előzmények közül, valamint szerkeszthetjük azokat.

7.1.6. Gyermekeink védelme

Gyermekeinket nem célszerű eltiltani a számítógép használatától, hiszen a tiltás csak a kíváncsiságot fokozza. A legtöbb, amit megtehetünk, hogy a szerintünk megfelelőnek tartott szempontok szerint korlátozzuk számukra a hozzáférést.

Az Internet Explorer Tartalmi tanácsadója segítségével szabályozhatjuk, hogy gyermekeink a böngészés során ne férhessenek hozzá a számukra tiltott oldalakhoz. Ugyanakkor a szűrés hatékonysága az oldalak készítőin múlik, ugyanis a szűrés alapjául az oldalakban található minősítés szolgál. A Tartalmi tanácsadó bekapcsolása után már csak a szempontjainknak megfelelő, minősített tartalom jelenhet meg a képernyőn.

Ezen túlmenően, nyugalmunk megőrzése érdekében nem tanácsos lehetővé tenni, hogy gyermekeink a számunkra fontos adatainkhoz hozzáférjenek. Ezért a Tartalmi tanácsadó használata mellett célszerű a következő óvintézkedéseket végrehajtani:

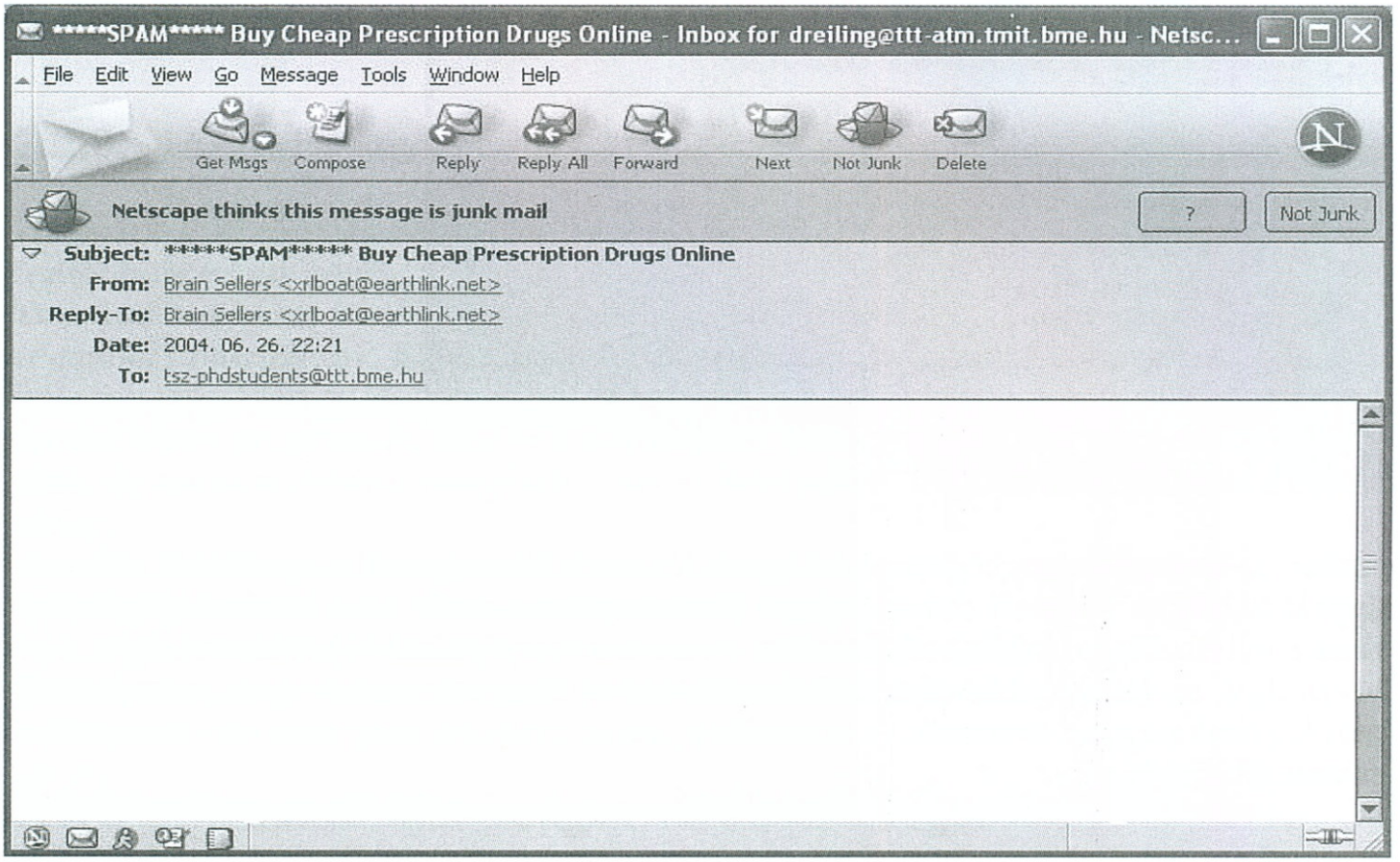
- Ne hagyjuk a gyermeket hosszabb ideig felügyelet nélkül a számítógép előtt.
- Készítsünk gyermekünk számára saját felhasználói profilt.
- Tiltsuk le számukra bizonyos programok használatát.

7.2. Levelezés biztonságosan

Az internet legnépszerűbb szolgáltatása, hogy a világháló felhasználói üzeneteket küldhetnek és fogadhatnak. Annak ellenére, hogy korszakalkotó találmány, számos hátránnyal is rendelkezik. Elég, ha csak az e-mail címünkre nézünk: ez elárulja a nevünket (ha nem becenevet használunk, akkor a saját nevünket is), az internetszolgáltatónk nevét, sőt, akár azt is, hogy a szolgáltatónk melyik kiszolgálójához, szeréhez tartozunk. Ez nem túl megnyugtató, nem is beszélve az elektronikus levelezéshez kapcsolódó támadási pontokról. Ezeket és ezek ellenszereit tekintjük át ebben a részben.

7.2.1. Levélbombák – túlcsorduló postafiók

A levélbombák vagy nem kívánt üzenetek (angol szakkifejezéssel spamek) nem jelentenek közvetlen veszélyt az internetfelhasználók adataira vagy számítógépére, inkább csak zavarók, hiszen elég időigényes lehet, ha valakinek hirtelen több száz, nem kívánt levelet kell törölnie postafiókjából. A levélbomba-támadásnak az a következménye, hogy a címzett postafiókja hamar túllépi a megengedett maximális kapacitást, és nem képes további e-maileket fogadni. A 10. ábra egy levélbombát mutat.

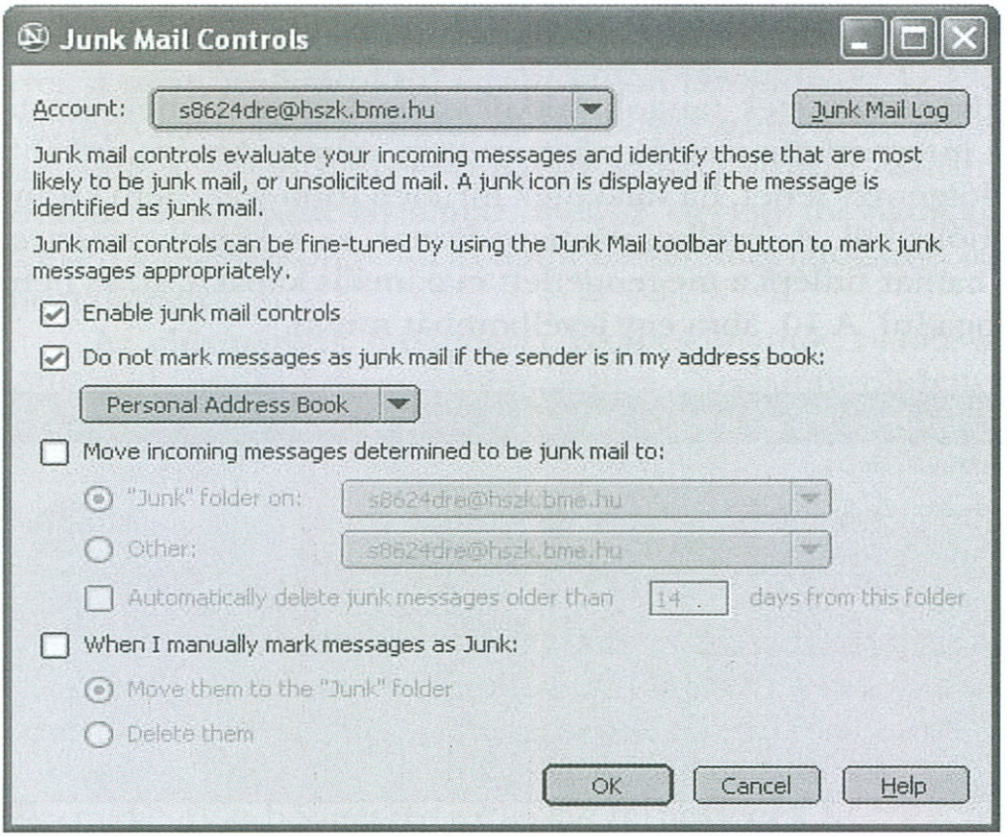


10. ÁBRA • Levélbomba

Ehhez a támadáshoz számos programot fel lehet használni, továbbá maga a támadó is anonim maradhat, sőt, még arra is van lehetőség, hogy valaki hamis feladót adjon meg. Szerencsére védekezhetünk a nem kívánt üzenetek ellen: a legtöbb szolgáltató lehetővé teszi, hogy kiválasszuk az úgynevezett anti-spam opciót. Ez a módszer megakadályozza, hogy az esetenként elképesztő tömegű levél egyáltalán továbbítódjék a felhasználóhoz. A Netscape anti-spam opciójának beállításait mutatja a 11. ábra.

7.2.2. E-mail vírusok

Mivel az Outlook és az Outlook Express használata igen széles körben elterjedt, a víruskészítők legfőbb célpontjaivá ezek a programok váltak. Az Outlook Express 6 két nagyon fontos újdonsággal rendelkezik, amelyekkel nagyságrendekkel csökkent a ví-



11. ÁBRA • Az anti-spam konfigurálása

rusfertőzés veszélye: a program korlátozza a csatolt állományok megnyitását, valamint figyelmeztet, ha bármely más program a nevünkben e-mailt akar küldeni gépünkről. Ezek a jellemzők és beállítások azonban messze nem nyújtanak teljes biztonságot. Akár használjuk az alábbiakban ismertetésre kerülő módszereket, akár nem, mindenképpen legyünk nagyon óvatosak, és semmiképpen se nyissunk meg nem várt üzeneteket, csatolt állományokat.

Csatolt állományok korlátozása

A csatolt állományok megnyitása során az állomány kiterjesztésének megfelelő alkalmazás lép működésbe. Ez azt jelenti, hogy ha nem ismerjük a fájl kiterjesztését, nem tudhatjuk, milyen program fog elindulni a megnyitásakor. Ha a melléklet maga egy program, akkor annak elindítása után már nem ismert, hogy mi történik a számítógépünkkel.

Néhány vírus megpróbálja elrejteni a melléklet típusát azáltal, hogy a csatolt állománynak két kiterjesztést ad. Ha olyan módon állítottuk be a Windowst, hogy az ne jelenítse meg az ismert kiterjesztéseket, a látvány könnyen félrevezethet bennünket. Ezért tanácsos, hogy ne rejtsük el az ismert fájltípusok kiterjesztését. Ezen túlmenően a két kiterjesztéssel bíró fájlmellékletet valószínűleg nem az ismert program ikonja jelöli. Tehát mindig figyeljünk a megfelelő ikon meglétére is.

Természetesen az ikonokat is lehet hamisítani. Ezért az Outlook Expressben lehetőségünk van arra, hogy a veszélyesnek ítélt mellékleteket a levelezőprogram zárol-

ja. Általános tanácsként elmondható az is, hogy először mentsük merevlemezre, és ellenőriztessük vírusellenőrző programmal az ismeretlen forrásból érkező levelek csatolt állományait.

Más programok megakadályozása abban, hogy nevünkben e-maileket küldjön

Az Outlook Expresst más programok is használhatják e-mailek automatikus küldésére. Egy vírus ezt a tulajdonságot használhatja ki, és saját magát továbbíthatja. Ezt a viselkedést megváltoztathatjuk oly módon, hogy az Outlook Express minden automatikus levélküldés esetén értesít bennünket, és jóváhagyásunkat kéri.

7.2.3. Anonimitás

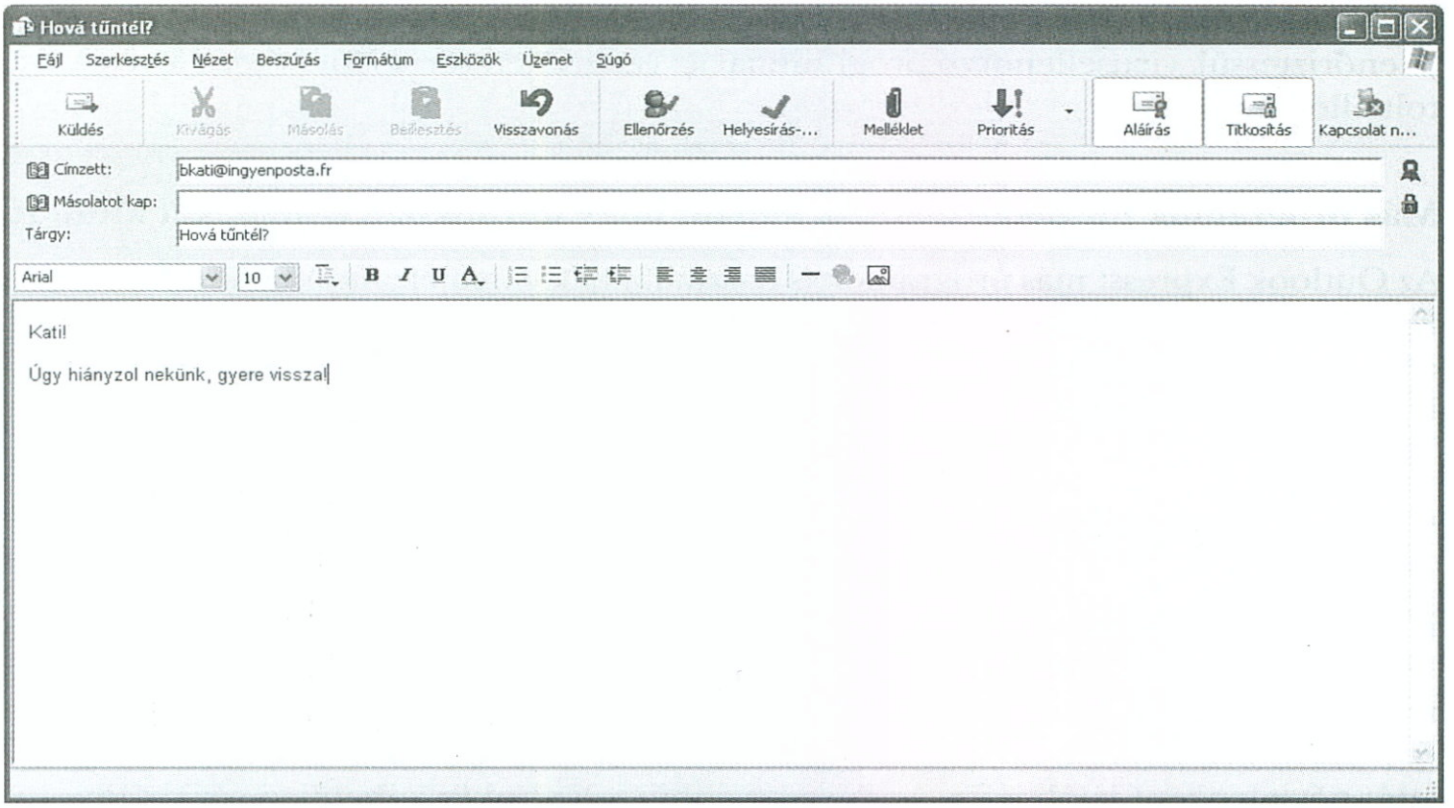
Ha saját e-mail címünket használjuk, nem tudunk névtelenül üzenetet küldeni, és mint fentebb már említettük, az e-mail cím sok mindent elárul rólunk. De megőrizhetjük anonimitásunkat, ha úgynevezett továbbító postafiókot (angol szakkifejezéssel re-mailer) használunk. Ekkor a továbbító az üzenetet eljuttatja a címzettnek, de a feladót névtelenként jelöli meg. Az ilyen továbbítók bárhol fellelhetők a világhálón. Léteznek olyan programok, amelyek segítségével nemcsak névtelen üzeneteket küldhetünk, de anonim módon böngészhetünk az interneten. Ilyen szoftver például a Private idaho.

Ne feledkezzünk meg azonban arról, hogy mi magunk sem szeretünk ismeretlenektől, különösen nem anonim idegenektől levelet kapni. Ezért ne lepődjünk meg, ha a névtelenül elküldött leveleink a címzett szemeteskosarában végzik! (Ugyanez lehet a sorsa a tárgy, subject megjelölése nélkül elküldött leveleknek is.)

7.2.4. Az e-mail biztonságos küldése és fogadása

A levelezőprogramok kétféle típusú biztonsági szolgáltatással rendelkeznek: aláírással és titkosítással. Az aláírások lehetővé teszik, hogy levelünkhöz csatoljunk egy aláírási blokkot, amelyekkel igazolható, hogy a levelet valóban mi írtuk, és az a kézbesítés során nem módosult. Az aláírás az e-mail végéhez csatolódik, így annak tartalma nem módosul, továbbá a címzett az aláírás ellenőrzése nélkül is elolvashatja a levelet. A titkosítás során magát a tartalmat változtatjuk meg olyan módon, hogy azt csak a címzett tudja dekódolni. Bárki, aki a levél továbbítása közben belenéz az üzenetbe, értelmetlen szöveget talál ott.

Lehetséges, hogy a két módszert egyszerre használjuk: azaz először digitálisan aláírjuk, majd titkosítjuk a levelet. Ez garantálja, hogy csak a címzett tudja az üzenetet elolvasni, ráadásul meg is bizonyosodhat afelől, hogy a levelet biztosan mi küldtük. Egy aláírt és titkosított levél üzenetablakát mutatja a 12. ábra, ahol az aláírást egy sárga szalag jelzi, mely az üzenetszerkesztő ablakban a Címzett sorának végénél látható, míg a titkosítást egy boríték melletti kis kék lakat jelöli.



12. ÁBRA • Egy aláírt és titkosított levél üzenetablaka

7.3. Csevegés biztonságosan

A csevegőprogramok és fórumok előnye, hogy azokat bárki, alacsony költséggel használhatja. Ezzel a módszerrel sokkal gyorsabban üzenhetünk egymásnak, mint az elektronikus levelezéssel, a beszélgetésbe többen is be tudnak kapcsolódni, továbbá a rövid szöveges üzenetek mellett lehetőségünk van élőszavas, mozgóképes kapcsolat kialakítására is.

Ugyanakkor az utóbbi időben elszaporodtak azok a vélemények, amelyek biztonsági kockázatként jelölik meg a csevegőprogramokat. A legnagyobb veszély tulajdonképpen abban rejlik, hogy a program a támadónak információkat szolgáltat ki az áldozatról, de támadási típus lehet az is, amelynek során a támadó üzenetek sokaságával bombázza az áldozatot. Tekintsük át, hogy milyen támadási lehetőségekkel kell szembenéznünk, és hogyan védekezhetünk ellenük!

- **Korrupt linkek:** a különböző linkek megnyitásával aktiválhatunk egy állományt (például egy vírust), vagy esetleg a merevlemezt is formázhatjuk. Ez ellen olyan módon lehet védekezni, ha úgy állítjuk be a rendszerünket, hogy a nekünk küldött ismeretlen linkeket azonnal eldobja.
- **Állományok küldése és fogadása:** ahogyan a levelezésben, úgy a csevegés során is lehet állományokat küldeni és fogadni. Ezért azok a tanácsok, amelyeket az elektronikus levelek mellékleteivel kapcsolatban ismertettünk, a csevegés során továbbított fájlokra is érvényesek.

- **Partner felvétele engedély nélkül:** a támadók az áldozataikat úgy szeretnék felvenni a partnerek listájába, hogy ezt az áldozatok ne vegyék észre. Szerencsére a csevegőprogramok készítői folyamatosan dolgoznak a rendszer biztonságán, ezért például a Windows Messenger azonnal tájékoztat bennünket arról, ha valaki felvett bennünket partnereinek listájába.
- **Programok vezérlésének átadása:** lehetőségünk van arra, hogy átengedjük a beszélgetés többi résztvevőjének bizonyos megosztott programok irányítását. Beszélgetőtársaink szabadon adhatnak ki parancsokat, miközben saját gépükön az adott programnak még csak telepítve sem kell lennie. Ez természetesen magában hordozza azt a kockázatot, hogy beszélgetőtársunk tönkreteheti munkánkat, így a program vezérlésének átadása előtt tanácsos biztonsági másolatot készíteni a fontosabb állományokról.

8. A JELSZAVAKRÓL

„Mundus ratione, non casu administratur."
Augustinus[12]

Mivel már sok mindent tudunk a számítógépünk védelméről, vizsgáljuk meg, miként érhető el az, hogy csak az arra jogosult személyek férhessenek hozzá a gépen tárolt adatokhoz. A jelszó megadása az első biztonsági beállítás, amellyel adatainkat megvédhetjük az illetéktelen személyektől. Ebben a fejezetben elsőként azt tekintjük át, hogy Windows-rendszerekben milyen jelszótípusokat használhatunk. Ezt követően pedig azt, hogy miként lehet a megfelelő jelszót kiválasztani, milyen jelszót ne válasszunk, és hogyan védelmezzük jelszavainkat.

8.1. Jelszótípusok a Windows-rendszerekben

A Windows számos erőforrása védhető jelszóval. A legfontosabb jelszótípusok a következők:

- **BIOS jelszó:** a számítógép elindulásakor elérhető BIOS számos fontos beállítást tesz lehetővé. Ha jelszót rendelünk hozzá, a rendszert nem tudják elindítani azok, akik ezt a jelszót nem ismerik (lásd „A BIOS jelszavas védelme" című fejezetet).
- **Felhasználói jelszó:** a felhasználói fiókhoz tartozó jelszót jelöli, amelyet akkor kell begépelnünk, amikor a Windows elindul, vagy az egyik jelszóval védett felhasználói fiókból a másikba váltunk. Ezt a jelszót bármikor megváltoztathatjuk.
- **Tartományi jelszó:** a különféle LAN-szerverek által felügyelt helyi hálózat részét képező gazdaszámítógép felhasználói fiókját ellenőrző jelszó. Ha hiányzik vagy érvénytelen a tartományi jelszavunk, nem férhetünk hozzá a helyi hálózat erőforrásaihoz.
- **Titkosított ZIP tömörített mappák:** a ZIP tömörített mappákhoz rendelt jelszó. A jelszóval ellátott ZIP tömörített mappákat csak a jelszót ismerő személy tudja kitömöríteni.
- **NTFS titkosított jelszó:** az NTFS partíciókon tárolt állományokhoz vagy mappákhoz rendelt jelszó. A Windows XP Professional esetén lehetőségünk van arra, hogy jelszót rendeljünk az NTFS partíciókon tárolt állományokhoz és mappákhoz. A titkosítás FAT32 partíciók esetén nem áll rendelkezésünkre.
- **Képernyőkímélő:** a képernyőkímélő jelszavas védelme. Ezzel a jelszóbeállítással gon-

[12] „Értelem kormányozza a világot, nem a véletlen." *Latin mondások 2.* Lazi Bt., 2003. ford.: Nagyillés János.

doskodhatunk arról, hogy számítógépünk rövid távollétünk alatt is védett legyen: a képernyőkímélő bekapcsolása után csak a megfelelő jelszót megadó felhasználónak engedi meg a rendszer elérését. Ha mások is hozzáférhetnek gépünkhöz, célszerű beállítanunk ezt a jelszót, különben könnyen eshetünk gonosz tréfa áldozatául. Képzeljük el, hogy valaki öt perc után működésbe lépő jelszavas képernyőkímélőt állít be. Ha ez megtörténik, akár egy rövid telefonbeszélgetés után sem tudunk hozzáférni rendszerünkhöz. Ilyen esetben szerencsére (vagy inkább sajnálatos módon) többféleképpen fel lehet törni a képernyőkímélő jelszavas védelmét. Ennek leghatásosabb módszere a számítógép újraindítása, vagy Windows 95 alatt a futó folyamat leállítása a Feladatkezelő segítségével.

8.2. A megfelelő jelszó kiválasztása

A helyi támadásoknál nagy szerepük van a jelszavak kikémlelésének. Jelszófeltörő programok segítségével a hackerek szinte minden, Windows alatt tárolt jelszót képesek megszerezni. Sajnos ebben a rendszerben nagyon könnyű hozzáférni ezekhez az információkhoz, a felhasználóknak pedig egyre nehezebb a jelszavak elrejtése. Tekintsünk át néhány hasznos tanácsot, hogy ennek ellenére a lehető legnagyobb mértékben megnehezíthessük a behatolók dolgát!

8.2.1. Milyen jelszót ne válasszunk?

Az emberek többsége nem szereti a bonyolult jelszavakat, mert attól fél, hogy elfelejti azokat, ezért hajlamos túl könnyen kitalálható jelszavakat használni. Lássuk, milyen jelszavakat kell mindenképpen elkerülnünk!

- Nevek: ne válasszunk jelszóként velünk vagy családunkkal kapcsolatos neveket (vezetékneveket, keresztneveket, becenéveket).
- Kedvenc dolgaink: a jelszó ne utaljon hobbinkra, szenvedélyeinkre, kedvenc autómárkánkra, úticélunkra stb.
- Dátumok: ne válasszunk születési, illetve egyéb, számunkra fontos dátumot.

8.2.2. Milyen a jó jelszó?

Ennyi tiltás után nézzük, hogy milyen tulajdonságokkal rendelkezik a megfelelő jelszó!

- Nehezen jegyezhető meg, nem értelmes szó.
- Nem túl rövid, mivel a megfejtés ideje arányos a jelszó hosszával.
- Tartalmaz számot és különleges karaktert is, amely tovább nehezíti a feltörést.

8.2.3. A jelszavak védelme

Ha már jelszót rendeltünk a felhasználói fiókhoz, állományainkhoz, mappáinkhoz és még sok minden máshoz, akkor egy sor jelszót kell valahogyan titokban tartanunk. Ezért tartsuk észben a következő tanácsokat:

- Ne mentsük el a jelszót! Ugyanis lehetőség van arra, hogy az internetkapcsolathoz tartozó jelszót elmentsük, hogy azt ne kelljen minden alkalommal beírnunk. De ha számítógépünket többen használhatják, akkor az elmentett jelszónak köszönhetően az internetkapcsolatunkhoz is bárki hozzáférhet. Ezért tanácsos, ha ezt a jelszót nem mentjük el.
- Ne áruljuk el a jelszót senkinek! Hiszen azt éppen azért használjuk, hogy rajtunk kívül senki ne férhessen hozzá bizalmas adatainkhoz.
- Ne írjuk le a jelszót! Még akkor se készítsünk ezekről feljegyzést, ha nagyon feledékenyek vagyunk. Ehelyett válasszunk számunkra könnyen megjegyezhető jelszót.
- Váltsunk időnként jelszót! A gyakran cserélt jelszavakat nehezebb kikémlelni, megfigyelni.

IRODALOMJEGYZÉK

Die Hackerbibel I. Werner Pieper Vlg., Löhrb. 1985.
Farmosi István–Kis János–Szegedi Imre: *Víruslélektan.* Cédrus, 1990.
Holbrook, P.–Reynolds, J.: *Site Security Handbook.* IETF RFC 1244, 1991. július.
Kis János–Szegedi Imre: *Vírushatározó.* Cédrus, 1992.
Nagy Gábor: *Vírusvédelem a PC-n.* ComputerBooks, 1995.

TÁRGYMUTATÓ

Vírusvédelem

A **Panem Praktikus Informatika_** sorozat azoknak a számítógép-felhasználóknak szól, akik átlagos számítástechnikai ismerettel rendelkeznek, és az adott témát valamilyen praktikus okból kívánják használni.

A sorozatnak ez a kötete a vírusokkal és a velük szembeni védekezéssel foglalkozik.

A tartalomból:

- Vírusok csoportosítása, vírustípusok
- Antivírus-programok
- Vírusra utaló jelenségek
- Tennivalók fertőzés észlelésekor
- Az operációs rendszer védelme
- Adataink védelme
- Védelem az internetes támadások ellen
- Jelszavak és védelmük

Keresse a **Panem Praktikus Informatika_** sorozat köteteit!

PANEM

www.panem.hu

790 FT

ISBN 963-545-412-0

9 789635 454129