PC-BIZTONSÁG
felsőfokon

CHIP
Professzionális

PC-biztonság
felsőfokon

CHIP

Felelős kiadó: Carsten Gerlach ügyvezető igazgató
Szerkesztő: Horváth Annamária
Olvasószerkesztő: Kudella Magdolna
Tervezőszerkesztő: Dancs Katalin
Címlapterv: Szincsák László

A kötetet készítette:
Levilágítás: HVG Press
Nyomtatta és kötötte: Kaposvári Nyomda Kft. – 241387
Felelős vezető: Pogány Zoltán igazgató
ISBN 963 217 309 0
ISSN 1786-2825

TARTALOM

1 **Előszó: Adatbiztonság és adatvédelem** 5

Adatbiztonság és adatvédelem – nagyon tág területről van szó. A böngésző és az e-mail program kiválasztását ugyanúgy érinti, mint az adatmentés helyes stratégiáját, a spyware elleni védelmet, valamint a spam, a vírusok és a férgek elterjedésének megelőzését.

2 **Spam és antispam** 8

Ebben a fejezetben szót ejtünk a spamküldők trükkjeiről, és bemutatunk néhány olyan eszközt, amelyek valóban segítenek ellenük.

3 **Kémeszközök** 21

A spyware vagy az adware a tudomásunk nélkül gyűjt információkat rólunk. Általában ezek az információk reklám célokat szolgálnak, azonban másnemű információk is lehetnek. Ebben a fejezetben arról olvashatnak, hogy miként ismerhető fel a spyware, és hogyan szabadulhatnak meg tőle.

4 **Az e-mailek és a csatolt fájlok védelme** 29

Elküldenénk valaha is a kutatási eredményekről szóló közleményeket, a cég forgalmának adatait, vagy a bizottsági elnök leváltásáról szóló híreket egy levelezőlapon? Természetesen nem, még levélben sem, hiszen modern emberek vagyunk, és ezért mindent e-mailen keresztül bonyolítunk, annak ellenére, hogy a kódolatlan e-mail sem jobb semmivel sem egy levelezőlapnál.

5 **Spamről, vírusokról és más gazságokról** 36

Amikor PC-nk furcsán reagál, amikor támadások érik, amikor a spam átveszi az irányítást – mindezekben az esetekben védekeznünk kell. Ebben segítséget nyújtanak weboldalak, amelyek információkat gyűjtenek a károkozókról.

6 Vírusok és vírusölők 40

Nem elég, hogy az e-mailek 80%-a csupán értelmetlen spameket tartalmaz, a vírusgyártók még egyfajta versenyt is vívnak egymással: ki programozza a legalattomosabb férget? Ebben a fejezetben bemutatunk néhány eszközt a ma és a holnap csapásai ellen.

7 A holnap vírusai 49

A vírusok, a férgek és a trójai programok elértek egy eddig nem ismert összetettséget. A szakemberek pedig még gyorsabb támadásokra és még gonoszabb támadókra hívják fel a figyelmet.

8 Biztonsági adatmentés 61

Elismerjük, a PC-s hardver ma már nagyon megbízható, ritka a PC-hibák miatt bekövetkező adatvesztés. Az adatmentés témáját mégsem vehetjük könnyedén, hiszen adataink elveszhetnek vírustámadás, programhiba vagy akár hibás egérkattintások következtében is.

9 Image-programok 70

Ha a Windows sztrájkba lép, nem árt, ha van róla biztonsági másolatunk. Nem kell mindjárt újratelepíteni: elég egy image, és percek alatt friss operációs rendszert varázsolhatunk elő.

10 A PC újraélesztése 78

Sehogy sem akar a Windows úgy elindulni, ahogy megszoktuk? Ebben a fejezetben megmutatjuk, hogyan hozható újból működésbe a PC egy alattomos támadás vagy a rendszer teljes kiesése után.

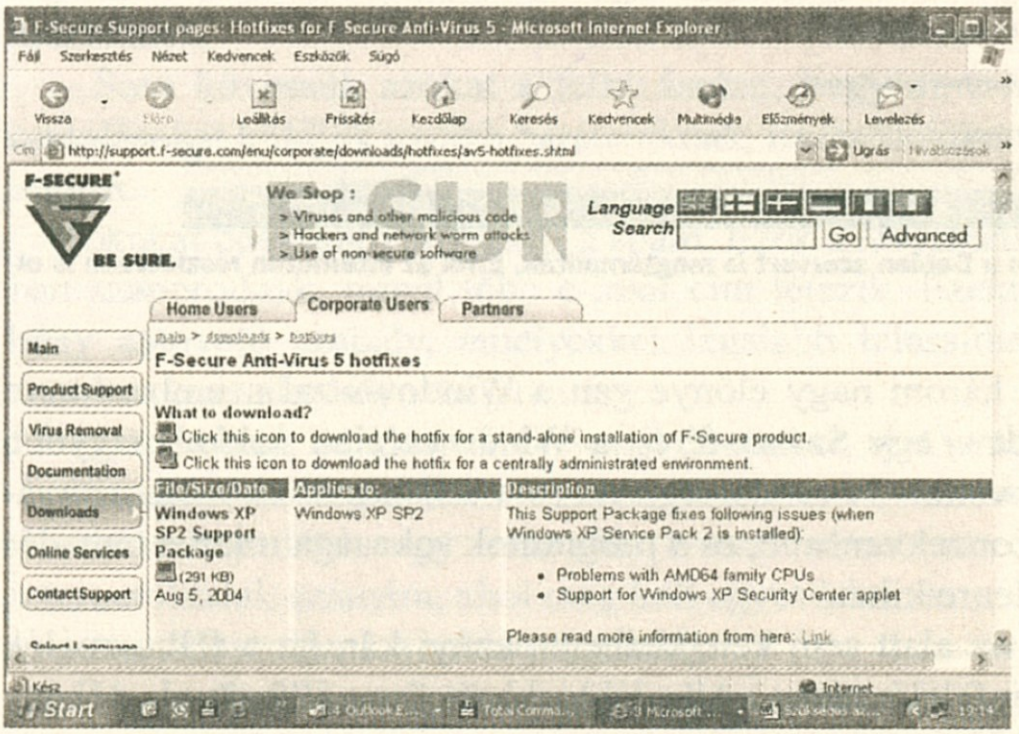
11 Hálózati biztonság 86

A vírusok és hackerek elleni legsürgősebb védőintézkedéseket tíz perc alatt végrehajthatjuk, és a hálózatunk minden irányból védett. És aki még a legmagasabb biztonsági fokozatra vonatkozó profi tippjeinket is megfogadja, az ellen semmi esélyük nem marad a webről érkező támadóknak.

1 Előszó: Adatbiztonság és adatvédelem

Adatbiztonság és adatvédelem – egy nagyon tág területről van szó. A böngésző és az e-mail program kiválasztását ugyanúgy érinti, mint az adatmentés helyes stratégiáját, a spyware elleni védelmet, valamint a spam, a vírusok és a férgek elterjedésének megelőzését.

A biztonsági fal réseiről szóló jelentések nem akarnak megszűnni: egyszer az Internet Explorerben találkozunk hamis szervercímmel **(www.zapthedingbat.com/security/ex01/vun1.htm)**, ami ellen egy biztonsági frissítés nyújt segítséget, azután az F-Secure jelenti, hogy a vírusszkennelő programja bizonyos körülmények között nem ismer fel egy Sober-férget, ezért azonnal játsszuk be a legújabb patch-et **(http://-support.f-secure.com/enu/corporate/downloads/hotfixes/av5-hotfixes.shtml)**, vagy egy támadó a Windows XP Support Centerének egy résén keresztül scripting kódokat futtathat **(www.microsoft.com/germany/ms/technetservicedesk/bulletinMS04-015.htm).**



Az F-Secure-tól patch-et tölthetünk le vírusszkennelőjéhez

Szinte senki sem ismeri ki magát teljesen. Mi segíthet? Talán a radikális megoldás, nevezetesen, hogy félre a Windows-zal, elő a Linuxot? Csak részben: hiszen néhány program nem létezik a szabad operációs rendszer alatt, másrészt pedig ott sem állandóan felhőtlen az égbolt. Ezt bizonyítják például a Debian szerverre irányuló múlt év novemberi támadások **(www.debian.de/News/2003/20031121)**. A Linux alatt azonban mégis vidámabb az élet, mert itt a vírusok általi támadásokat éppen oly kevésbé ismerik, mint a betárcsázó vagy a spyware programokat.

2003 novemberében a Debian szervert is megtámadták. Erről az interneten részletesen is olvashatunk

A Linuxnak három nagy előnye van a Windows-zal szemben: nem annyira elterjedt – egy Sasser-féreg a Windows alatt sokkal nagyobb nyilvánosságot vonz –, a rendszergazda és a felhasználó közötti szétválasztás sokkal konzekvensebb, és a programok sokasága miatt a támadás nem lehet mindenre kiható.

De a Windows alatt sem keletkezhetne annyi kár, ha a felhasználók viselkedése megfelelő lenne. Az alábbiakban összeállítottunk néhány megszívlelendő jó tanácsot.

– Aktiváljuk a számítógép biztonsági funkcióit: jelszavas védelem, jelszavas képernyőkímélő, stb.

– Használjunk antivírus-programokat.

– Aktiváljuk az Intézőben az összes fájltípus megjelenítését.

– Aktiváljuk a makróvírus elleni védelmet a Wordben, a PowerPointban, az Excelben stb., és ügyeljünk a figyelmeztető jelentésekre.

– Állítsuk be az internetböngészőnk biztonsági beállításait a legmagasabb fokra: a Javát, a JavaScriptet, és az ActiveX-et éppúgy kapcsoljuk le, mint a script nyelveket (Visual Basic Script).

– Azonnal, megnyitás nélkül töröljük ki az idegenektől származó nyilvánvalóan nem fontos e-maileket.

– Legyünk óvatosak a hasonlóan hangzó tárgyú többszörös e-mailekkel is.

– Ne kattintsunk duplán a futtatható programokra (*.com, *.exe) vagy script nyelvekre (*.vbs, *.bat). Szintén vigyázat az Office fájlokkal (*.doc, *.xls, *.pps), valamint a képernyővédőkkel (*.scr).

– Csak a megbízható e-mailek csatolt fájljait nyissuk meg.

– Semmiképpen ne küldjük HTML formátumban e-maileket.

– Ne küldjünk vicces programokat vagy hasonlókat tartalmazó felesleges e-maileket, mert ezek esetleg valamilyen számítógép-vírust tartalmazhatnak.

– Sose kövessük azokat a felhívásokat, hogy az e-maileket vagy a csatolásokat küldjük tovább barátainknak, ismerőseinknek vagy kollégáinknak.

Sokakat bosszantó probléma a spam. Ezek a levélszemetek annál jobban szaporodnak, minél több e-mail cím létezik. Ezekre is létezik néhány alapvető szabály, amelyekkel legalább lelassíthatjuk a spamet, azonban nem akadályozhatjuk meg:

– Csak annak adjuk tovább e-mail címünket, akit ismerünk.

– Honlapunkon grafikaként mentsük el e-mail címünket.

– Hozzunk létre egy második e-mail címet az olyan listák és internetoldalak számára, ahol meg kell egyet adnunk.

– Ne válaszoljunk a reklám mailekre.

– Használjuk a szolgáltató spam elleni védelmét (sajnos gyakran ez nem ingyenes).

– Használjunk szűrőt e-mail programunkban.
– Ne dőljünk be a hamis Tárgy soroknak.

Amennyiben ezekből a jó tanácsokból kialakítjuk saját viselkedési szabályainkat, bár nem vagyunk minden veszély ellen felvértezve, mégis jóval nyugodtabban kapcsolhatjuk be a számítógépet. Hogy milyen további intézkedésekre és kiegészítő programokra lesz még szükségünk, azt kiskönyvünkből tudhatják majd meg.

Amennyiben döntöttünk egyik vagy másik program mellett, megkezdődhet a munka, hiszen nagyon fontos ezek helyes beállítása, és a mindenkori aktuális szinten tartásuk.

2 Spam és antispam

Senkinek sem kellenek, és mindenki ismeri a problémát: a reklám-mailek elárasztják a bejövő postafiókokat. Tíz üzenet közül nyolc spam. Ebben a fejezetben szót ejtünk a spamküldők trükkjeiről, és bemutatunk néhány olyan eszközt, amelyek valóban segítenek ellenük.

A nem kívánatos reklám mailek előfordulása az elmúlt tizenkét hónap alatt jelentősen megnőtt. Természetesen nem azért, mert a szörfölők szeretnek reklámot kapni – a küldő számára ez egyszerűen olcsó módszer arra, hogy potenciális ügyfelek millióit érjék el. És ha a címzetteknek csupán egy töredéke szánja rá magát a vásárlásra, már meg is érte a spam mail elküldése.

Eugene Kaspersky, az antivírus-kutatás vezetője az Oroszországban székelő Kaspersky-Labs nevű számítógépes biztonsági cégnél, úgy becsüli, hogy 2004 tavaszán az összes bejövő üzenet közel 60-70%-át tették ki a spam mailek. Olyan becslések is léteznek, amelyek szerint a spam mailek aránya az e-mailek között még ennél is nagyobb.

Aki egyszer felkerült a spamek listájára, az aligha menekülhet meg az adatszemét elől – így néhány felhasználó postafiókjában akár napi száz vagy akár annál is több kéretlen küldemény landolhat. A magánfelhasz-

nálók esetében ez zavaró, a vállalatok számára mindenekelőtt drága, hiszen az alkalmazottaknak meg kell szabadítaniuk bejövő postafiókjaikat a lomoktól, ami viszont költséges, lévén, hogy a munka addig nem igazán produktív. Egy nemrégiben napvilágot látott számítás szerint egyedül az EU-nak évi 2,2 milliárd euróba kerül, hogy azonosítsa és megsemmisítse az elektronikus szemetet.

2.1 Spamküldők trükkjei

A spamipar állandóan innovatív utakon jár, hogy az egyre jobb szűrőket kicselezze és mégiscsak kézbesítse az elektronikus szemetet. Ezeknek a trükköknek néhánya nagyon cseles és ezért sikeres, mások pedig csak annak a megállapításában segítenek, hogy az üzenet valóban elérte-e a címzettet. Egy biztos: a spamküldők fogásai még a legjobb eszközöknek is megnehezítik a nem kívánatos küldemények felismerését.

2.2 Nyitott kapuk

Gyakran alkalmazott trükk az *open relay*-ek és a *proxy szerverek* használata a küldő címének eltakarására.

Az *open relay*-ek mailkiszolgálók, amelyeken keresztül a spamküldők előzetes felhasználói bejelentkezés nélkül, ismeretlenül, tömeges e-mailek elküldésére képesek, legalábbis addig, amíg a szolgáltató és az antispam rendszerek fel nem fedezik és le nem zárják ezek IP címét.

A proxyk olyan szerverek, amelyek köztesen mentik el a HTTP-kapcsolatokat, ezáltal az ugyanazon cím utáni ismételt lekérdezések gyorsabbak. Néhány azonban protokollokat is továbbít, például az SMTP-t, és így visszaélhetnek velük a küldő címének névtelenné tételében.

Ezért a spamküldők állandóan új, védtelen relay-ek és proxyk után kutatnak, hogy felhasználják ezeket a névtelen reklámküldésben. Sajnos még manapság is elegendő nem szakszerűen konfigurált rendszer létezik, amelyek könnyen áldozatul esnek a spamprofiknak, és így életben tartják a spamproblémát.

2.3 Láthatatlan bogarak

A spamküldők kedvelt trükkje az úgynevezett *web bug* (web bogár) bevetése a használt e-mail címek hitelesítésére. A web bug egy apró grafika, tipikusan 1×1 pixel méretű, amely egy e-mail üzenetben rejtőzik. A trükk: mielőtt megjelenhetne a grafika a mailprogramunk előzetes ablakában, azt először le kell hívnia a szervernek. Ebből a lekérdezésből tudja a reklámozó, hogy a mailcím létezik, amelyet ezentúl bátran bombázhat adatlomjaival.

2.4 Ellenintézkedések

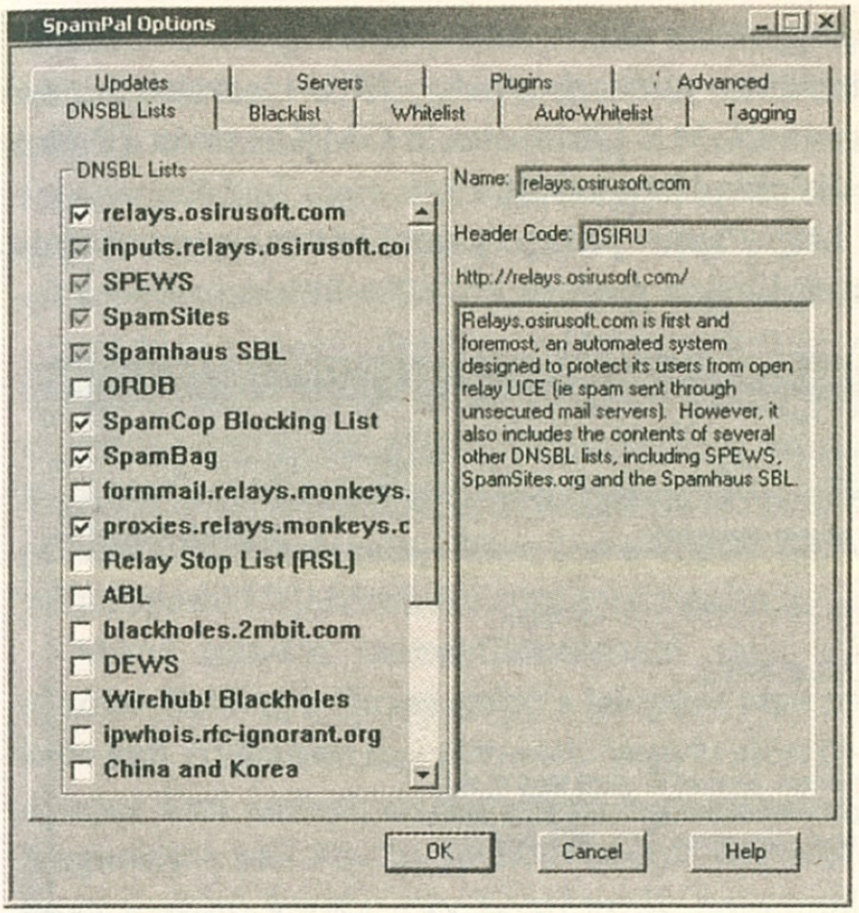
A spam maileknél egyvalami igazán bosszantó: amennyiben mailbe követeljük a spamküldőtől címünk törlését az adatbankból, az csak olvasási visszaigazolásnak számít, és senki sem veszi figyelembe. Vagyis az egyszerű lemondás nem működik. Egy jó szűrő azonban elűzi a szemetet a postafiókból. Megmutatjuk, hogy miként védhetjük és óvhatjuk magunkat hatékonyan és felfedjük a spamküldők trükkjeit.

A legegyszerűbb megoldást – a szabályon alapuló szűrő létrehozását az Outlookban – akár meg is spórolhatjuk magunknak: ez a változat túl pontatlan és nagyon sok spamet beenged a postafiókba. A kezelése pedig elég időigényes, mivel állandóan módosítani kell a szűrőt. Ráadásul az időbeni ráfordítás sem sokkal alacsonyabb az e-mailek manuális törléséhez képest.

2.5 Fekete listán az ismert spamküldők

Az Outlook fedélzeti eszközénél jelentősen jobb hatékonysággal működnek az úgynevezett feketelista-szűrők, mint például a *SpamPal*, a *SpamAssassin* vagy a *MailWasher*.

A spam elleni védelem ezen fajtája esetében egy szűrő figyel a helyi e-mail kliens és a szolgáltató mailszervere között úgy, hogy minden üzenet átmegy a feketelista szűrőjén. A reklámszita feladata: egyezteti a beérkező leveleket több DNSBL szerver adatbázisaival (a DNSBL a DNS-en alapuló Blacklistet – fekete listát – jelenti), amelyek mindenki számá-



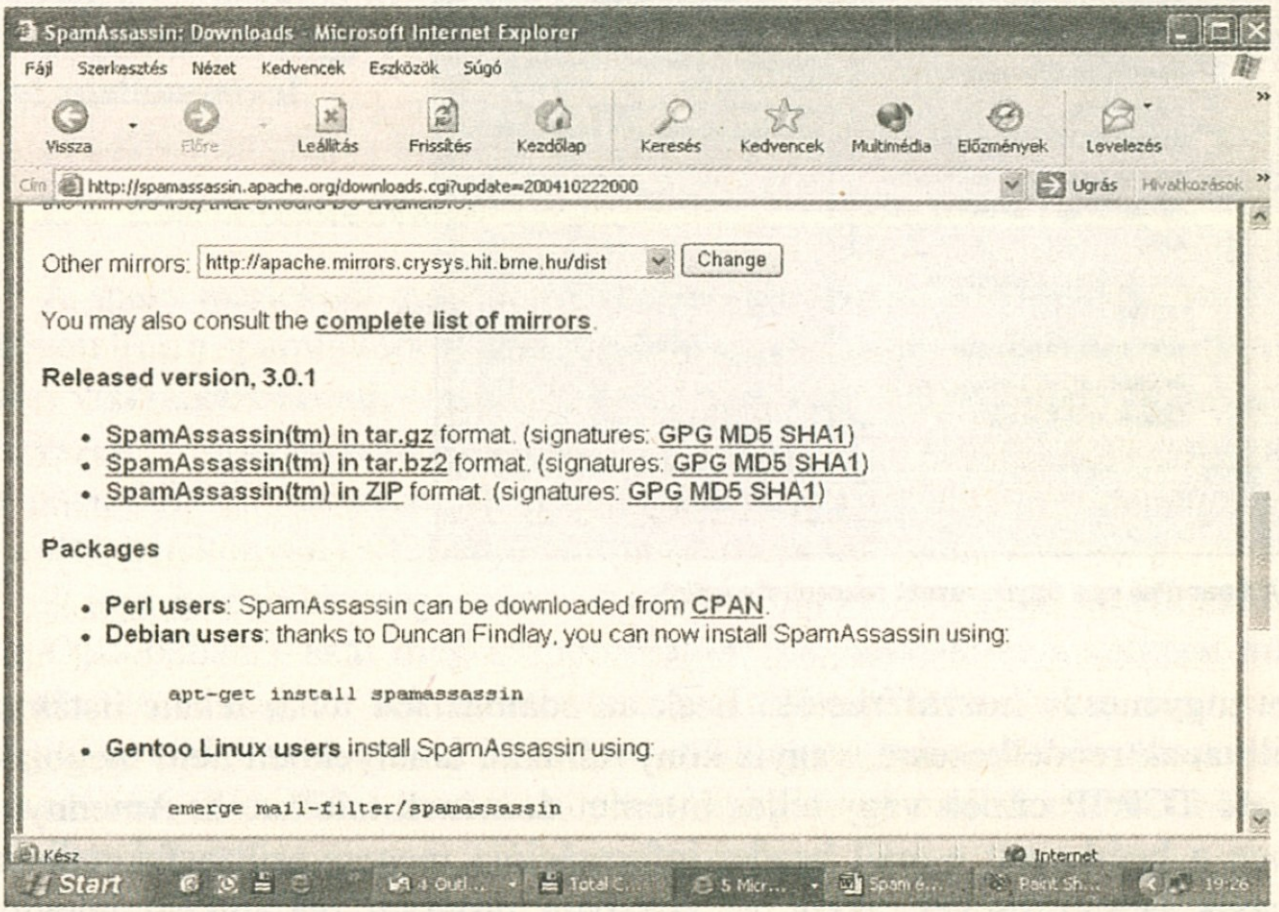
A SpamPal egy úgynevezett feketelista-szűrő

ra ingyenesen hozzáférhetők. Ezek az adatbázisok tehát fekete listákat állítanak rendelkezésre, vagyis könyvtárakat, amelyekben nem megbízható TCP/IP címek vagy teljes internet domének találhatók. Amennyiben a beérkezett e-mail header-információja megegyezik a feketelista egyik bejegyzésével, akkor az antispam program reklámként jeleníti meg az üzenetet.

Ez az eljárás magasabb találati aránnyal dicsekedhet, mint az e-mail kliens általi szűrés, azonban a hiba valószínűsége is nagyobb. Ennek az az oka, hogy mivel az összes üzenet egyeztetésre kerül a fekete listával, megtörténhet, hogy egy „tiszta" üzenetküldő is felkerül egy ilyen listára, és így a várt e-mailek is spamként szerepelnek. Így járt egyszer a GMX mailszerver is, amely egy hibás konfiguráció miatt az egyik fekete listára került. Hirtelen a GMX ügyfelek rengeteg levele nem érkezett meg a címzettekhez, és a mailszerver nem kis fáradságába került, amíg megszüntette az antispam adatbázisba történő bejegyzéseket.

A lehetséges hibás bejegyzések oka: a fekete listák gyakran az internetes szörfözők jelentéseire támaszkodnak. Mivel azonban sok internetező spamnek tekinti a GMX körlevelet, a GMX szerver IP címe szintén a fekete listára és blokkolásra került.

Ingyenes eszközök: **http://spampal.spxy.net, www.spamassassin.org, www.mailwasher.net**. Ezek a spamek kb. 80%-át kiszűrik.



Erről az oldalról tölthetünk le spamszűrőket

2.6 Tanulékony spamblokkolók

A fekete és a fehér listák szűrése annyira sikeres, mint a lekérdezett DNSBL rendszerek minősége, de persze az adatbázisok nem alkalmazkodnak személyes mailmennyiségünkhöz. A legjobb eredményeket a tanulékony spamszűrőkkel érhetjük el, amelyek a *bayes-i teóriának* megfelelően a valószínűségszámításon alapulnak (*Thomas Bayes* angol matematikus volt).

Ez bonyolultabbnak tűnik, mint amilyen valójában: a Bayes-szűrők abból indulnak ki, hogy az e-mailben található minden egyes szó valamilyen előfordulási valószínűséggel rendelkezik. A „Viagra olcsón" kifejezés például nagy valószínűséggel spam mailnek számít, míg a „tegnap az olasznál ebédeltem" mondatrész szinte biztosan egy magánjellegű levélben fordul elő. A szabályok segítségével, amelyeket Bayes határozott meg a maga idejében, a Bayes-szűrő kiszámítja a teljes valószínűségét annak, hogy az üzenet spam-e avagy sem. Minél egyértelműbben mutat az egyik irányba a valószínűség, annál bizonyosabban lehet az üzenetet pozitívként, illetve negatívként osztályozni. Csak ha nem állapítható meg tendencia, akkor lép a képbe egy szófilter, amely azután tipikus spamkifejezéseket keresve vizsgálja át az üzenetet.

Mivel minden internetfelhasználó saját világnézettel rendelkezik a spamet illetően, a Bayes-szűrő a telepítés után még nem tudhatja, hogy miként kell értékelnie egy üzenetet. Vagyis először meg kell ismernie a tulajdonosa által kedvelt és elutasított fogalmakat. Ez annyit jelent, hogy saját magunknak kell kb. 20-30 elektronikus üzenetet „spam"-nek kikiáltanunk, hogy a szűrő kapjon egy képet arról, hogy melyek a kívánt és melyek a nem kívánt üzenetek. Az így kapott első lecke után a Bayes-szűrő már 80-90 százalékos valószínűséggel felismeri a várt és nem várt leveleket. Ehhez felépít egy adatbázist, amelyben súlyozva szortírozza a megtalált szavakat.

Így lehetséges azután, hogy a tanulási fázisban használt üzenetek elemzése azt adja ki, hogy a „Sex", a „Viagra", az „Enlargement" vagy a „Money" kifejezéseknek nagyon magas a spamvalószínűségük, míg a „munka", a „megbeszélés", a „mozizás" szavak inkább egy nem spam üzenetre utalnak.

A szűrő az összes további spamelemzésnél összehasonlítja az e-mail szavait az adatbázisába mentett kifejezésekkel, és a nyert ismeretek összegéből kiszámítja a teljes valószínűséget. Ami a legjobb: a Bayes-szűrő állandóan tovább tanul. Az előforduló hibáknál egyszerűen javítsuk ki a besorolást: a jól edzett rendszer akár 99%-os találati eredményt is elérhet. Az állandó tanítgatás emellett az úgynevezett „False Positives" felbukkanását is lecsökkenti, vagyis az olyan e-mailekét, amelyeket meg szeretnénk kapni, de egy hibás interpretáció végett a szűrő spamként sorolja be őket.

Sajnálatos módon azonban a spamküldők is ismerik a szűrő működésének módját, és egyre újabb taktikákkal próbálják meg összezavarni ezeket a spamvadászokat.

2.7 A Bayes-szűrők edzése

Az edzett Bayes-szűrő jó spamblokkolóként szolgál. Az alábbi tippek abban segítenek, hogy optimálisan „képezzük ki" a szűrőnket.

Gyűjtsünk össze egy szolid kiindulási alapot a tanulási folyamathoz, amelyet válasszunk szét jó („ham") és rossz („spam") üzenetekre. Indulásként elegendő kb. 30 üzenet.

A megfelelő és a nem kívánatos e-mailek aránya lehetőleg legyen egyforma.

Korlátozzuk körülbelül ezer e-mailre a szűrő adatbázisát, mert a túl nagy tartalom csak lelassítja a rendszert, de nem ér el jobb felismerési arányt.

Ha a jó és a rossz e-mailek szűrésekor a program hibát vétett, a hibát azonnal javítsuk ki az antispam programunkban, és semmi esetre se hagyjuk javítatlanul. Ellenkező esetben a szűrő rossz példák alapján tanul.

Amennyiben fontos számunkra a sebesség, töröljük rendszeresen a szűrő adatbázisát, majd ezek után tanítsuk újra, mivel a spam üzenetek karakterisztikája is változik.

Állandóan tanítsuk a szűrőt úgy, hogy a hibásan osztályozott e-maileket a helyes csoportba helyezzük át. Csak így képes a rendszer gyorsan reagálni a spamre. Különben ismét egyre több reklámüzenet csúszik majd be a postafiókunkba.

2.8 Álirodalom bújtatja a spamet

Éppen a tanulékony Bayes-rendszerek kicselezése miatt egyre több spam mail tartalmaz néhány mondatot, amelyek teljesen értelmetlen szavakból vannak összetákolva. Az ok: mivel a Bayes-szűrők elemzik az üzeneteket, és az előforduló szavak alapján számítják ki a spamvalószínűséget, az ilyen értelmetlen, azonban szándékosan elhelyezett szómezők, amennyiben nem tipikus spamszókincsből állnak, csökkentik

a felismerési arányt. A szűrők ilyenkor inkább személyes kommunikációnak tartják és átengedik az ilyen üzeneteket.

Azonban a személyes e-mailek kritériumai minden felhasználó esetében különbözőek, a betanított Bayes-szűrőtől függően. Ezért a szűrő speciálisan kondicionálható erre a zavarkeltő stratégiára. Ráadásul ezek az értelmetlen szólisták azonnal feltűnnek olvasás közben. A spamküldők időközben rákényszerültek arra, hogy ezeket a részeket az éppen használt háttérszínbe bújtatva formázzák.

Különösen gonosz ebben a stratégiában, hogy a megfelelő spam gondoskodik arról, hogy azokat a szavakat is, amelyek a magánjellegű üzenetekben fordulnak elő, a szűrő gyanúsnak érzékelje, és így a magán üzeneteket is relám mailnek sorolja be („False Positives").

2.9 Peer-to-peer koncepciók a spam mailek ellen

A nem kedvelt reklámüzenetek időközben olyan gyorsan terjednek, hogy még a Peer-to-peer koncepciók is bevetésre kerültek a spamek elleni harcban. A programok, mint például a Cloudmark SpamNet vagy a Razor egyszerű elven működnek: valaki, aki felismer egy spam mailt, figyelmezteti a többi internetezőt.

Spamszűrés peer-to-peer alapokon

Egy spam üzenet általában több tízezerszer, de akár milliószor is elküldésre kerül ugyanabban a formában. Ez azt jelenti, hogy az e-mail tartalmán keresztül kiszámítható egy ellenőrzőszám, amely egyértelműen azonosítja a küldeményt. Amennyiben egy megfelelően felszerelt e-mail kliens minden új elektronikus üzenet számára ellenőrzőszámot képez, akkor ez a digitális ujjlenyomat összehasonlítható a központi antispam szerverben tároltakkal.

Amennyiben a tömegeknek szánt e-mail még ismeretlen, ezt egy tetszőleges internetező reklámként sorolhatja be, és ennek ellenőrzőszámát közölheti a szerverrel. Ez az eljárás mindenekelőtt azért működik ennyire jól, mert világszerte éjjel-nappal elárasztják a reklámüzenetek a felhasználókat, és ebből kifolyólag folyamatosan látják el ellenőrzőszámokkal az adatbázisokat. Ezzel a „közösségi gondozással" a nem kívánatos e-mailekről szóló információk szinte valós időben állnak rendelkezésre.

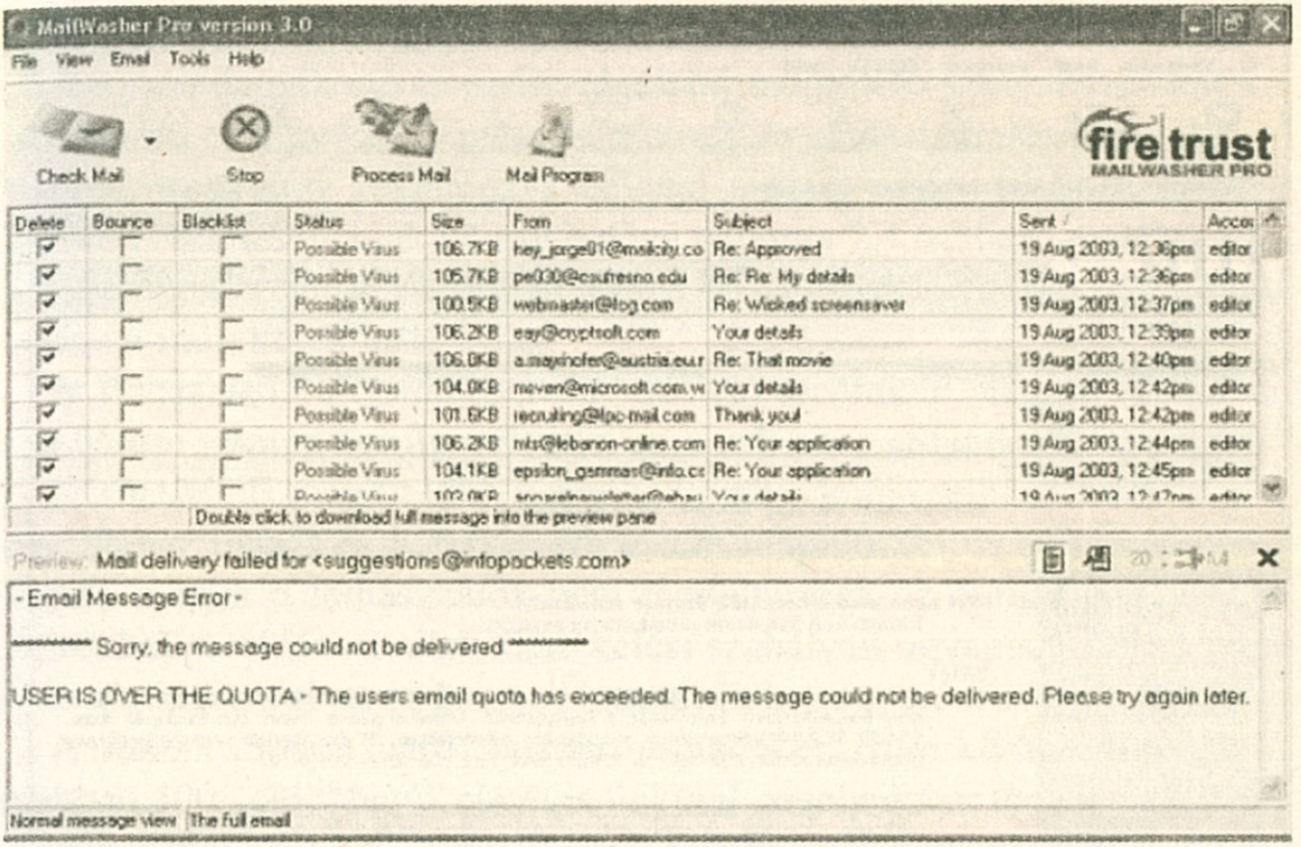
Ingyenes eszközök: **www.cloudmark.com, http://razor.sourceforce.net.** Az eszközök 95%-os biztonsággal szűrnek.

2.10 Új ötletek

Hogy úrrá legyenek a spamproblémán, a csavaros eszű felhasználók meglepő stratégiákat dolgoznak ki a probléma okozói ellen.

Érdekes kezdeményezéssel állt elő például a *MailWasher*: a *Bounce* funkcióval. A junk mailként felismert üzeneteket a program nem törli ki egyszerűen, hanem automatikusan visszaküldésre kerülnek a feladóhoz. A trükk: a spam mailre érkező válasz azt a látszatot kelti, hogy a megspammelt e-mail cím érvénytelen.

Amikor a reklám küldője kiértékeli a visszaérkezett e-maileket, azt gondolja, hogy a cím nem létezik, és ezért ezt ki kell törölnie az adatbázisából. Kívánatos mellékhatás: amennyiben elegendő felhasználó rendelkezik ezzel a Bounce funkcióval, megtörténhet, hogy a küldőt szintén több tízezer visszaérkező e-mail bombázza, és a mailszerver összeomlik a teher alatt. Azonban ez a funkció ártatlanokat is az idegösszeomlás szélére kergethet: a spamküldők ritkán küldik az üzeneteket a saját valós címük alatt, a legtöbb esetben hamisított a küldő címe. Így a visszaküldési hullám idegeneket is érinthet.



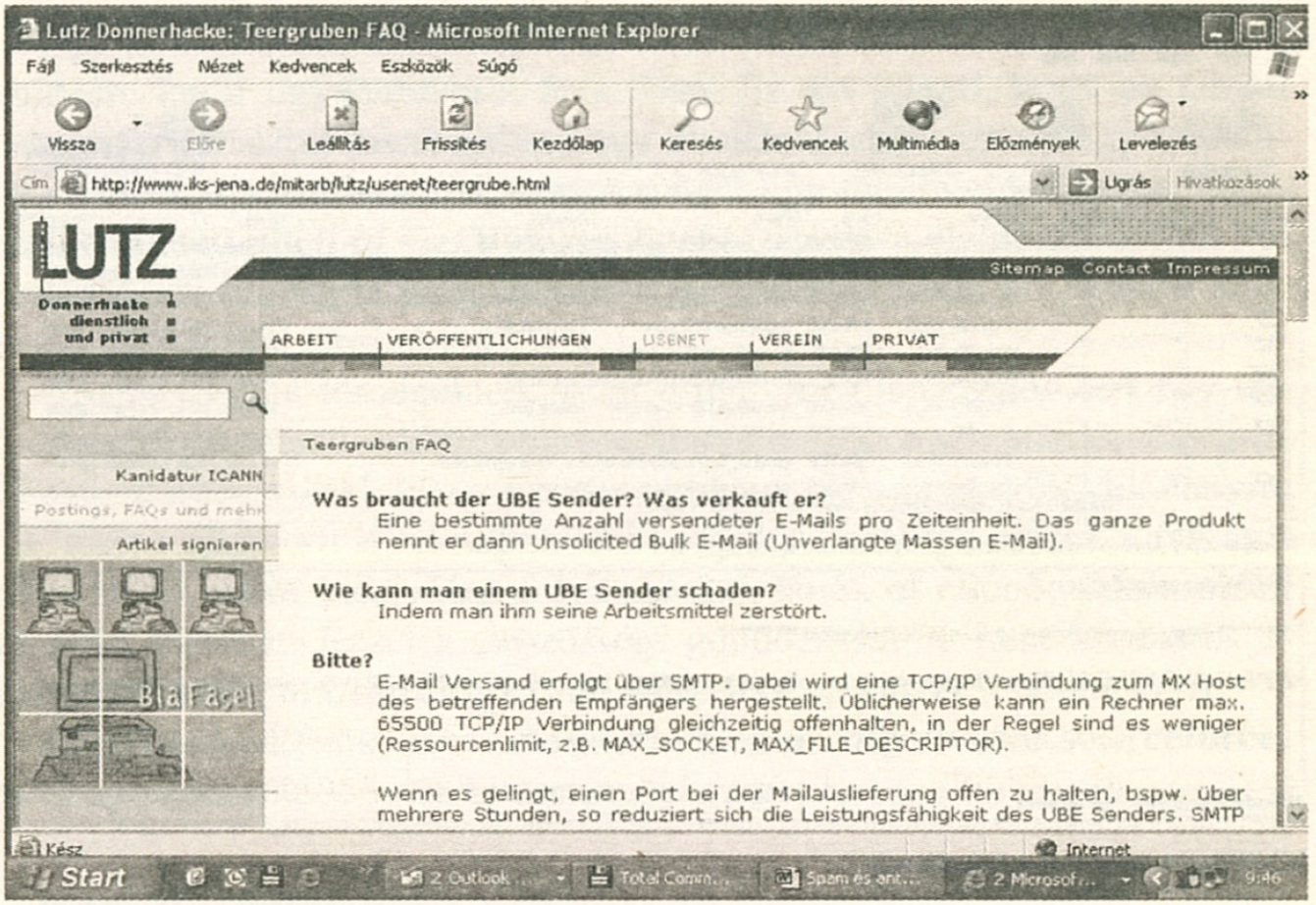
MailWasher: vissza a feladónak!

Ingyenes eszközök: **www.mailwasher.net**. A módszer 99%-os biztonságig szűr.

2.11 Saját mailszerver: hogy lophatjuk el a spamküldők idejét?

A szükséges tudással spamcsapdaként is beállíthatjuk a mailszervert, ilyenkor speciális parancsokkal egy reguláris SMTP kapcsolatot színlel, a tulajdonképpeni cél azonban az, hogy a túl sokáig nyitva tartott kapcsolatok által lebénítsák a spamküldők erőforrásait. Amennyiben a weben elegendő mennyiségű ilyen elven működő csapda létezik, a spamküldők SMTP-portjai foglaltakká válnak, anélkül, hogy akár egyetlen e-mailt is küldeni tudnának.

Az az elképzelés is roppant kreatív, hogy egy spam mailben található minden hivatkozást összehasonlítsunk a fekete listákkal, és egyezés esetén a bizonyos URL-t egyszerre többször is lehívjuk (*Filters that Fight Back)*. Ez hatalmas adatforgalmat generál a spam mail megbízójánál és a



Információk a spamcsapdáról, igaz, német nyelven

tulajdonképpeni spamokozónál, és mindkettőjük forgalomkiadásait megnöveli.

Ha csak minden tizedik felhasználó élne ezzel a módszerrel, a reklámok elküldőit hamarosan magas reklámköltségek terhelnék, azonban megrendelésre hiába várnának – ez is egy lehetőség ennek az üzleti modellnek a tönkretételére. Hogy részletesen hogyan működnek ezek a „visszaütő" szűrők, azt Paul Grahamtől tudhatjuk meg a **www.paulgraham.com/ffbfaq.html** oldalon.

További információk:

www.iks-jena.de/mitarb/lutz/usenet/teergrube.html

2.12 A szolgáltatói hozzájárulás

Nem mindenki akar, vagy nincs olyan helyzetben, hogy helyileg telepítsen egy spamszűrőt, vagy azt állandóan tanítsa. Ebben az esetben le-

hetőség nyílik arra, hogy átengedjük ezt a munkát a mailszervernek. Időközben mindegyik neves mailszolgáltató megfelelő szolgáltatásokat kínál, hiszen ez a funkció fontos marketing- és eladási stratégiává vált.

A Hotmail úgy reklámozza például a saját spamvédelmét, hogy a „szűrési technológiának köszönhetően naponta 2,4 milliárd nem kívánatos e-mail nem ér célba. Ez az MSN kiszolgálón keresztül továbbított összes e-mail kerek 80%-a."

A felhasználó a „SmartScreen" szűrési technikán alapuló szolgáltatást három szinten konfigurálhatja, amelyek neve „Standard", „Kiemelt" és „Exluzív". E mögött több technika kombinációja rejlik, többek között egy „fehér lista", és a Bayes-elméleten alapuló valószínűségszámítás. Sajnos maguk a felhasználók nem rendelkeznek az önmaguktól tanuló szűrőkkel, a reklám mailek kiértékelési szabályait ugyanis egész egyszerűen általánosságban az összes Hotmail fiókra egyaránt érvényesek.

A *Yahoo* „SpamGuard"-ja szűri a maileket. Ezen kívül a szolgáltató újabban 500 „eldobható" címet is felkínál, amelyek bár továbbítják a beérkező e-maileket a fő postafiókra, szükség esetén azonban azonnal kikapcsolhatók.

A *Freenet* viszont fekete listát használ a spamek blokkolására. Itt a védelem szintje egyénileg állítható be: a legalacsonyabb szinten azok az e-mailek blokkolódnak, amelyeket ismert feladók küldtek. A legmagasabb biztonsági szint viszont IP-alapon szűr, és az összes olyan e-mailt blokkolja, amelyek küldői már küldtek valaha is spamet.

2.13 A jövő: perek a spamküldők ellen

Sem a spamek okozóinak, sem az áldozataiknak nincs idejük arra, hogy kipihenjék magukat. Mindkét oldal állandóan újabb és újabb koncepciókat fejleszt ki, jól tudva, hogy soha senki sem nyeri meg a versenyt.

Mégis állandóan születnek új ötletek, mint például legutóbb a Microsoftnál, amely a „Caller-ID" által *saját antispam szabványt* szeretne bevezetni.

Itt az e-mail küldőknek a mailszerverük IP címét a Domain Name Systemben (DNS) egy speciális, a Microsoft által meghatározott formá-

tumban kell nyilvánosságra hozniuk. Az e-mail címzettek így ellenőrizhetik, hogy szerepel-e az elküldő mailrendszer a DNS-ben, és a küldeményt szükség esetén spamként sorolhatják be. Ez a módszer tulajdonképpen a már ismert fekete lista egy továbbfejlesztett változata.

De a kormányok is bekapcsolódnak a harcba. Az amerikai kongresszus az év elején elfogadta az *Antispam törvényt,* amely kemény intézkedéseket hoz a spamküldők ellen: hatmillió dollár értékig terjedő pénzbírság, vagy 5 évig terjedő szabadságvesztés. Az AOL, a Microsoft, az Earthlink és a Yahoo, a négy legnagyobb amerikai online szolgáltató, időközben az új törvény alapján több száz spamküldő ellen tett feljelentést.

Bár a konkurensek együttműködését a szükség szülte, ez már nagyon szükséges volt, hiszen a spamküldőknek teljesen mindegy, hogy kinek az ügyfeleit bombázzák reklámüzenetekkel. Ennek ellenére ez az együttműködés csak az első lépésnek számít, amennyiben a spamproblémát egy napon valóban meg szeretnék oldani: hiszen a legjobb törvények sem használnak semmit, ha a Viagra reklámmailje Indonéziából vagy a Kajmán Szigetekről érkezik.

2.14 Antispam: a legjobb szűrők

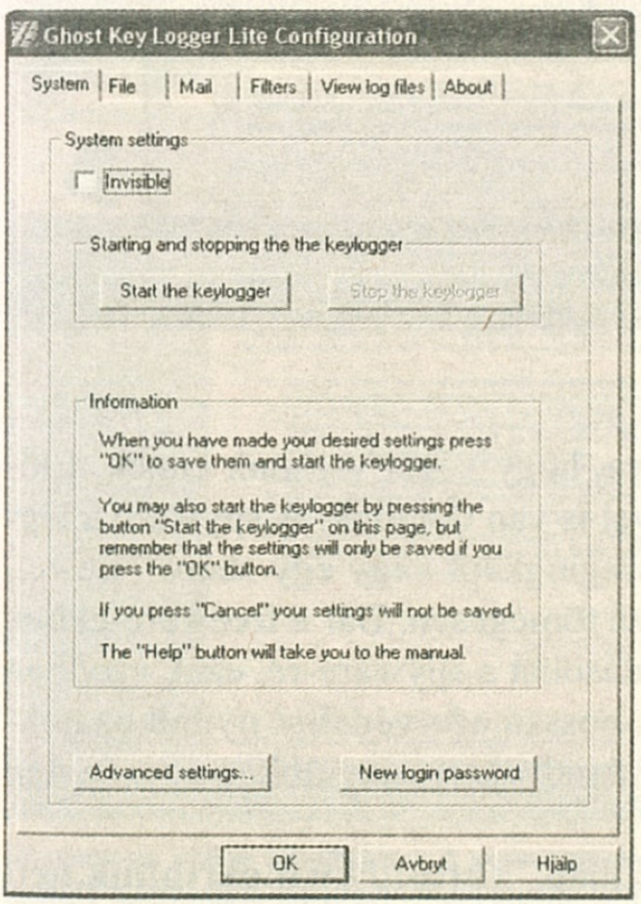
A Bayes-szűrők, mint láthattuk, a spam elleni harc különösen hatásos módszerének számítanak. Éppen ezért e fejezet végén összeállítottuk a legjobb freeware és Open-Source megoldásokat. Hogy miként integrálható a szűrő a rendszerünkbe, arról az illető weboldalakon olvashatnak.

Spamihilator (freeware): **www.spamihilator.com**
POPFile (Open Source): **http://popfile.sourceforge.net**
SpamBayes (Open Source): **http://spambeyes.sourceforge.net**
InBoxer (shareware, 23 euró): **www.inboxer.com**
Outclass (freeware): **www.vargonsoft.com**
Bogofilter (Open Source): **http://bogofilter.sourceforge.net**
Squirrelmail (Open Source): **www.squirrelmail.org**
Spammunion (freeware): **www.upserve.com**
K9 (freeware): **www.keir.net/k9.html**

3 Kémeszközök

A spyware vagy az adware a tudomásunk nélkül gyűjt információkat rólunk. Általában ezek az információk reklámcélokat szolgálnak, azonban másnemű információk is lehetnek. Ebben a fejezetben arról olvashatnak, hogy miként ismerhető fel a spyware, és hogyan szabadulhatnak meg tőle.

Adware-nek azokat a programokat nevezzük, amelyek információkat továbbítanak rólunk a számítógépünkön és szörfölési szokásainkon keresztül. Ez a legtöbb esetben a reklám célját szolgálja, és majdnem minden esetben a tudomásunk nélkül történik. Online vásárlás során megadjuk a hitelkártyánk számát, vagy kiválogatjuk a legújabb albumokat a még aktuális cserebörzéken? A kis alattomosak mindezt figyelemmel kísérik és késedelem nélkül jelentik.

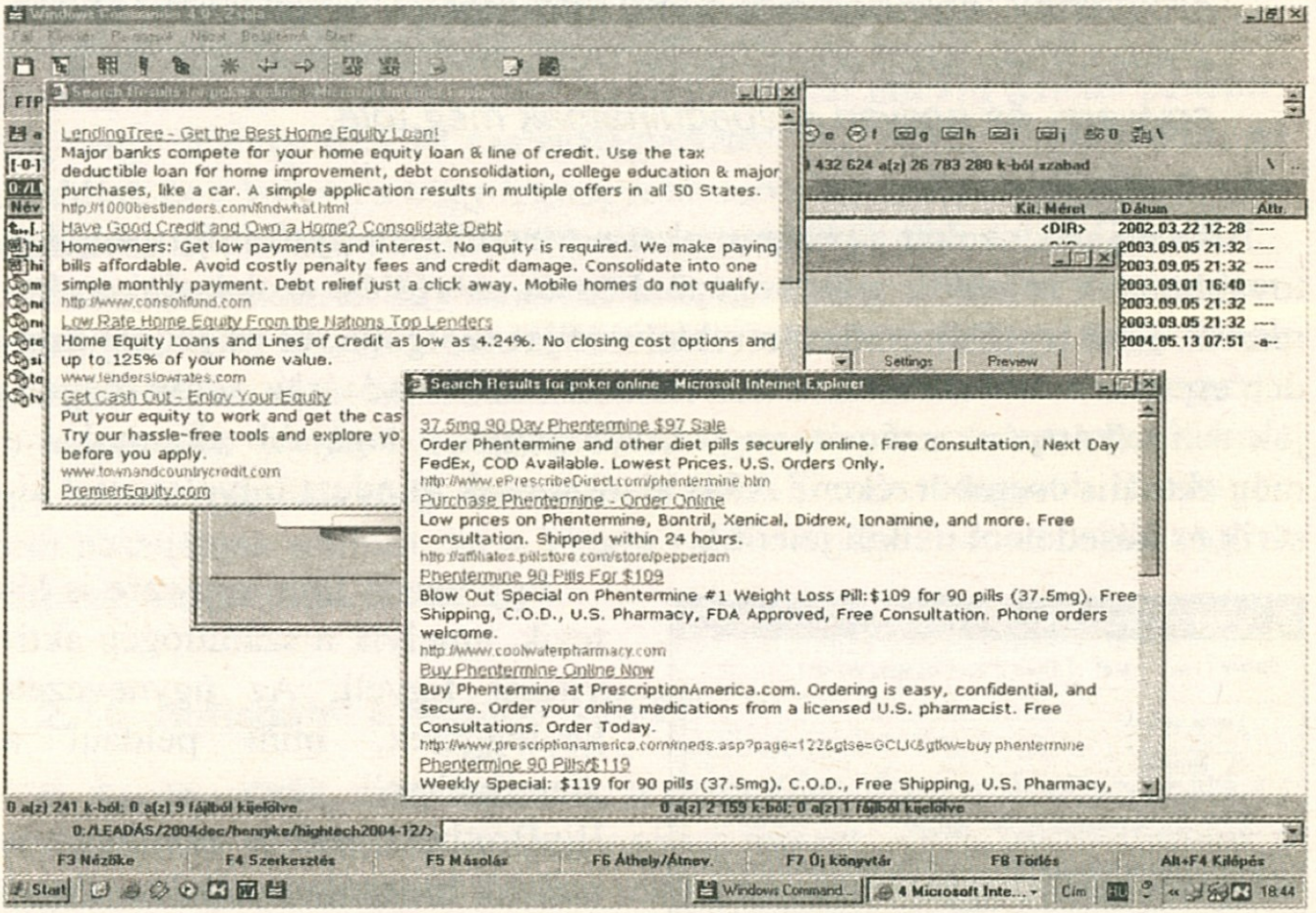


Munkában egy keylogger

Egy másik fajta spyware is létezik, amelyik a számítógép aktivitását figyeli. Az úgynevezett keyloggerek, mint például a „familyCam" vagy az „I am BigBrother", már a nevükben is utalnak használati céljukra. Ezzel munkatársak, gyerekek vagy élettársak figyelhetők meg titokban. Így lehetséges az e-mailek másolatának továbbítása a figyelőhöz, a chatelés feljegyzése vagy a köztesen bekapcsolt proxy szerveren keresztül lehívott internettartalmak láthatóvá tétele.

A spyware azonban más módon is kellemetlen lehet: a rendszer egészen a lefagyásokig ingataggá válhat, mert a spyware

programon keresztül bizonyos funkciók módosulnak. Általuk bejátszásra kerülnek a szörfölési viselkedésünkön alapuló popup és a banner reklámok, vagy a bizonyos tartalmak utáni keresést a program célirányosan más oldalakra téríti el.



Azok a bosszantó popup ablakok...

Mindez már elegendő ok lehet arra, hogy véget vessünk ennek. Először azonban tudnunk kell, hogy mivel is van dolgunk. A spyware a legtöbb esetben e-mailben, Instant Messagingként vagy egy shareware-rel, illetve freeware-rel érkezik, méghozzá tömegesen. Bár a freeware-ekben és a shareware-ekben találhatunk utalásokat a spyware-re, ezek azonban gyakran nagyon el vannak bújtatva a hosszú adatvédelmi nyilatkozatokban vagy a licencmegegyezésekben, amelyeken a legtöbben egyszerűen csak tovább kattintanak.

Az amerikai Earthlink szolgáltató **(http://www.earthlink.net/spyaudit/press/)** három hónapig tartó aktuális vizsgálata több mint egy-

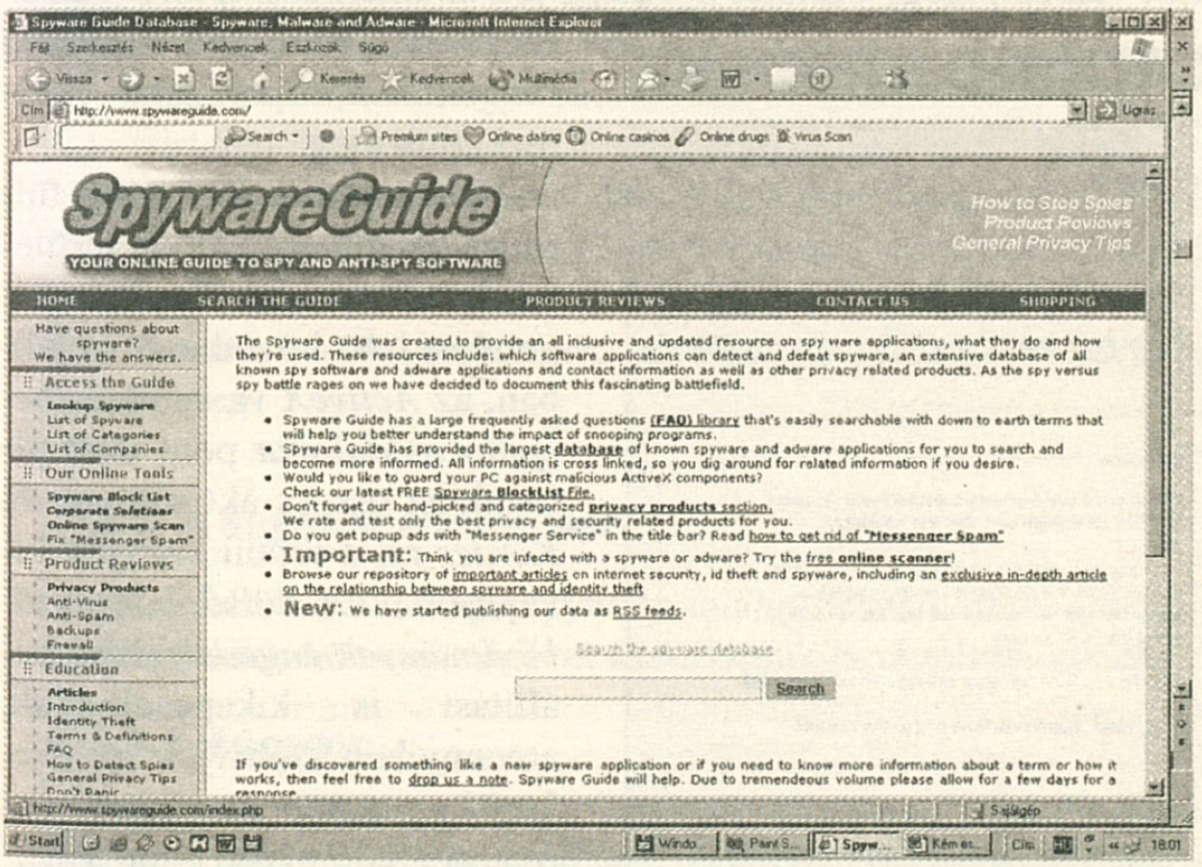
millió vizsgált PC esetében majdnem 30 millió spyware jelenlétét állapította meg. Ezek oroszlánrészét, majdnem 24 milliós részvéttel a cookie-k képezték, amelyek segítségével a marketingvállalatok átfogó felhasználóprofilokat hoznak létre, ötmilliót tettek ki a spyware programok, az adatokat feljegyző és továbbító trójai programok és rendszermonitorok száma pedig kétszázezerre rúgott.

3.1 Megelőző óvintézkedések az adatlopás ellen

Sajnos nincs más megoldás: önmagunknak kell segítenünk magunkon. A spyware megelőzésénél ügyeljünk a következő szabályokra:

– Sose nyissunk meg ismeretlen feladóktól származó hivatkozásokat az e-mailekben.

– Csak olyan programokat telepítsünk, amelyekre valóban szükségünk van.



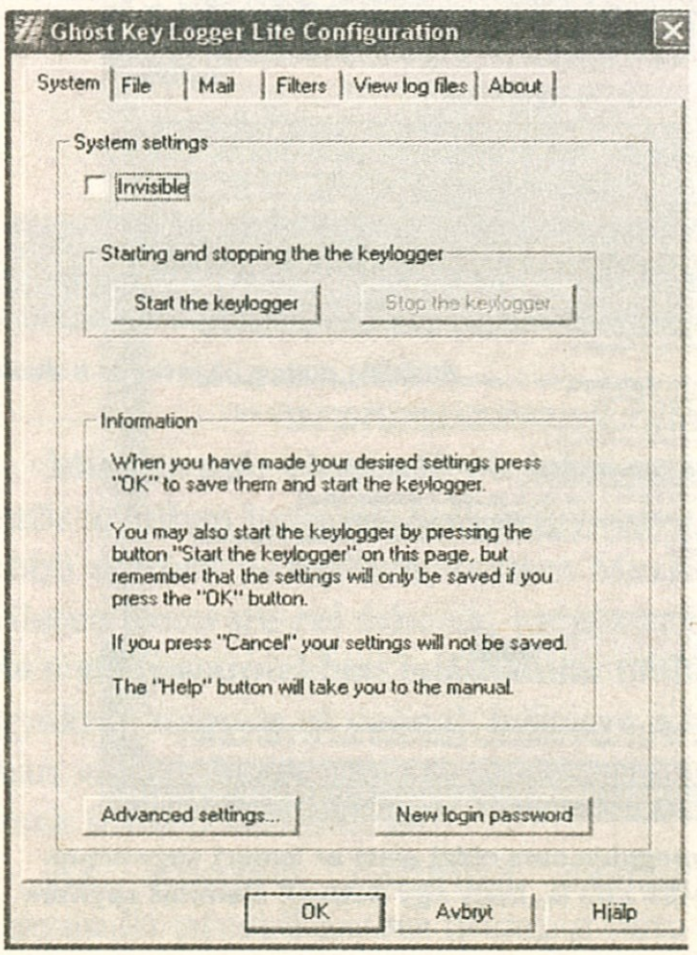
Spyware-ek online felkutatása: A www.spywareguide.com oldal alatt az ismert spyware-ek listáját találhatjuk, emellett lehetőségünk nyílik arra is, hogy egy ActiveX elemmel spyware programok után nyomozzunk

– A telepítés előtt olvassuk el a licencmegállapodást vagy az adatvédelmi irányvonalakat. Néhány gyártó ebben a lehető legkisebb feltűnéssel utal arra, hogy a programok mellett kiegészítésképpen spyware programok is települnek.

– Állítsuk be helyesen az Internet Explorer biztonsági beállításait, vagy használjunk másik böngészőt.

Mielőtt telepítenénk egy új programot, nézzünk utána, hogy ez spyware program-e. A több mint 400 programot tartalmazó spywarelistát a www.spywareguide.com oldalon találhatjuk. Itt lehetőségünk nyílik arra is, hogy egy ActiveX elem segítségével online spyware-ek után nyomozzunk.

A spyware-ek gyártói szintén az ActiveX elemet használják, amelyeket csak az Internet Explorer képes futtatni. Ennek megakadályozására meg kell tanítanunk az Internet Explorernek, hogy ne nyisson meg és futtasson mindent kérés nélkül, ami a webről érkezik – és ezek többnyire az ActiveX elemek. Hogy ezekkel mit csináljon az Internet Explorer, azt az *Eszközök* pont alatt található *Internetbeállítások* alatt határozhatjuk meg.



Váltsunk át a *Biztonság* fülre, válasszuk az *Internet* területet, kattintsunk az *Egyéni szint* gombra. A következő ablakban, az *ActiveX vezérlők és beépülő modulokat* pont alatt állítsuk az összes aktivált opciót *Kérdés*-re, a többit hagyjuk kikapcsolva. *A külső böngésző-bővítmények engedélyezése* beállítást is kikapcsolhatjuk, amennyiben előhívjuk az *Eszközök* menüpont alatt az *Internetbeállítások* pont *Speciális* fülét.

Még biztosabb a dolog, ha a

biztonsági beállításokat *Magas*-ra állítjuk. Ehhez válasszuk ugyanebben a párbeszédablakban az *Alaphelyzetek* listából a *Magas* bejegyzést, és ezután kattintsunk az *Alaphelyzet* gombra.

Azonban azzal is tisztában kell lennünk, hogy ez az intézkedés szörfölés közben korlátozásokhoz vezethet, és hogy bizonyos – kívánt – tartalmak többé nem jeleníthetők meg. Ezen kívül a biztonsági beállítások csupán az olyan spyware-ek megelőzésére szolgálnak, amelyek közvetlenül az interneten keresztül kerülnek telepítésre, de az olyan spywareekre nem, amelyek mondjuk egy szoftverrel kerültek a számítógépre.

3.2 Hogyan ismerhető fel a spyware?

Hogy van-e telepítve spayware a számítógépünkre, azt a megfelelő eszközök segítségével ellenőrizhetjük, és el is távolíthatjuk őket. Ha eddig semmilyen programot sem használtunk ellenük, bizonyos tünetek esetében kiindulhatunk abból, hogy számítógépünkön fut valamilyen spyware program. Lássuk ezeket!

– Megállapítottuk, hogy rendszerünk lassabban fut.

– Hirtelen megváltozik az internetböngészőnk indítóoldala.

– Új és ismeretlen ikonokat találunk az internetböngésző eszköztárában.

– A Windows Messenger Chat-programja állandóan reklámüzeneteket jelenít meg.

– Ismerős oldalakon hirtelen reklámot tartalmazó popup ablakok jelennek meg.

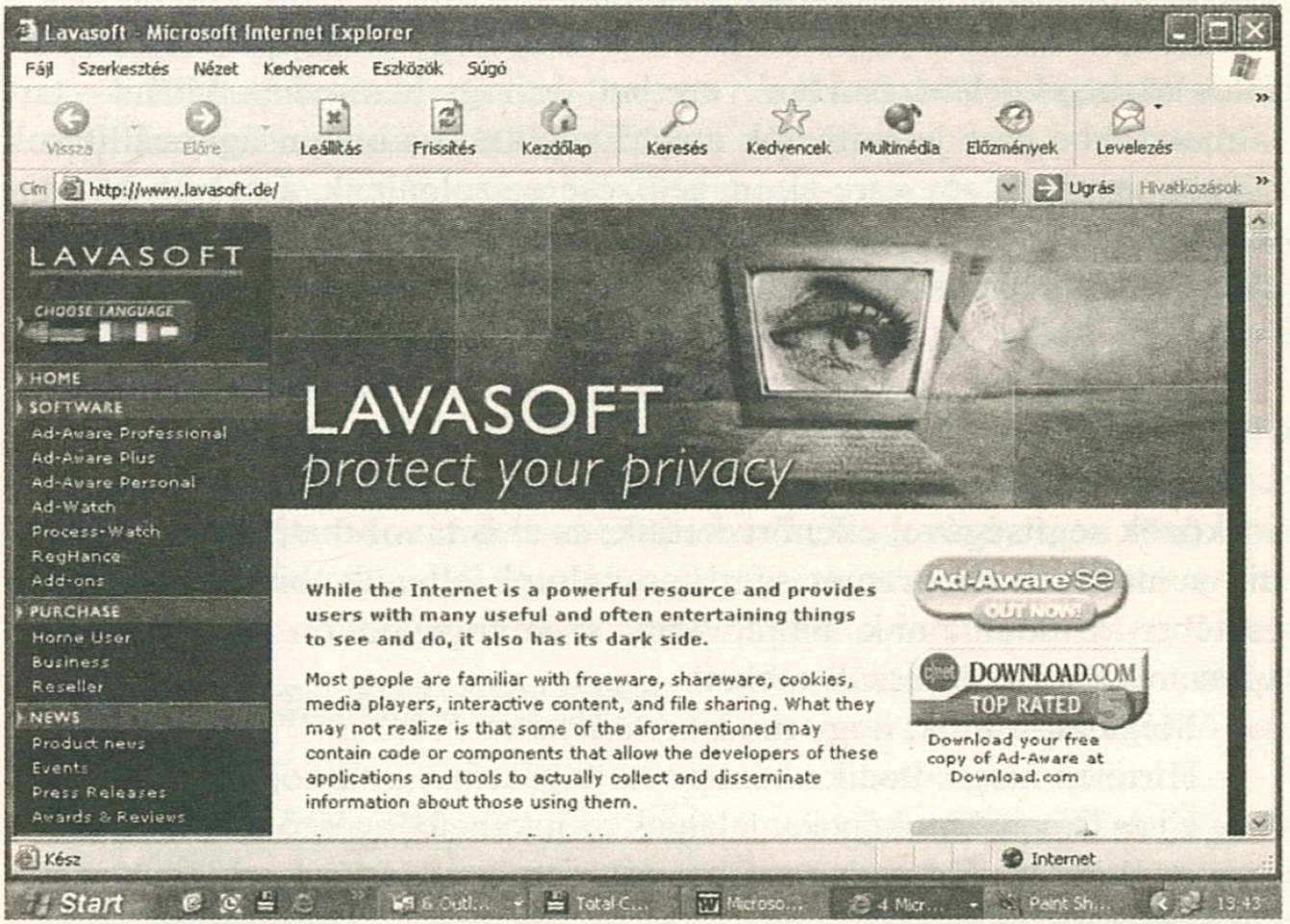
3.3 A spyware eltávolítása

Ha feltételezzük, hogy spyware található számítógépünkön, azt egy megfigyelőeszköz segítségével észlelhetjük és távolíthatjuk el.

3.3.1 Ad-aware

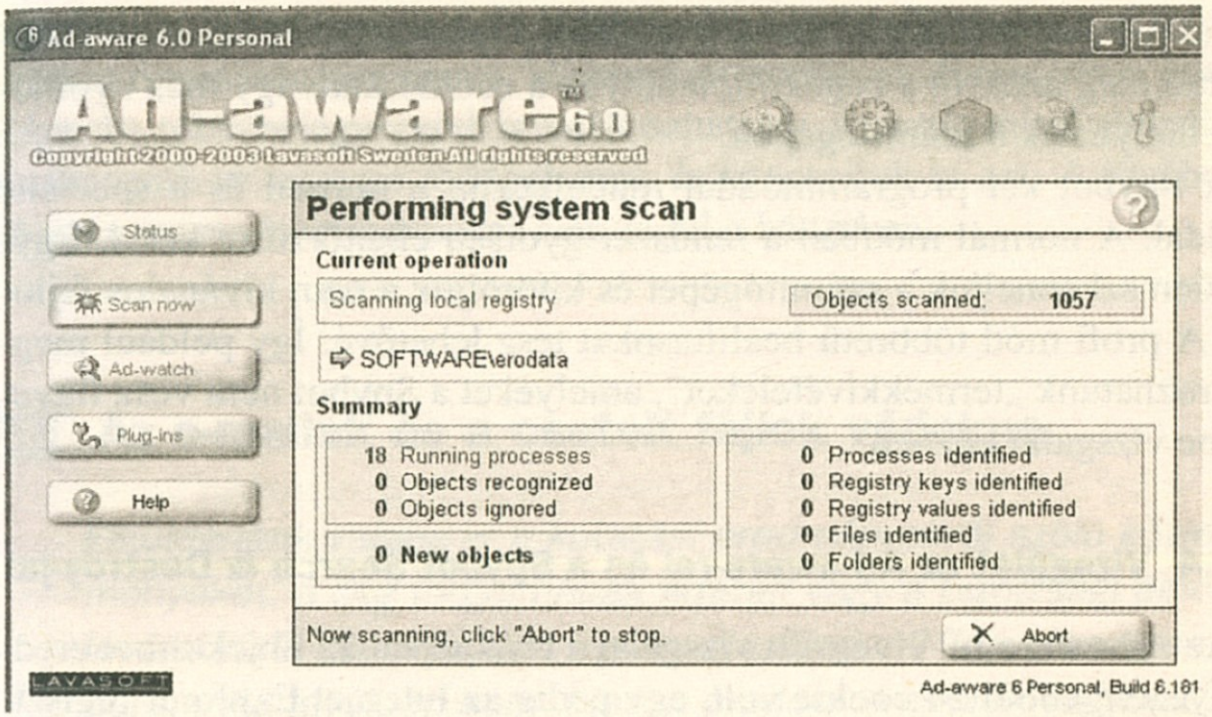
Az ilyen sorozat egy ismert eszköze a Lavasoft cég *Ad-aware* programja. A program ártalmas adatok, valamint reklámösszetevők után kutatja át a munkamemóriát, a regisztrációs adatbázist, a merevlemezeket és egyéb meghajtókat. E freeware-nek több verziója is létezik egészen

egy licenc verzióig, amely 40 euróba kerül: ezeket a **www.lavasoft.de** weboldal alatt tölthetjük le, vagy természetesen megvásárolhatjuk.



Innen érkezik a segítség

Kattintsunk a *Download* hivatkozásra, hogy letölthessük az Ad-aware freeware verzióját. A telepítés után a szoftver egy egyszerűen kezelhető felülettel jelentkezik, amelyen keresztül az egérrel az egész számítógépet átvizsgálhatjuk spyware vagy más ártalmas programok után. Kattintsunk a *Scan now (Vizsgálat most)* gombra a merevlemez szkenneléséhez. Végezetül a talált objektumok listájából egyes, vagy akár az összes elemet is karantén alá helyezhetjük. Ez azt jelenti, hogy ezek ezután semmilyen információkat nem képesek többé gyűjteni és továbbítani. Azonban ezeket a fájlokat szükség esetén újra vissza is állíthatjuk, mondjuk abban az esetben, ha az eltávolítás következtében valami nem működne megfelelően.



Az Ad-aware a számítógépet fürkészi

Az Ad-aware átvizsgálja a ZIP fájlokat, a futó folyamatokat, a regisztrációs adatbázist – beállítás szerint – és az Internet Explorer *Kedvencek* pontját is. A pénzbe kerülő verzióban ehhez az úgynevezett Ad-Watch funkció is hozzájön, amely például blokkolja a felismert folyamatokat.

Mielőtt átvizsgáljuk az Ad-aware programmal a számítógépet, ellenőrizzük először is, hogy létezik-e már egy új referenciafájl, mert ebben szerepelnek az ismert spyware-ek. Ezt a referencialistát, amely az összes verzióval működik, letölthetjük az internetről.

3.3.2 Spybot Search & Destroy

A *Spybot Search & Destroy* **(www.spybot.info)** is egy freeware. Ez az Ad-aware programhoz hasonlóan zavaró reklámmodulok és spyware-ek után vizsgálja át a rendszert. És – az Ad-aware-hez hasonlóan – a Spybot is rendelkezik egy frissítési funkcióval, amellyel letölthetők az aktuális felismerési szabályok. Emellett a Spybot több keresési és eltávolítási lehetőséget is kínál: az úgynevezett követő cookie-kon kívül a program a trójai, a hijacker, a tárcsázó és a keylogger programokat is felkutatja, és réseket keres a biztonsági falon.

Az Ad-aware programmal ellentétben, a felhasználó a Spybottól többet tud meg azokról a cégekről, amelyek a cookie-kat vagy más nyomokat elhelyezték a számítógépen.

A Spybot két programmóddal rendelkezik: a normál és a speciális móddal. A normál módban a rendszer gyorsan ellenőrzésre kerül. Egyszerűen szkenneljük a számítógépet és kitöröljük a nem kívánatos fájlokat. A profi mód többrétű beállításokat tesz lehetővé. Így például meghatározhatunk „termékkivételeket", amelyeket a Spybot nem vesz figyelembe vizsgálat közben.

3.4 Vizsgálat az Ad-aware-rel és a Spybot Search & Destroy-jal

Az Ad-aware-rel elvégzett vizsgálat a tesztgépen 25 objektumot eredményezett: ebből 24 cookie volt, egy pedig az Internet Explorer regisztrációs kulcsa, amely az *Eszközök* pont alatt az Alexa Botra utalt. Az Alexa híres az Alexa Toolbar Spyware-ről, amely adatokat gyűjt, bár hogy ez a keresőoldal esetében is érvényes-e, az nem biztos.

Az Internet Explorer ezen parancsát a Spybot Search & Destroy szintén megtalálta.

Az Ad-aware több cookie-t talál, mint a Spybot (13). Az Ad-aware-rel ellentétben a Spybot azonban még néhány DSO-Exploit-et is fellelt, amelyek hatásairól a **http://www.greymgic.com/security/advisories/gm001-ie/** internetcím alatt olvashatnak.

Összegzés: Mivel az Ad-Aware és a Spybot különböző problémákat fedeznek fel, tanácsos mindkét termék használata és ezekkel a számítógép időről időre történő ellenőrzése. Mivel a Spybot freeware és az Ad-aware-től is létezik egy freeware verzió, az egész nem kerül többe, mint a letöltési idő és egy kicsinyke hely a merevlemezen. Azonban minden vizsgálat előtt ellenőrizzük, hogy léteznek-e aktuálisabb felismerési listák, és töltsük le ezeket.

3.5 Profi tipp: a Windows Messenger teljes kikapcsolása

Amennyiben nem dolgozunk a Messengerrel, jobb, ha ennek előhívását már a rendszerindításkor megakadályozzuk. Ehhez hívjuk elő a *Start*

menüben a *Futtatás* pontot, és indítsuk el az *msconfig* paranccsal a rendszerkonfigurációs programot. Váltsunk át azután az *Automatikus indítás* fülre. Itt több bejegyzéssel is találkozhatunk, és ezek mind aktiváltak. Kattintsunk az *msmsgs* indítóelemre, és kapcsoljuk ki azt. A jövőben a Messenger rendszerindításkor nem indul a háttérben.

4 Az e-mailek és a csatolt fájlok védelme

Elküldenénk valaha is a kutatási eredményekről szóló közleményeket, a cég forgalmának adatait vagy a bizottsági elnök leváltásáról szóló híreket egy levelezőlapon? Természetesen nem, még levélben sem, hiszen modern emberek vagyunk, és ezért mindent e-mailen keresztül bonyolítunk – annak ellenére, hogy a kódolatlan e-mail sem jobb semmivel sem egy levelezőlapnál. Ebben a fejezetben az e-mailek és csatolt fájljaik védelméről szólunk.

A kódolatlan e-mailek megörvendeztetik a gazdasági kémeket: csak a számítógép előtt kell ülniük, és elfogni az üzeneteinket. Ez sokkal egyszerűbb, mint a postai levél átvizsgálása. És gazdaságosabb is, hiszen az üzenetet gyorsabban átmásoljuk, mint ahogy a levelet átírjuk. Ez ellen csak egy jó kódolószoftver nyújt segítséget.

Nos, a GnuPG megbízható kódolószoftvernek számít, méghozzá jó okkal: szabad szoftver, és a *GNU General Public Licence* alatt áll. A szabad szoftvereket mindenki a saját belátása szerint használhatja, testre szabhatja és a testre szabott verziót szétoszthatja.

Így volt ez a *PGP (Pretty Good Privacy),* az 1990-es évek kódolási szabványa esetében is. *Phil Zimmermann,* a PGP feltalálója 1996-ban megalapította cégét, amelyet 1997-ben átvett a *Network Associates.* 2001-ben Zimmermann elhagyta a céget. A Networks Associates sikertelen próbálkozásokat tett arra, hogy pénzt keressen a PGP-vel, és egy évvel később eladta azt a frissen alapított *PGP Corporation* nevű cégnek.

Időközben meghonosodott a GnuPG, amelynek működéséről a következő oldalakon bővebben is írunk.

A GnuPG 1.0 verziója 1999 óta létezik a Unix-kompatibilis operációs rendszerek számára. Azóta már több összetevője is napvilágot látott:

– GnuPG: A GNU Privacy Guard szoftver kódolja és kikódolja az adatokat.

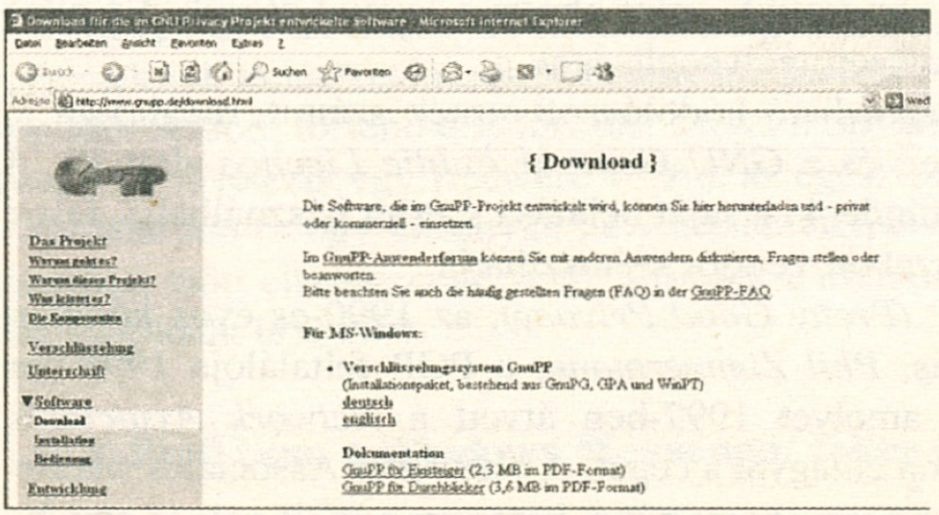
– GPA: a GNU Privacy Assistant, amely grafikus felülettel rendelkezik, a nyilvános kódokat felügyeli, valamint kódolja és kikódolja a fájlokat, mondjuk a mailcsatolásokat.

– WinPT: a Windows Privacy Tray a Tálca rendszerterületén található eszköz, amelynek segítségével a mailek kódolhatók és kikódolhatók, illetve aláírhatók a Vágólapon keresztül. A program a GnuPG egy grafikus felülete, amely minden mailprogrammal használható.

– Outlook-Plugin: az Outlook számára létezik egy GnuPG-Plugin a G DATA cégtől. Ez kapcsolóelemként szolgál az Outlook és a GnuPG, illetve a GPA kódfelügyelet között.

A GnuPG kompatibilis a PGP-vel az 5.x verziótól felfelé, azonban a PGP régebbi 2.x verzióival nem. Ennek az az oka, hogy a régebbiekben egy szabadalmaztatott algoritmust használtak, amelyet a szabad szoftverekben már nem alkalmaznak.

4.1. A GnuPG letöltése és telepítése



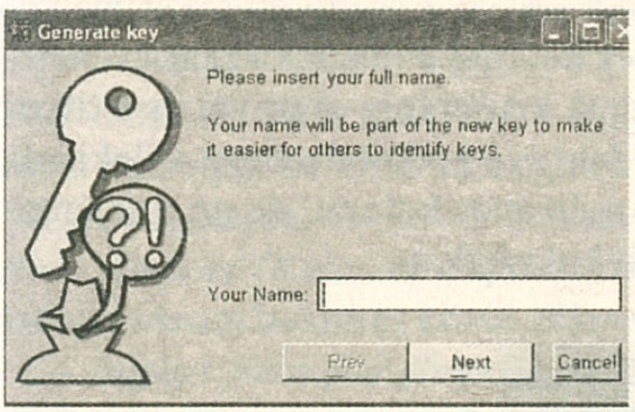
A www.gnupp.de/download.html oldalról a GnuPG kodolóprogramot, a Varázslót és a Vágólap eszközét is letölthetjük

Lépjünk fel a **www.gnupp.de/download.html** weboldalra. A *Für MS Windows* (*MS Windowshoz*) rész alatt található részben kattintsunk a *Verschlüsselungssystem GnuPP* (*Kódolórendszer GnuPP*) sor alatt található *englisch* (angol) hivatkozásra, hogy a körülbelül 3 Mbájt méretű telepítési csomagot letöltsük a GnuPG, a GPA és a WinPT számára.

Végezetül telepítsük ezt a fájlra történő dupla kattintással. A telepítési Varázsló megjeleníti a licencet, amelyet el kell fogadnunk. Ez ekkor egy könyvtárat javasol, amelyben a programok telepítésre kerülnek. Végezetül meghatározásra és telepítésre kerül egy Start menü csoport.

4.2. Kulcspárok létrehozása

A *Start* menün keresztül indítsuk el a *Programok* alatt található „GnuPP" bejegyzéssel szereplő *Gnu Privacy Assistant* programot. Első indításkor felbukkan egy jelentés, hogy nem rendelkezünk kulccsal. Kattintsunk ezért a *Generate key now* (*Kód létrehozása most*) pontra.

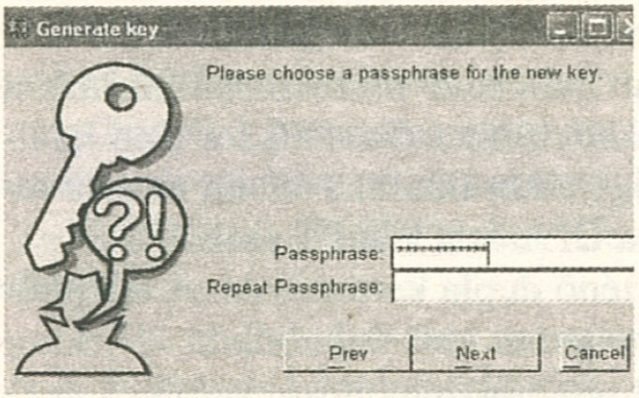


A kulcs generálásához meg kell adnunk a nevünket

Ezt követően megjelenik egy ablak, amelyben meg kell adnunk a nevünket. Ebben a párbeszédablakban adjuk meg tehát nevünket és az ezt követő ablakban az e-mail címünket. A harmadik beadási ablakban megjegyzést fűzhetünk a kulcshoz, amely csupán számunkra látható.

Ezután az a pillanat következik, amikor egy jelszómondatot kell megadnunk. Ennek a mondatnak a megerősítése érdekében adjuk meg ezt mégegyszer. A mondat legyen olyan, hogy más személyek ne, vagy csak nagyon nehezen tudják kideríteni. Azonban nem tartalmazhat ékezeteket, ellenkező esetben nem lehet kikódolni a WinPT-vel.

Most hozzuk létre a kulcs biztonsági másolatát. Válasszuk ki a könyvtárat vagy a meghajtót, majd kattintsunk a *Finish* (*Kész*) pontra. Létrehozzuk a privát és a nyilvános kulcsot, és bezárhatjuk a párbeszédablakot.

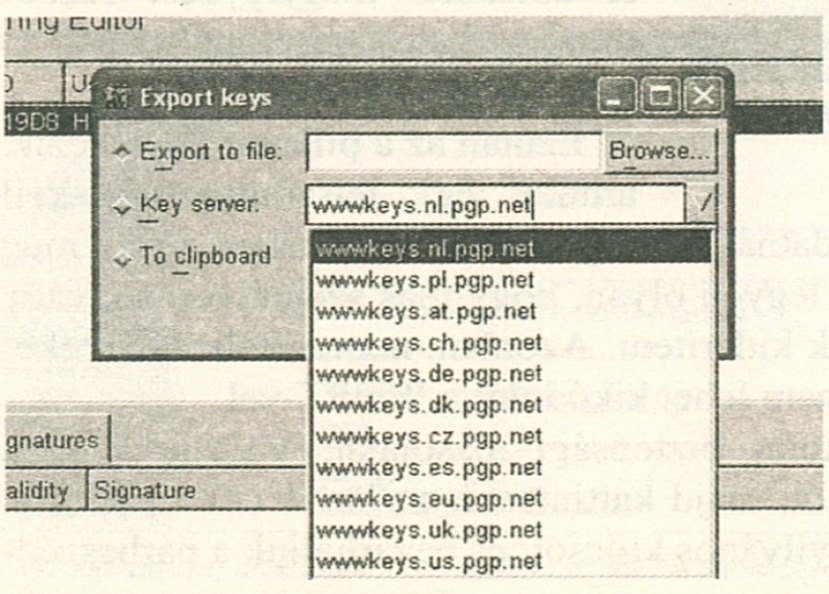


ügyeljünk a jelszómondat megadásának szabályaira!

4.3. A nyilvános kulcs exportálása

A nyilvános kulcsra olyan barátainknak és üzleti partnereinknek van szükségük, akik biztonságos üzeneteket küldenek. Ezért a nyilvános kulcsot ne rejtegessük: vagy tegyük fel a honlapunkra, vagy küldjük szét e-mailen keresztül, esetleg hozzuk nyilvánosságra az úgynevezett kulcsszervereken, vagy – és ez a legbiztonságosabb – közvetlenül adjuk át egy lemezen.

Ezzel a kulccsal más személy képes kódolni a nekünk szánt üzeneteket. Ezeket az üzeneteket csak mi tudjuk kikódolni – a privát és a titkos kulccsal. Amikor mi szeretnénk elküldeni egy kódolt üzenetet valakinek, akkor használjuk az érintett személy nyilvános kulcsát, de ne a sajátunkat, és semmi esetre sem a saját privát kulcsunkat.



Itt választhatunk kulcsszervert

Jelöljük ki a kulcsot, és kattintsunk a GNU Privacy Assistant programban az *Export* ikonra. A következő párbeszédablakban a következő három lehetőség áll rendelkezésünkre:

– *Export to file (Exportálás fájlba):* ekkor a kulcsot elküldhetjük fájlként vagy a honlapunkon is elhelyezhetjük.

– *Export to Key Server (Elküldés a kulcsszervernek):* Itt válasszunk ki egy kulcsszervert a listából.

– *Export To Clipboard (Exportálás a Vágólapra):* továbbítja a kulcsot a Vágólapra: innen beilleszthető az e-mailekbe a **Ctrl** + **V** billentyűkombinációval.

4.4 A nyilvános kulcs importálása

A partnerek nyilvános kulcsának importálása az exporthoz hasonló módon működik. Amennyiben a partner fájlmellékletként küldi át a nyilvános kulcsot, mentsük el ezt egy fájlban. Ha a nyilvános kulcs a honlapon található vagy egy e-mailbe beszúrva érkezik, jelöljük ki, méghozzá a „-----BEGIN PGP PUBLIC KEY BLOCK-----" sortól a „-----END PGP PUBLIC KEY BLOCK-----" sorig. (Ezt a két sort is ki kell jelölni). Most másoljuk be ezt a szövegblokkot a **Ctrl** + **C** billentyűkombinációval a Vágólapra. A GNU Privacy Assistant programban válasszuk a *Keys, Import (Kulcsok, Importálás)* pontot. A következő párbeszédablakban három beállítás közül választhatunk:

– *Import from file (Importálás fájlból):* Válasszunk ki egy fájlt egy nyilvános kulccsal. Ezt a beállítást akkor válasszuk, ha a kulcsot csatolt fájlként kaptuk, vagy ha ezt egy weboldalról töltöttük le.

– *Receive from Server (Kulcs fogadása a kulcsszervertől):* Ezzel a beállítással a kulcsszervereken kereshetünk nyilvános kulcsokat. Bár tesztünk közben megjelentek a kulcsok a szerveren, az importálás azonban minden esetben megszakadt a *Key ID must contain only hexadecimal digits* hibajelentés kíséretében.

– *Import from Clipboard (Importálás a vágólapról):* Amennyiben kijelöltünk egy, a nyilvános kulcsot tartalmazó szövegblokkot, és azt átmásoltuk a vágólapra, akkor azt ezzel a beállítással importálhatjuk onnan.

4.5 E-mailek kódolt archiválása

Most már ismerjük az e-mailek kódolásának és kikódolásának folyamatát, de egy valami még hiányzik: az elküldött üzeneteinket esetleg archiválni szeretnénk a merevlemezünkön, és nem szeretnénk tisztázott szövegként megtartani a számítógépen. Azonban a mailek a címzett nyilvános kulcsával kerülnek kódolásra. Ezek olvasásához szükség lenne az illető személy titkos kulcsára – ez így azonban természetesen már nem lenne többé titkos.

A rejtély megoldása: küldjük el az e-maillel a standard kulcsunkat is. Ezt a GnuPG automatikusan elvégzi. E célból nyissuk meg a WinPT-ben a *Preferences, GPG (Beállítások, GPG)* bejegyzést. Végezetül a *General Options (Általános GPG-beállítások)* területen található *Saját kulcs* mezőben adjuk meg a standard kulcsunkat.

Ha most szeretnénk archiválni kódolt üzenetet az e-mail programunkban, ezt egy későbbi időpontban a vágólapon keresztül a WinPT segítségével kikódolhatjuk, amennyiben megadjuk a jelszómondatunkat.

4.6 E-mailek aláírása és kódolása

Az e-mail kódolása helyett azt alá is írhatjuk. Bár így az üzenet mindenki számára látható, azonban tartalmazza az elektronikus aláírásunkat. Így láthatja a címzett, hogy az üzenet tőlünk származik és nem változtattak rajta. A kódolás a titkos kulcs segítségével történik.

Amikor megírtunk egy üzenetet, jelöljük ki azt a **Ctrl + A** billentyűparanccsal, majd a **Ctrl + C** billentyűkombinációval helyezzük át a vágólapra. Most válasszuk a WinPT alatt a *Clipboard* menüpontban található *Sign (Aláírás)* pontot. Jelöljünk ki egy titkos kulcsot, és az *OK*-ra történő kattintás után írjuk be a jelszómondatot. Ezek után kattintsunk kétszer az *OK*-ra.

Most illesszük be az aláírt üzenetet a vágólapról a **Ctrl + V** billentyűkombinációval. Most az e-mail program ablakában újra látható az eredeti üzenet, azonban az aláírással együtt. Ezen aláírás alapján a címzett a mi nyilvános kulcsunkkal ellenőrizheti, hogy az üzenet tőlünk származik-e.

4.7 A csatolt fájlok kódolása és aláírása

Semmit sem használ, ha kódolunk egy e-mailt, de a bizalmas adatokat tartalmazó csatolt mellékletet azonban nem. Ezért a fontos üzenetekben mindenképpen kódoljuk a csatolt mellékleteket is.

Ha mások is belenézhetnek a fájlokba, és biztosak vagyunk abban, hogy semmi sem fog megváltozni, elegendő a csatolt fájl aláírása is. Így rögtön felismerhető, hogy az adatok változtak-e az interneten át vezető úton, amíg az megérkezik a címzetthez. Amúgy a WinTP segítségével a saját merevlemez fájljai is kódolhatók.

A csatolt fájlokat nem az e-mail üzenettel együtt kell kódolni vagy aláírni, hanem külön-külön. Válasszuk ehhez a WinPT menüjéből a *File Manager (Fájlkezelő)* bejegyzést. Ezután megnyílik a hasonló elnevezésű párbeszédablak. Ebbe a Drag & Drop módszer segítségével húzzuk át azt a fájlt, amelyet kódolni, illetve aláírni szeretnénk. Végezetül jelöljük ki a fájlt, és a *File* (*Fájl*) menüben válasszuk az *Encrypt (Kódolás)*, illetve a *Sign (Aláírás)* parancsot. Amennyiben a kódolás mellett döntöttünk, a következő ablakban a címzett nyilvános kulcsát kell kiválasztanunk. Ezt követően kódolásra kerül a fájl, és a „.gpg" végződéssel ellátva bekerül ugyanebbe a mappába. Az eredeti fájl is megmarad. Az elküldendő üzenethez a „.gpg" végződésű fájlt csatoljuk.

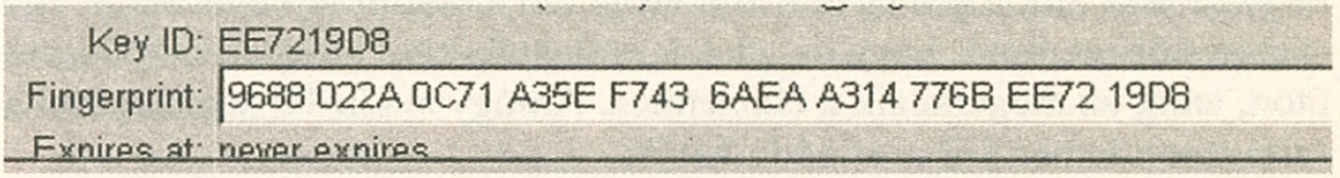
A címzettnek a kódolt fájl kikódolásához szintén be kell azt húznia a *File Manager*-be *(Fájlkezelő)*, ezt követően pedig a *File* (*Fájl*) menüpont alatt található *Decrypt (Kikódolás)* parancsot kell kiválasztania, majd meg kell adnia a jelszómondatot.

Amennyiben a fájlt ehelyett csak alá szeretnénk írni, válasszuk a *File* (*Fájl*) menüben a *Sign (Aláírás)* pontot. A következő ablakban válasszuk ki a titkos kulcsunkat, és végezetül adjuk meg a jelszómondatunkat. Ezt követően ugyanabban a mappában, amelyben az eredeti fájl is található, létrejön egy hasonló nevű fájl, azonban a „.sig" végződéssel.

A fájl ellenőrzéséhez az aláírt és az eredeti fájlnak ugyanabban a könyvtárban kell lenniük. Nyissuk meg az aláírt fájlt a WinPT *File Manager (Fájlkezelő)* bejegyzése alatt, és a *File (Fájl)* pontban válasszuk a *Verify (Ellenőrzés)* menüpontot. Ha a következő ablakban a *Status* pont alatt az *Aláírás érvényes* bejegyzés áll, akkor senki sem nyúlt a fájlhoz.

4.8 A kulcs eredetiségének ellenőrzése

Amennyiben valaki elküldi számunkra a nyilvános kulcsát, még mindig nem lehetünk biztosak abban, hogy ez valóban ahhoz a személyhez tartozik-e. Csak abban az esetben lehetünk teljesen biztosak ebben, ha a kulcsot személyesen – mondjuk egy lemezre másolva – vettük át az illetőtől.



Ilyen egy ujjlenyomat

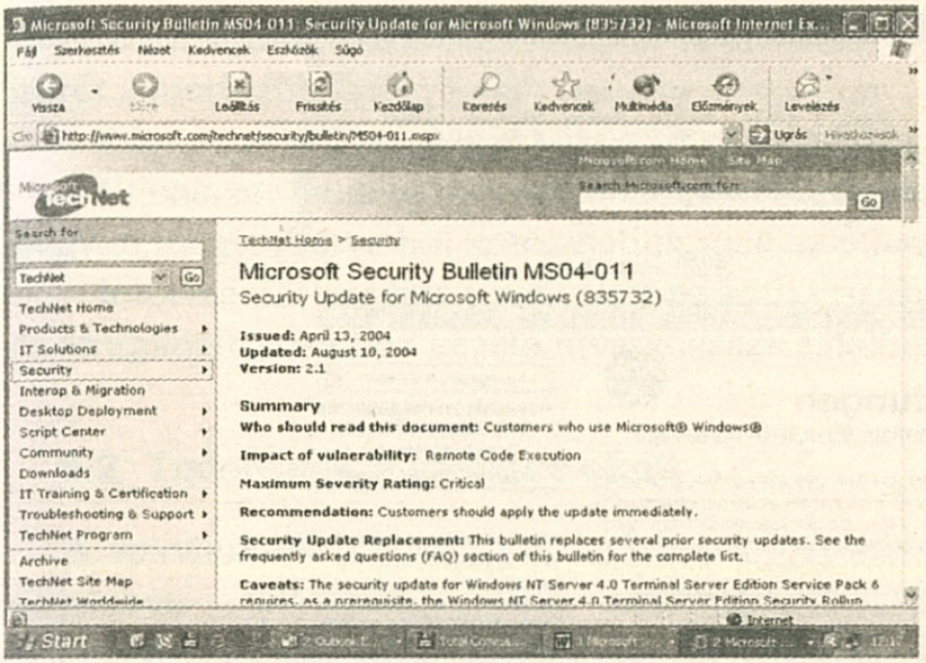
Ez azonban nem minden esetben lehetséges. Ilyenkor megadhatjuk az ujjlenyomatot (*Fingerprint*) is – minden kulcs rendelkezik ilyennel, és a *Gnu Privacy Assistant*-ben láthatjuk ezt, amikor kijelölünk egy nyilvános kulcsot. Váltsunk át, amennyiben szükséges, a *Detailed (Részletek)* fülre. Itt található a kulcs 40 karakterből álló ujjlenyomata.

Hívjuk fel a kulcs tulajdonosát, és olvastassuk be vele az ujjlenyomatot. Így megbizonyosodhatunk arról, hogy a nyilvános kulcs valóban tőle származik.

5 Információk spamekről, vírusokról és más gazságokról

Amikor PC-nk furcsán reagál, amikor támadások érik, amikor a spam átveszi az irányítást – mindezekben az esetekben védekeznünk kell. Ebben segítséget nyújtanak weboldalak, amelyek információkat gyűjtenek a károkozókról. Ebben a fejezetben megtalálhatják a legfontosabb tudnivalókat és az elhárítási stratégiákat.

Talán még emlékeznek olvasóink a Sasserra: április végén, május elején megbénította a Windows-világ egy részét. Villámgyorsan. Világszer-



Védőszer a Microsofttól

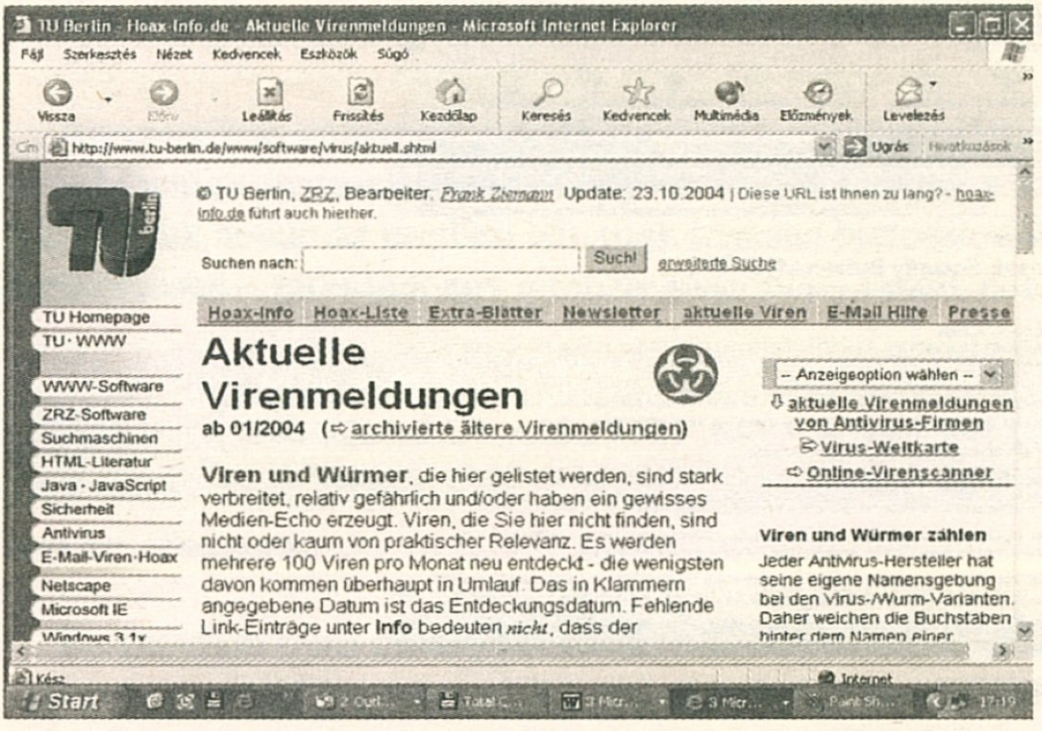
te. Hogy végezetül mekkora lett a kár, az alig mérhető fel. Ám a féreg fiatal német programozójának nem lesz minek örülnie egyhamar.

A Sasser a Windows 2000 és az XP biztonsági falának rését használja. A biztonsági rést és a módot, hogy miként védhetjük magunkat, a **www.microsoft.com/technet/security/bulletin/MS04-011.mspx** oldal alatt tárgyalja a Microsoft. Ez nyilvánvalóan sokak számára kissé megkésett. A következmény: a rendszer lefagyása és a hátsó ajtók megnyitása az 5554 és a 9996 portokon. Így kerül a támadó olyan helyzetbe, hogy átvegye a megtámadott számítógép feletti teljes irányítást.

Ingyenes ellenszert a Sasser féreg ellen a *Symantec* **(www.symantec.com/avcenter/tools/list.html)** és a *McAfee* **(http://vil.nai.com/vil/averttools.asp)** kínál. Erről több információt a **www.hoax-info.de/va** webcím alatt találhatunk.

5.1 Vírusok, férgek, trójai programok

Amennyiben vírusokról, férgekről vagy trójai programokról van szó, Frank Ziemann információs szolgálata ad információkat, igaz, német nyelven. A szolgálatot a berlini Műszaki Egyetem honlapján találhatjuk a **www.tu-berlin.de/www/software/virus/aktuell.shtml** cím, vagy rö-



Ezen a német nyelvű oldalon számtalan hasznos vírusinformációt találunk

videbben a **www.hoax-info.de** cím alatt. Az oldalak áttekintést adnak majdnem mindegyik jelenleg aktív vírusról és féregről. Az ott felsorolt károkozók bizonyos szinten híresek az elterjedésük, a veszélyességük vagy a médiában megjelenő visszajelzések alapján.

Minden vírushoz és féreghez még a következő információ tartozik a nevén, a felfedezésének dátumán és az elterjedési fokán kívül:

– Alias: ez alatt a név alatt is ismert a vírus vagy a féreg.

– Elterjedés: a vírusok és a férgek elterjedésének leggyakoribb formája jelenleg az e-mail.

– Feladó adatai: az adatok a legtöbb esetben hamisítottak, emellett ezek gyakran különböző adatok, így nem lehet szűrni őket. Ezért a legtöbb esetben nem használ semmit, ha ennek a személynek e-mailt küldünk, amelyben felhívjuk a figyelmét a féregre vagy a vírusra.

– Tárgy/Subject: a Tárgy sor különböző lehet, némelyik német, másik angol. Hogy melyik Tárgy sorok fordulnak elő, azt gyakran a „Details" hivatkozáson keresztül nézhetjük meg.

– Üzenet: az üzenet szövegére ugyanaz vonatkozik, mint a Tárgy sorra.

– Melléklet: itt az áll, hogy mi a fájl neve, valamint hogy milyen a végződése és a mérete.

– Szimptóma: itt minden féregről és vírusról kimerítően leírják, hogy miről ismerhetők fel.

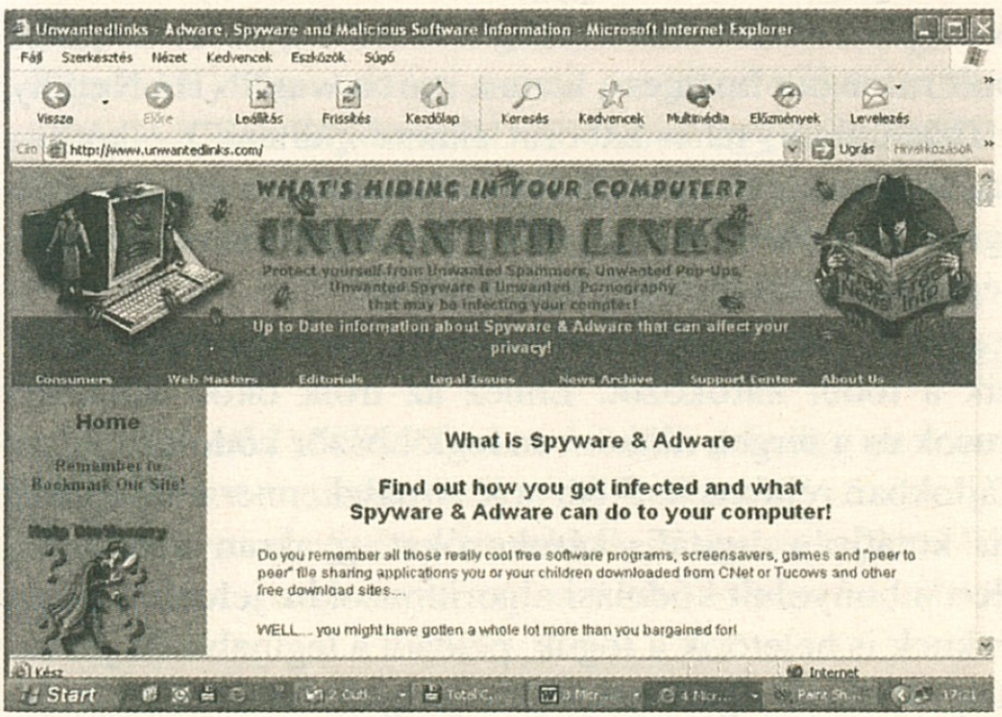
– Kár: itt az áll, hogy mekkora kárt okoz a féreg vagy a vírus.

– Ellenszer: ha még van mit megmenteni, itt tudhatjuk meg, hogy ez hogyan megy, illetve hol szerezhetjük meg az ellenszert.

– Információ: ez alatt a pont alatt az antivírusokat gyártó cégek vírus- és féregadatbázisaihoz vezető hivatkozásait találhatjuk.

5.2 Tudnivalók a spyware-ekről

A spyware-ekről szóló információk a legtöbb esetben angol nyelvű oldalakon találhatók. Sok információval szolgál például a **www.unwantedlinks.com** oldal. Itt egészen a lap végéig kell mennünk, és ott a „CHECK OUR ADDITIONAL RESOURCES & INFORMATION" fejezet alatt rengeteg információt találhatunk a spyware-ekről, az adware-ekről, részleteket ismerhetünk meg a peer-to-peer felkínáló Kaaza cég és a gyanús hirdetés- és marketingvállalatok közötti együttműködésről, valamint arról is, hogy hogyan és miért kerülnek eladásra a személyes adatok, és hogy ki nyer ezzel az üzlettel.



Információk spyware-ekről, adware-ekről és egyéb gazságokról

A spyware-gyártókat tartalmazó adatbázist a **www.spywareguide.com** oldalon találhatjuk. Ezen kívül egy online teszttel megállapíthatjuk, hogy található-e számítógépünkön telepített spyware. Az *Educations* terület elmagyarázza, hogy mi a spyware, és hogy miként védhetjük meg magunkat.

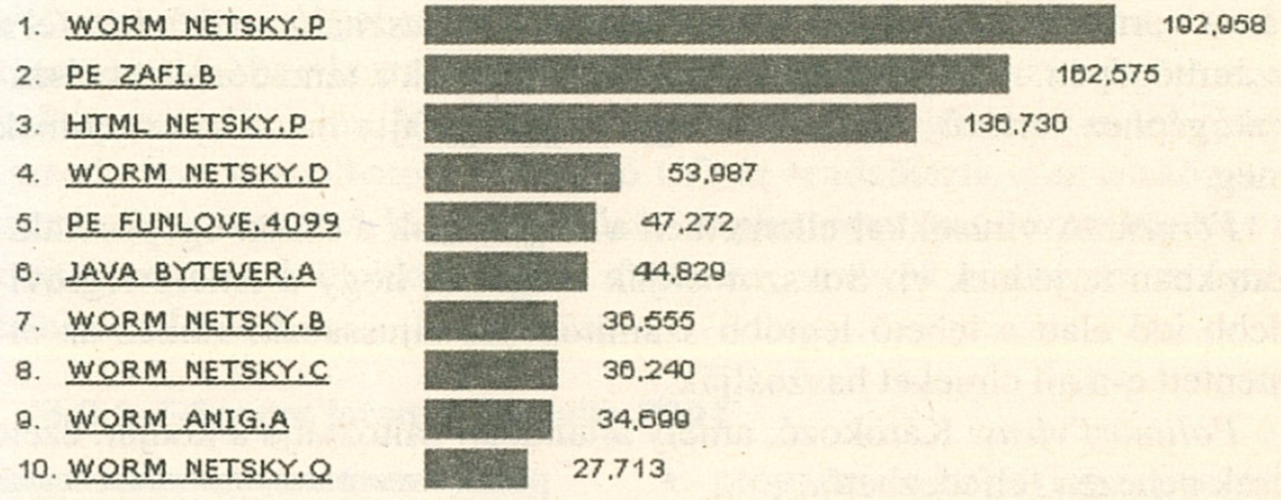
6 Vírusok és vírusölők

Nem elég, hogy az e-mailek 80%-a csupán értelmetlen spameket tartalmaz, a vírusgyártók még egyfajta versenyt is vívnak egymással: ki programozza a legalattomosabb férget? Ebben a fejezetben bemutatunk néhány eszközt a ma és a holnap csapásai ellen.

A férgek keményen kézben tartják a webet, szinte naponta születnek a Bagle, a NetSky és a Mydoom egyre veszélyesebb változatai. És mintha ez még nem lenne elég rossz, a vírus gyártói között szabályszerű harc tört ki, amelynek a felhasználók isszák meg a levét. Egymást hergelik: „Hey NetSky, don't ruine our business, wanna start a war?" (Hé NetSky, el a kezekkel az üzletünktől, talán háborút akarsz indítani?) – kérdi a NetSky íróinak szánt üzenet, amelyet a Sophos víruskutatói a Bagle-J féregben (W32/Bagle-J) fedeztek fel. Az egyik gúnyolódása arra készteti a másikat, hogy még gonoszabb férgeket fejlesszen ki.

Gyors és agresszív férgek uralják tehát a terepet, és már majdnem teljesen kiszorították a többi károkozót. Ehhez az íróik okos trükköket használnak: a vírusok és a férgek időközben legtöbbször kódolt és jelszó által védett ZIP fájlokban rejtőznek. S bár sok vírusszkenner a tömörített archívumokban is kutatja a digitális károkozókat, gyakran nem sokra mennek ezzel. Mert a bonyolult kódolási algoritmusokba jelenleg még a legjobb szkennereknek is beletörik a foguk, például a legújabb Bagle variációkba (F-től I-ig) is. Ezek a gonosztevő kis programok a védett archívumokban lapulnak, amelyeknél a csatolt fájl megnyitásához a jelszó a

felhasználó számára normális szövegként látható az e-mailben. Az alkalmazott technikák a szövegben első osztályúak, senki sem sejt semmi rosszat mögöttük.



Trend Micro WTC – A tíz legelterjedtebb rosszindulatú kód (2004. október 20.)

Ezzel a „Social Engineering" módszerrel győzik meg a felhasználókat az e-mail ártalmatlanságáról vagy fontosságáról. A többi már ismerős: a felhasználó megnyitja a csatolt fájlt, megadja a jelszavát, és a vírus aktívvá válik. Ha már egyszer a számítógépre került, megszerzi magának az összes elmentett címet, és szétküldi magát e-mailben. Ehhez a férgeknek még csak egy e-mail programra sincs szükségük. A Netsky.F, a Bagle.K és a Mydoom.H változatok egy saját SMTP-Engine-t is tartalmaznak, és a felhasználó nélkül is továbbküldik magukat. Éppen a legveszélyesebb férgek terjednek így eszméletlen sebességgel.

6.1 Vírusok, vírusölők: a legfontosabb szakkifejezések

In the wild (ITW): Ezek a vírusok jelenleg az interneten keringenek, és gyakran e-maileken keresztül fertőznek.

Zoo-vírusok: Laborvírusoknak is nevezik őket. Ezeket a kártevőket laborokban „tenyésztik", és a jobb felismerési eljárások utáni kutatást szolgálják.

On Demand: Ennél az eljárásnál a felhasználó manuálisan indítja a merevlemez szkennelését.

On Access: A bekapcsolt vírusellenőrzőnek önállóan kell aktívvá válnia. Például ha a felhasználó e-mailt kap, az ellenőrző ezt automatikusan átnézi vírusok után kutatva.

Trójai programok /Backdoor vírusok: Mivel a trójai program egy teljesen normális programnak álcázza magát, a felhasználó nem fedezi fel a számítógépén. A trójai programok lehetővé teszik a támadónak a célszámítógéphez történő hozzáférést úgy, hogy egyfajta hátsó ajtót nyitnak meg.

Férgek: A vírusokkal ellentétben a férgek csak a számítógépes hálózatokban terjednek el. Sokszorosítják magukat, hogy a lehető legrövidebb idő alatt a lehető legtöbb számítógépre eljussanak. Ehhez az elmentett e-mail címeket használják.

Polimorf vírus: Károkozó, amely állandóan változtatja a kódját, ezért csak nehezen felfedezhető.

Makróvírus: Betolakodó, amely egy makró formájában válik aktívvá a fájlban, és magától csatlakozik a többi fájlhoz.

Hoax: „Vicc-vírus", amely hibás jelentéseket produkál, hogy ezzel elbizonytalanítsa a felhasználót. Azonban nem okoz kárt a célszámítógépen.

ZIP-bombák: Az elv éppoly egyszerű, mint amilyen káros. A ZIP fájl egy csupán néhány Kbájt méretű e-mailben található. Amint ki szeretné csomagolni a szkenner a fájlt az ellenőrzéshez, az megbénítja a PC-t. Ugyanis a látszólag apró fájlban hatalmas méretű, kitűnően csomagolható adatok rejlenek. Ilyen eset például, amikor egy szövegben például 10 az ötvenedikenszer szerepel az „A" betű.

6.2 Vírusszkennelők közelebbről

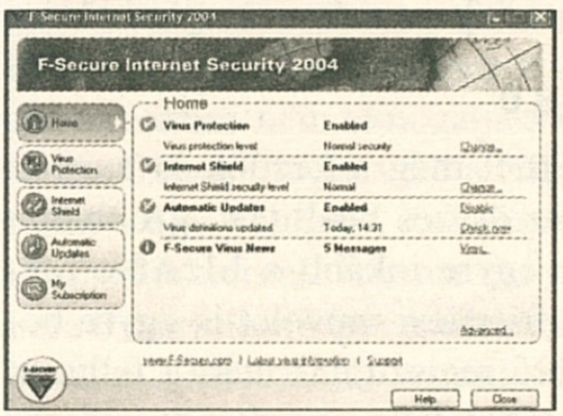
Minden felhasználónak szüksége van tehát egy jó antivírus eszközre. Tesztlaboratóriumunkban is megvizsgáltunk néhány ilyen eszközt.

Nézzünk néhány fontos vizsgálati szempontot! A legfontosabb tesztkritérium az interneten bolyongó *In the wild vírusok (ITW)* szkennelési teljesítménye volt. Egyet előrebocsátunk: mindegyik eszköz tökéletes munkát végez. Mindemellett hangsúlyt fektettünk az úgynevezett Zoovírusok felismerésére is, amelyek programozása laborokban folyik, és amelyeket kutatási célokra használnak: itt be kell bizonyítaniuk a szken-

nereknek, hogy milyen jók a feltalálóik, ugyanis a tesztvírusok számára nem rendelkeznek megfelelő vírusdefinícióval.

Az erőforrás leterheléséről sem feledkezhetünk meg, ugyanis a vírusölők gyakran lefékezik a rendszert. Emellett ellenőriztük, hogy a gyártók milyen gyakorisággal jelentetik meg a vírusaláírások frissítéseit, és milyen anyagi következményekkel jár ez a felhasználók számára. Azt is tudni szerettük volna, hogy milyen funkciókkal szolgál a szkenner vírustámadáskor: bootolható-e a telepítő CD és rendelkezik-e az eszköz karantén funkcióval? A kiegészítő tűzfal is pluszpontokat hozott, mert ez a trójai programok blokkolására is alkalmas, amelyek ki akarják szolgáltatni az adatokat.

6.2.1 F-Secure Internet Security 2004



A program, viszonylag egyszerű kezelése miatt, kezdőknek is ajánlható, s ugyancsak pozitívum, hogy már a telepítéskor aktiválja az automatikus frissítési funkciót is. A szkennelési teljesítménye is nagyon jó, ami persze nem is csoda, hiszen az Internet Security-ben a Kaspersky Engine mellett két saját fejlesztésű motor is működik, a „Libra" és az „Orion". Ezért az F-Secure a Zoo-vírusok esetében jobb értékekkel szolgál, mint Kaspersky szkennerje.

A regisztrálás szükséges, de az F-Secure csak a regisztrációs számot ellenőrzi. Ezek után az eszköz feltölti a számítógépre a legújabb updateet. Az új aláírásokat a gyártó naponta szétküldi. A műszaki támogatás számára az F-Secure egy webűrlappal szolgál, azonban a felhasználónak fel kell készülnie a mintegy 3 napos reakcióidőre.

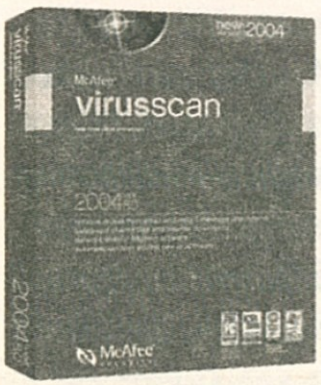
A felhasználó még a telepítés előtt elvégezhet egy vírusszkennelést DOS szinten, a folyamat jó fél órát vesz igénybe. Sajnos a program-CD nem bootolható, s éppily kevésbé teszi lehetővé az F-Secure a bootmédium létrehozását. A karantén funkció is hiányzik. Az integrált tűzfal ellenben nagyon jól felszerelt, és lehetővé teszi a szabályok meghatározását az egyes programok internetes hozzáféréséhez.

6.2.2 Kaspersky Anti-Virus 4.5

A Kaspersky Engine kiemelkedő eredményekkel szolgál, méghozzá éppen azokban a pontokban, amelyekben a többiek gyengék: a trójai programok és a Backdoor vírusok ellen. A program csak a makró- és a scriptvírusok esetében nem éri el a 100%-os teljesítményt. Nincs sok automata funkciója. Bár telepítés után beindul az őrző, de az eszköz sem új aláírásokat nem szerez automatikusan, sem a szkenner nem lép önként akcióba, hogy ellenőrizze a rendszert.

Az átfogó program öt összetevőt kínál, köztük az Office dokumentumok külön-külön történő felügyeletét, egyet az scripteknek, egyet a maileknek. De sem a konfigurációnál, sem ezeknek a komponenseknek az alkalmazásánál nem kap a felhasználó segítséget, ráadásul a felület nem egyszerű. Csak a kézikönyv segítségével állítható be tökéletesen a szoftver. Jó pont viszont, hogy alacsony a rendszermegterhelés.

6.2.3 McAfee Virusscan 2004 Version 8.0



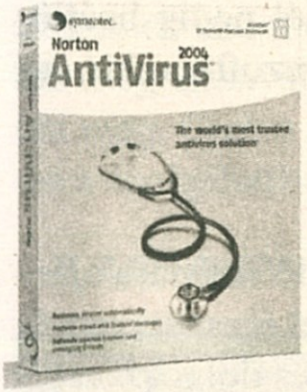
Bár ennél a terméknél még a kezdők is nagyon gyorsan megtalálják az összes beállítást, azonban a felület az évek során egyre inkább a McAfee reklámfelületévé vált. A frissítési művelet is egyre bonyolultabb: a kényszerű regisztrálás után a felhasználó a McAfee oldalán találja magát. Itt először megkapunk egy ActiveX-Applet-et a frissítés számára, ami már önmagában ellentmondásos, hiszen az ActiveX már alapjában egy bizonytalan technológia. Ha biztosra akarunk menni, kapcsoljuk ki az Internet Explorerben az ActiveX-et, hogy a lehető legkisebb támadási felületet kínáljuk.

A Scan-Engine azonban a tesztelt termékek legjobbjaihoz tartozik. Még a Zoo-vírusoknál is 99%-osnál magasabb felismerési arányt ér el az eszköz. Csupán az ActiveX vírusoknál és a trójai programoknál nem olyan hatásos az eszköz. Szintén negatívum: a telepítő CD nem bootolható.

A támogatás viszont remek: a felhasználó e-mailen keresztül is kérdezhet, vagy a számítógépét is ellenőriztetheti a programba integrált Security Center-en keresztül. A napi használatban az eszköz egész jónak

mondható: bár a felhasználó észreveszi, hogy az őrző működik a háttérben, azonban ez nem zavaró munka közben.

6.2.4 Norton AntiVirus 2004



A Symantec vírusszkennelője ideális a kezdők számára. Már a telepítésnél is majdnem minden teljesen automatikusan történik. A program először egy komplett szkenneléssel vizsgálja át a PC-t, majd ezután aktiválja az új aláírások frissítését. A szkennelési teljesítményt illetően a Norton AntiVirus az élbolyban végzett. A Zoo-terület script- és makróvírusainál a szkennelési teljesítmény majdnem 100%-os, de amennyiben az ActiveX-ről, a trójai programokról vagy a backdoor vírusokról van szó, csökken a felismerési arány. Negatívumként kell megemlítenünk, hogy a szoftver sem a normális, sem az önmagukat extraháló archívumokban nem támogatja a kedvelt ACE csomagolási formátumot.

Az Office Plugin védi a felhasználókat a makróvírusok ellen, amennyiben egy fertőzött dokumentum próbál meg elindulni. A veszélyes OLE-objektumok felismerési aránya 100%-os. Az internetről származó veszélyek ellen egy mailszűrő nyújt támogatást, s ezt kiegészítve, a Norton ellenőrzi az Instant Messenger üzenetek csatolt fájljait. Nagy kár, hogy hiányzik a tűzfal. A rendszerleterhelés a középmezőnyben mozog, Windows XP alatt azonban nagyon lassan fut a szkenner.

6.2.5 Panda Antivirus Platinum 7.0

A Panda szkenner felismerési teljesítménye bizony jócskán hagy kívánnivalókat maga után a Zoo-vírusok területén. A polymorph (vagyis a magukat megváltoztató) vírusokat a szkenner csak 90%-os biztonsággal ismeri fel. A trójai programok és a backdoor vírusok 75 százalékos felismerési aránya sem épp vonzó. De legalább a támogatás példaértékű: e-mailen keresztül lehet felvenni a kapcsolatot a technikusokkal. Az új aláírásokat a szoftver csak 14 nappal a telepítés után tölti le automatikusan.

Az erőforrás-tartalékok kordában tartják magukat. Kiegészítő funkcióként a szoftver felkínálja a CPU-terhelés megszabályozását. Bosszantó a hibás riasztások gyakori előfordulása. Az internetfunkciók teljesen rendben vannak: a program lehetővé teszi az integrált tűzfalhoz tartozó egyszerű szabályok meghatározását. A mailfelügyeletnél pedig beállítható, hogy melyik felhasználó profil felügyelje a szoftvereket az Outlookban és az Outlook Expressben.

6.2.6 BitDefender 7.2 Professional

Ez a csomag az olyan felhasználó számára ajánlott, amelyek csak a biztonság érdekében szeretnék használni az eszközt. Éppen a webes dolgokban kínál sokat a BitDefender: módosítások a Registryben, a cookie-k elhelyezésének és a futtatásának felügyelete. Ezen kívül az eszköz rendelkezik egy hatékony tárcsázóprogramok elleni védelemmel. A biztonságot érintő feladatok esetében a BitDefender tehát komoly biztonsági központnak számít.

A program szkennerje azonban gyengélkedik, ha a Zoo-vírusokról van szó. A felismerési arányoknál ebben a pontban csak az AntiVir Freeware szerepelt rosszabbul. A polymorph vírusokat az eszköz kivétel nélkül felkutatja, minden más Zoo-területen azonban hibákat ejt.

Azonban a támogatás jól működik. A szolgáltatás már a programban megkezdődik, hiszen a BitDefender nem csak a fontos vírusaláírásokról informál, hanem a Windows biztonsági frissítéseiről is. A napi 24 órában telefonon, illetve e-mailen keresztül elérhető szolgálat mellett naponta új frissítéssel találkozunk. Az aktív őrző melletti megterhelés elég alacsony. Emellett a BitDefender a Systray feletti ablakban megjeleníti az őrző rendelkezésére álló rendszerteljesítményt.

6.2.7 G-Data AntiVirenKit 2004

A program az integrált Kaspersky-Scan-Engine-nek és a BitDefender-nek köszönhetően mindenféle vírus ellen 100%-os védelmet nyújt. Ennek az ára azonban magas, hiszen a Scan-Engine-ek kegyetlenül lelassítják a számítógépet: még a 2,5 GHz-es, 512 Mbájt RAM-mal rendelkező tesztszámítógépen sem lehetett folyamatosan dol-

gozni az aktivált őrző mellett. További negatívum: a G-Data produkálta a tesztmezőnyben a legtöbb hibás riasztást.

A kezelése azonban valóban egyszerű. Az Update funkción keresztül az eszköz az aktuális aláírások mellett a két Engine frissítését is megszerzi. Ennek azonban feltétele a regisztráció a G-Data-nál a személyes adatok megadásával. Az új aláírásokat a gyártó csupán hetente kétszer jelenteti meg. Csak a Premium támogatásnál biztosítja a napi frissítéseket – de ezt a szolgáltatást a G-Data alaposan meg is fizetteti: 30 euróba kerül.

6.2.8 AntiVir Personal Edition

Az ingyenes program nagyon könnyen kezelhető. Ám aki először használja, annak ajánlatos kicsit foglalkoznia a konfigurációs menüvel. A szkennelési teljesítmény az ITW-vírusoknál első osztályú. A Zoo-vírusok esetében azonban már nem ilyen jó a helyzet: a programnak komoly problémái támadnak a polymorph vírusokkal (84,42%), valamint a többi Malware programokkal, például a trójai programokkal és a backdoor vírusokkal. Ezeknél az AntiVir a maga 43,65%-os teljesítményével messze a legrosszabb teljesítményt hozta a tesztmezőnyben. A támogatásról a felhasználónak teljesen le kell mondania. A számos frissítés, amelyet a H + B EDV szinte naponta nyilvánosságra hoz, fabatkát sem ér.

Szkenneléskor a freeware nagyon gyors. Ami hiányzik a programból, az a rutin, amely a felhasználónak a vészesetre szánt médium elkészítésében segít: a felhasználónak ezt saját magának kell létrehoznia.

6.2.9 Összegzés

Gratulálunk valamennyi versenyzőnek: az ITW-felismerés hibátlan. Azonban csak a G-Data programja képes a Zoo-vírusok felismerésére is. Azonban ennek a biztonságnak az ára nagyon magas: ismét a G-Data rendelkezik a piacon a leginkább erőforrástartalék-igényes termékkel. Ennek ellenére, akinek számít a megbízható védelem, jól jár ezzel az eszközzel, amennyiben a számítógépe legalább 2,5 GHz-cel működik. Ha vészesetben fontos számunkra az olyan támogatás, amely nemcsak jutányos árú, hanem gyorsan is reagál, akkor válasszuk a Panda-t vagy a

Kaspersky-t. Azok, akik a szörfözéshez egy régi, második számítógépet használnak, két legyet ütnek egy csapásra az AntiVir Freeware-rel. Az eszköz nemcsak az összes ITW-vírust fedezi fel, hanem a legalacsonyabb rendszermegterheléssel is dolgozik a tesztmezőnyben.

6.3 Ingyenes féregölők

Az antivírus programok néhány gyártója ingyenes eszközöket is kínál weboldalain, amelyek csupán bizonyos, éppen aktuális férgek felkutatására és eltávolítására szolgálnak.

6.3.1 McAfee Avert Stinger

Ez az ingyenes eszköz a legveszélyesebb vírusokat és férgeket is letörli a merevlemezünkről. A Stinger jelenleg kereken 40 férget ismer fel.

Információ: **http://vil.nai.com/vil.stinger**

6.3.2 Symantec

A honlapon egy sor speciális víruseltávolító eszköz található, amelyek az aktuális férgekkel foglalkoznak.

Információ: **www.symatec.com/avcenter/tools/list/html**

6.3.3 BitDefender

A gyártó különböző eszközöket kínál a férgek eltávolítására a honlapján. Tipp: az oldal letöltési területén egy freeware vírusszkenner található a Linux, a DOS és a különböző Messaging eszközök számára.

Információ: **www.bitdefender.de/html/free_tools.php**

6.3.4 F-Secure

Itt az eszközök gazdag gyűjteménye áll letöltésre készen, közöttük teljes vírusszkenner DOS-bázison. Minden letöltéshez leírás is tartozik, amelyik megmutatja, melyik vírust lehet legyőzni.

Információ: **www.f-secure.com**

7 A holnap vírusai

A vírusvadászok szemmel tartják az egész világot. Hol bukkan fel egy újabb kártevő? Milyen gyorsan terjed? A vírusok, a férgek és a trójai programok elértek egy eddig nem ismert összetettséget. A szakemberek pedig még gyorsabb támadásokra és még gonoszabb támadókra hívják fel a figyelmet.

A PC-biztonság történelmének legrosszabb évét éljük: számítógépek milliói adják fel a szolgálatot, teljes cégek állnak le. Az adatok már nem biztonságosak. Az e-mail postafiókokat eltömíti a digitális szemét. Vírusok és férgek köröznek mindeddig ismeretlen sebességgel a Föld körül, a károk elérik a kétszámjegyű milliárdos nagyságot. A károkozók egyre összetettebbekké válnak. Csupán ez év utóbbi hat hónapjában 994 új vírust fedeztek fel, s például a Symantec cég egy jelentése szerint hetente általában 38 támadás ér egy vállalatot.

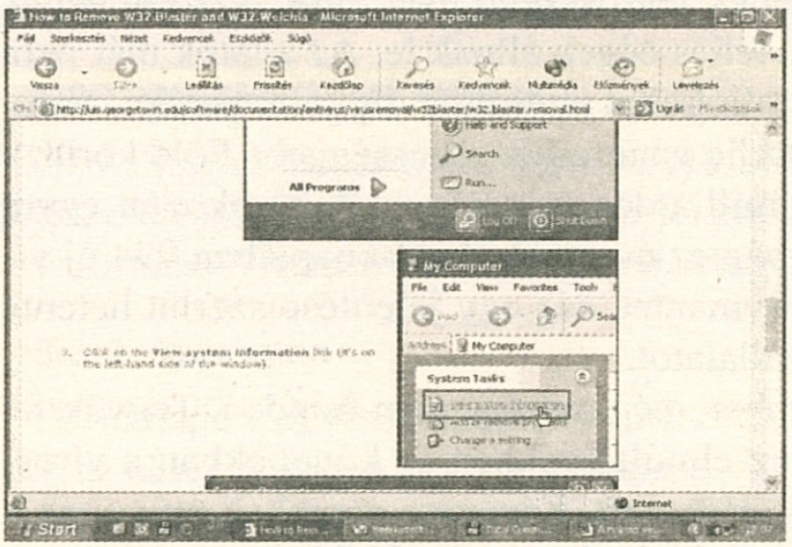
A szakértők szerint ez azonban még messze nem minden. Tegyük fel egész egyszerűen, hogy ami az elmúlt években és hónapokban a vírusfronton történt, az mind csak játék volt. Kíváncsi gyerekek műve, akik talán saját maguk lepődtek meg a legjobban „sikerük" láttán.

Továbbá azt is tételezzük fel, hogy a vírusok, férgek, trójai és más kártékony programok egész arzenálját hamarosan professzionálisan lehet felhasználni, és a gátlástalan gazfickók célirányosan alkalmazni is fogják, hogy ezzel romboljanak, gazdasági károkat okozzanak vagy bizonyos érdekeket kielégítsenek.

A vírusszakemberek számára ez az elképzelés egy rémálom, hiszen ők részletesen kiszínezhetik maguknak, hogy mi vár ránk. Közülük sokan azt gondolják, hogy ez a változás éppen most történik. S bizony láthatjuk is már annak nyomait, hogy a helyzet már változóban van. A rövid ideje köröző vírusokban már a jövő, sokkal célirányosabb támadásainak előzetes tesztjeit vélik felfedezni.

„A férgek és a vírusok a jövőben még fontosabb témává válnak. A Blaster és a Slammer még csak kis ízelítője volt annak, ami még előttünk van" – figyelmeztet *Christoph Fischer,* vírusszakértő. Az új kárte-

vők már nem is sorolhatók be pontosan egy bizonyos típusba. Túl összetettekké váltak, s több különböző mechanizmust egyesítenek egyetlen programban. Így kísérhet például egy féreg egy trójai programot, amely a megszállt számítógépben még egy kiskaput megnyit a további káros funkciók számára, vagy gyorsan megkaparintja a számítógépet saját céljaira. A férgek már nem korlátozódnak arra, hogy csak egyetlen lyukat használjanak ki a számítógép biztonsági falán. Közülük egyre többet úgy programoztak, hogy rögtön több rést is felhasználhassanak arra, hogy egyik-másik módon bejuthassanak a számítógépbe.



Az interneten képes útmutatót is kapunk a Blaster eltávolításához

„Kétségtelen, hogy a jövőben még gyorsabban terjedő és jelentősen gonoszabb fenyegetésekkel fogunk még találkozni" – véli *Steve Trilling*, a *Symantec* kutatói labor vezetője. A „Warhol" és a „Flash" férgek típusának megfelelő fenyegetések, becslése szerint, nagy hálózatokat vagy az internet hatalmas részeit perceken, vagy akár másodperceken belül is lebéníthatják anélkül, hogy akár csak halvány esélyünk is lenne az ellenintézkedésekre. Már két évvel ezelőtt leleplezték a Berkeley Egyetem vizsgálatai a károkozók veszélyes potenciálját.

7.1 Egy kis vírustörténelem

Mielőtt áttekintenénk, mit is hozhatnak a jövő vírusai, vessünk egy pillantást a múltra!

1981. Professzor Leonard M. Adleman bevezeti a „számítógépvírus" kifejezést.

1982. A Xerox Palo Alto Research Centerben (PARC) programozásra kerülnek az első férgek, amelyek a megosztott számítások célját szolgálják. Egy programhiba következtében az egyik féreg ellenőrizhetetlenül szaporodni kezd.

1983. Fred Cohen bemutatja az első vírust, amelyet Unix alatt programoztak.

1984. Cohen elkészíti a doktorátusi szakdolgozatát: Computer Viruses – Theory and Experiments". A munka gyors fejlődést vált ki.

1985. Napvilágot lát az első trójai program. Az álcázott program indítása után a merevlemez összes fájlja letörlődik.

1986. Berlinben felfedezik az első vírusfertőzést egy nagyszámítógépen.

Megjelenik az első MS-DOS vírus. Neve: Pakistani, Ashar vagy Brain vírus. Átnevezi a lemezek tartalomjegyzékét.

1987. Az első féreg egy IBM rendszerben. A „Tannenbaum" féreg robbanásszerűen terjed.

A vírusok második generációja: a Cascade vírus kódolva bukkan fel a fájlokban.

1988. Az első vírusszerszám megjelenése az Atari ST számára. Ennek az eszköznek a segítségével kezdők is képesek voltak vírusok létrehozására.

Az első internetféreg elterjedése világszerte.

1989. Az első polimorf vírus felfedezése: a V2Px vagy más néven Washburn. Az ilyen vírusok meghatározott módon újra és újra megváltoztatják magukat.

A Stealth vírusok fájlokat fertőznek meg, valamint elrejtik az elvégzett módosításokat és önmagukat.

1990. A DIR-II vírus egy teljesen új módszert alkalmaz a programok megfertőzésére: a FAT-bejegyzéseket szállja meg.

Orosz és bolgár crackerek „Dark Avenger"-ként agresszív károkozókat fejlesztenek ki.

1991. Versenyek és rendezvények szervezése a vírusprogramozásról.

Az újonnan talált vírusok száma mostantól exponenciálisan nő.

1992. Elsőként vált ki vírushisztériát a Michelangelo vírus.

Az Engine első mutációja. Ezzel a polimorf vírusok egyszerűen előállíthatók.

1993. Naponta kb. 2-3 új vírus. Havonta jelennek meg új Virus Construction Kitek.

A vírusok már a Windows programfájlokat is megfertőzik.

1994. Multipartite vírusok terjednek variálható kikódolási rutinon keresztül a fertőzött programban.

1995. Makróvírusok, például a Concept és a DMV, már nem futtatható programfájlokat fertőznek, hanem a WinWord teljes dokumentumait.

1996. Az első Windows polimorph vírus is képes megváltoztatni a külsejét.

A vírusok száma a PC-k esetében meghaladja a 10 ezer variációt.

1997. Az első Linux vírus egyidejűleg jelenik meg a Linux vírusszkennerrel.

A makróvírusok száma meghaladja a fájlvírusokét.

1998. Az első Java vírus tombol az interneten. A „Strange Brew" platformtól függetlenül terjed.

A CIH vírus első ízben okoz olyan kárt, amely csak egy hardverkomponens cseréjével orvosolható.

AOL trójai programok lopnak információkat és fertőznek meg e-maileket.

A „VBS.Rabbit" a Windows Scripting Host-ot használja.

1999. A „W97M/Melissa" féreg nagy cégek mailszerverét bénítja meg. Word dokumentumokat száll meg, és arra használja az MS Outlookot, hogy elküldje magát e-mail csatolmányként.

A polimorf „W32/Kriz" vírus átírja a Flash BIOS-t, kitörli vagy tönkreteszi a CMOS memóriát, és átírja az adatokat az összes meghajtón.

A „VBS.BubbleBoy" az e-mail elolvasásakor válik aktívvá. A vírus a Microsoft egyik programkönyvtárának hibáját használja.

2000. Az első globális katasztrófa a weben: az „I love you" féreg világszerte sok milliárd dolláros kárt okoz. Ez volt az első vírus, amelyik önállóan terjedt az interneten. Világszerte omlottak össze a vezetékek és a mailszerverek. A vírus egy egyszerű Basic script.

2001. A férgek éve. A Kournikova vírus az év legsikeresebb férgévé válik. Amennyiben a felhasználó meg próbálja nyitni az

„AnnaKournikova.jpg.vbs" csatolt fájlt, a féreg bemásolja magát a Windows könyvtárba, és az MS Outlook-on keresztül szétküldi magát az összes itt található címre.

A Back Orifice-t és a NetBus-t Remote-Access eszközként hackerek számára írták. Most az ilyen Remote-Access programok egyre több funkciója vándorol a vírusokban.

A „Code Red" féreg világszerte megszállja az NT4 szervereket. Webszerverek között terjed.

2002. A járványok éve: 12 nagyobb és 34 kisebb fertőzés állapítható meg.

Az agresszív „Nimda" féreg randalíroz a weben. Elterjedéséhez nincs szükség semmilyen felhasználói cselekvésre. E-mailen érkezik, vagy az idegen számítógépek hálózatán keresztül fészkeli be magát. Miatta összeomlanak a weboldalak és megosztja a helyi meghajtókat.

A „W32/SirCam" az első olyan féreg, amely rendelkezik egy saját mailszerverrel (AMTP-Engine). Önállóan átmásolja magát a hálózatban található meghajtókra, és ott aktívvá válik.

A „Spida" megfertőzi az SQL szervert.

A „Slapper" világszerte Linux-rendszerek tízezreit fertőzi meg.

A kommersz „Mailware" növekszik, bizalmas adatokat és jelszavakat szerez meg.

Tíz károkozó közül hat internetféreg. A legtöbb esetben az Internet Explorer-en keresztül érkeznek. A „Klez.H" és a „Klez.E" szabályosan tombolnak.

2003. Sobig.A, egy egész család első férge, forgalomba kerül.

Az eddig elképzelhetetlen víruskatasztrófa: 10 perc alatt a Slammer az összes Microsoft szerver 90%-át megbénítja a neten. Nem módosítja az érintett gépeket, de az UDP-protokoll-Stack lefagy. Ennek következményeként a szerver az 1434 UDP porton keresztül véletlen IP címekre küldi a vírust.

Felbukkan a Blaster, minden idők legsikeresebb internetférge. A Microsoft RPC-k (Remote Procedure Calls) gyenge pontjain keresztül terjed.

Porondra lép a Sobig.F, a férek hatodik verziója. A szerző egy spamküldő címlistáján keresztül indította útnak, és ezzel teljesen megbénította az e-mail forgalmat.

7.2 Vírusszakértők szűkítik a támadási ablakot

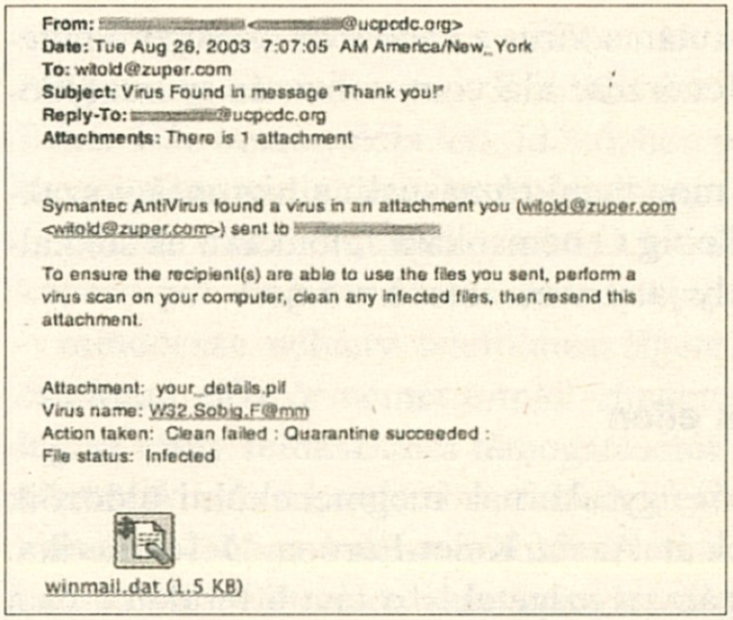
A vírusprogramozók és a hackerek gyakran kihasználják a szoftverek ismert gyenge pontjait. Általában a támadások röviddel a gyenge pontok felfedezése után történnek. „A gyenge pont felfedezése és ennek egy bizonyos fenyegetés általi nem engedélyezett használata között eltelt időt támadási ablaknak nevezzük" – fejti ki Trilling. Például a Nimda és a Slammer férgeknek a támadási ablaka több hónap volt, így a szoftverek gyártóinak elegendő idejük volt arra, hogy kifejlesszenek egy patch-et és figyelmeztessék a felhasználókat. Általában a támadások csak a gyenge pontok nyilvánosságra hozatalát követő hat hónappal történnek.

Trilling fejlődést vár a professzionálisabb vírusprogramozást illetően is. „A támadók jobb erőforrás-tartalékokkal rendelkeznek, célirányosabban járnak el, és gyorsabban kihasználják a gyenge pontokat, mint az az amatőrök számára eddig lehetséges volt" – jellemzi Trilling a fenyegetés új fajtáját.

A jövőben ezért sokkal rövidebb támadási ablakokkal kell számolnunk. Minél jobb a támadók pénzügyi felszereltsége, annál nagyobb tartalékokkal rendelkezik, hogy újabb gyenge pontokat fedezzen fel, és hogy új kártevőket programozzon. Ez végezetül elvezethet a végső támadáshoz a nulladik napon. „A nulladik napi támadás akkor áll fenn, ha közvetlenül a gyenge pont felfedezése után megtörténik a támadás, és így a szoftvergyártóknak, a számítógép rendszergazdáknak és a felhasználóknak nem marad idejük a reagálásra" – vélekedik Steve Trilling. Sajnos a jövőben azzal kell számolnunk, hogy a hálózaton keresztül érkező támadások néhány másodpercen belül megtörténnek.

7.3 A vírusok és a spamek összeolvadása

A szakemberek aggodalommal figyelik a vírus és a spam problématerületének egybeolvadását. „A tömeges e-mailek világára nagy nyomás nehezedik a világszerte folyó kezdeményezések által, hogy betiltsák a spam küldését betiltsák" – ismerteti *Christoph Fischer* a kiindulási helyzetet. Azonban félő, hogy ennek az lesz a következménye, hogy a spamküldők más platformokra térnek majd át, s például vírusok lesznek a


From: [redacted]<[redacted]@ucpcdc.org>
Date: Tue Aug 26, 2003 7:07:05 AM America/New_York
To: witold@zuper.com
Subject: Virus Found in message "Thank you!"
Reply-To: [redacted]@ucpcdc.org
Attachments: There is 1 attachment

Symantec AntiVirus found a virus in an attachment you (witold@zuper.com <witold@zuper.com>) sent to [redacted]

To ensure the recipient(s) are able to use the files you sent, perform a virus scan on your computer, clean any infected files, then resend this attachment.

Attachment: your_details.pif
Virus name: W32.Sobig.F@mm
Action taken: Clean failed : Quarantine succeeded :
File status: Infected

winmail.dat (1.5 KB)

Figyelmeztetés egy válasz e-mailben: a Symantec AntiVirus W32.Sobig.F vírust talált

jövőben a spamek szállítóeszközei. A vírusok célja csak a fertőzött gépek profitorientált használata. Ezzel magyarázható a spamek és a vírusok egyre nagyobb mértékű összefonódása: a vírusírók olyan szoftvereket (úgynevezett „Ratware"-t) használnak az új vírusok hatékony elterjesztésére, amelyekkel eddig a spameket küldték el. A spamküldők ezzel szemben trójai programokkal vagy olyan linkekkel látják el levélszemeteiket, amelyek automatikusan megnyíló, drága pornóoldalakra vezetnek.

A *Sobig.F* féreg már lehetne egy olyan vírusszállító tesztplatformja, amely célirányosan megkaparintja a PC-ket, hogy spamküldőként használja ezeket. A károkozó célja a backdoor-összetevő telepítése, amely lehetővé teszi a hozzáférést egy proxy szerverhez. Az „Open Proxy"-n keresztül akadály nélkül küldhetünk spam mailt hamis feladóval. A Sobig.F a múlt évben iszonyatos tempóban terjedt. A MessageLabs, egy e-mail biztonsági megoldásokat kínáló cég az üzleti szektorban, már az első 24 órában több mint egymillió Sobig.F mailt talált.

Először a féregnek minden tökéletesen ment: a Sobig.F olyan gyorsan terjedt, mint egy járvány. Azonban ironikus módon éppen ez a hatékonyság lett bukásának oka. Az eddig ismeretlenül nagymértékű vírusáradat láttán az egész világ vírusszakértői összefogtak, és így képesek voltak hatástalanná tenni a Sobig.F terjedésének irányítócentrumaként működő weboldalakat, mielőtt még befejeződött volna a vírus második

letöltési fázisa. A teljes telepítés után a vírus a backdoor összetevőin keresztül más IP címeket is az ellenőrzése alá vont volna, és spamküldőként használta volna ezeket.

A helyzet azért cseppet sem mondható rózsásnak: a biztonsági szakemberek attól tartanak, hogy a Sobig.G nemsokára felbukkan és sokkalta hatékonyabb lesz, mint a tavaly január óta létező elődje.

7.4 Harc az online bűnözés ellen

A vírusok és a spamek küldői úgy akarnak megmenekülni üldözőik elől, hogy más országokba térnek át. Ázsia, Kelet-Európa, Dél-Amerika, a Karib-szigetek, különféle magányos szigetek – a távoli területek és a saját törvényekkel rendelkező bizarr idegen világok az izgalmas ügynöktörténetek szívesen látott színterei. Azonban egyre gyakrabban vezetnek a számítógépes bűnözés digitális nyomai is ide, már amennyiben a kusza adathálózatokon keresztül ez egyáltalán követhető a kiindulási pontig. A gyermekpornográfia és a vírusok küldői, valamint különféle online csalók is ilyen helyeken találnak menedéket.

Azonban itt sem maradnak minden esetben érintetlenek. Amíg a filmekben James Bondot a helyszínre küldik, hogy kifüstölje a fészket, addig a nemzetközi online bűnözés elleni harc detektívjei csak a kagyló után nyúlnak. Ami úgy hangzik, hogy akár egy ügynök-thriller egyik epizódja is lehetne, valóságos: nagyjából kéttucatnyi, a világ különböző pontjairól származó számítógépes szakemberekből álló titkos társaság felvette a harcot az adathálózatok gonosztevőivel szemben. Működésük bázisa nem valamilyen szervezet vagy hivatal, hanem kizárólag az egymás közötti jó személyes kapcsolatok. Ezek saját maguk cselekszenek, gyakran a tulajdonképpen illetékes hivatalok és az előírt folyamatok bevonása nélkül.

„A szolgálati út túl lassú, ezért gyakran nem hivatalos utakon járunk" – kommentálja *Christoph Fischer* az eljárás mozgatórugóját. Ha a hackerek nemzetközileg együttműködnek, akkor az ellenkező oldalnak is ezt kell tennie. Nevek alig kerülnek említésre, és a kontaktszemélyek listája sem létezik. A lényeg a hallgatás.

E kör egyik kiemelkedő személyisége az amerikai *Harold Smith*. Először az FBI-nál, majd később az Interpolnál nyomozott, gyermekporno-

gráfia ügyben. Az ebben az időben kialakított kollegiális kapcsolatainak még ma is hasznát veszi. Későbbi útja a Microsofthoz vezetett, majd a Fehér Ház tanácsadója lett. Időközben újra visszatért a szabad gazdaságba: az eBay szolgálatában a biztonsági területért felelős.

Smith is ott volt, amikor a kör a közelmúltban újra bebizonyította ütőképességét, és három kontinensen keresztül buktatott le online csalókat – mindössze néhány telefonbeszélgetéssel. A hamisított eBay oldalak csalására először német e-mail címzettek lettek figyelmesek. Az állítólag az eBay felhasználói támogatásától származó e-mailek mögött a beavatottak már a header-ben felfedeztek egy koreai szervercímet. Azzal a kifogással, hogy valami probléma lenne az accounttal, tömeges üzenetek hamisított eBay oldalakra irányították át a felhasználókat. Itt azután nemcsak az eBay felhasználó nevet, jelszót, nevet és születési dátumot szerezték meg a vásárlóktól, hanem egyidejűleg a hitelkártyaadatokat és a PIN kódot is. Smith csapata közbelépett, s amikor a szaksajtó még csak figyelmeztetett az egyik legnagyobb csalási trükkre, akkor már kattantak is a bilincsek egy koreai lakás pincéjében.

Persze nem minden esetben kell rögtön támadni. Amennyiben lehetséges, a gyanúsítottakat egy ideig megfigyelik, hogy minél többet tudjanak meg a módszereiről és szokásairól. „Az ügyes csalók átszelik az országokat, hogy lehetőség szerint eltüntessék a nyomaikat a hálózatban, mások ellenben nagyobb problémák nélkül elkaphatók" – tudatja *Fischer,* majd hozzáfűzi: „csak ismerni kell a megfelelő embereket a megfelelő helyeken".

Amúgy a vírustámadásokat illetően is gazdag tapasztalatokkal rendelkeznek. Néha szerencséjük van, és be tudják bizonyítani, hogy elindítottak egy károkozót. Ha egy vírus olyan gyorsan terjed, mint például az *SQL-Slammer*, amely a kezdetekben 8,5 másodpercenként megkettőződött, akkor a legjobb vírusvadászoknak is alig van esélyük arra, hogy időben reagáljanak. „A Slammer tulajdonképpen egy egész primitív rész, ám ez okozza a legnagyobb bosszúságot" – foglalja össze Fischer azt a 15 percet, amelyben az egész internet gyakorlatilag bénultan állt. Szerencsére a károkozó a behatolásra egy olyan portot használt, amelynek nincs különösebb jelentősége az internet szempontjából, így ezt egyszerűen lehetett blokkolni.

A Slammer néhány óra alatt világszerte megszállta a rendszereket. A *Symantec* Internet Threat Security jelentésében abból indult ki, hogy az ilyen férgek tovább terjednek, ami a hálózatok túlterheltségéhez, valamint az adatforgalom korlátozásához vezet. Nézzük most meg közelebbről, hogyan is bénította meg a Slammer az internetet!

1. Behatolás: A Slammer egyetlen UDP-adatbáziscsomagnak álcázza magát, amely ártatlan adatbázis-lekérdezéseket végez. A TCP6IP-vel ellentétben ennél a protokollnál nem várunk kézfogásra, mielőtt kicserélésre kerülnek az adatok. A String 04 első bájtja közli az SQL szerverrel, hogy a következő adatok tartalmazzák a keresett adatbázis nevét. A Microsoft specifikációi szerint ez a név legfeljebb 16 bájt hosszúságú és 00-val végződik. A Slammer csomag bájtjai azonban túlfutnak, mert a kód nem tartalmaz 00-át. Az SQL szerver ezért mindent felvesz a memóriába.

2. A számítógép átprogramozása: A 01-sorozatok a féreg elején meghaladják a 128 bájtot, és átfolynak a szomszédos stack-be. Ez durván kifejezve a számítógép következő feladatainak listája. A számítógép átírja az eddigi utasításait az új parancsokkal, amelyeket a Slammer rutinlekérdezésnek leplezett. A számítógép átprogramozza magát, anélkül, hogy ezt észrevennénk.

3. További áldozatok keresése: A Slammer létrehoz egy véletlen IP címet, hogy egy másik, bármilyen számítógépet vegyen célba az interneten. A véletlenszerű választáshoz azoknak az ezredmásodperceknek a számát veszi, amennyi eltelt a CPU rendszer-órajelében, és ebből generál egy IP címet.

4. Sokszorosítás: A Slammer elküldi a saját kódját a véletlenszerűen létrehozott IP címre. A megfertőzött számítógép elkészíti ennek másolatát, és új címet generál.

5. Ismétlés: A Slammer újra kezd mindent, hogy rögtön megtámadjon egy újabb számítógépet. Hogy ne pazaroljon időt, nem feji meg mégegyszer a rendszerórát, hanem csak a már a memóriában található cím bitjeit keveri meg, és ebből állít elő új címet.

7.5 A nyúl és a sün

A Magdeburgi Egyetem gazdaság-informatikai munkacsoportjának munkatársa, *Andreas Marx* vírusszakértő számára a vírusprogramozók-

nak és az antivírus szoftverek gyártóinak működése a nyúl és a sün közötti versenyfutáshoz hasonlítható: „A károkozók programozóinak a világ összes ideje a rendelkezésükre áll. Kódjaikat teljes nyugalomban tesztelhetik, optimálhatják és álcázhatják. Eközben akár aktuális AV-szoftvereket is bevonhatnak tesztelési környezetként." Az ellenszerek esetében a cégek azonban nyomás alatt vannak, méghozzá jelentős időnyomás alatt. „Nemcsak az összetettség tör össze bennünket, hanem az új vírusok sokasága is" – mondja Marx. A 20 új vírus esetében, amennyi jelenleg naponta felbukkan, sosem lehet naprakész az ember.

A valóban új vírusok azonban még inkább ritkaságszámba mennek. A legtöbb esetben módosított régi ismerősökről van szó, amelyek új változatban bukkannak fel. Úgy módosították őket, hogy csak a szövegsorokon változtattak, vagy az új álcázás miatt alig felismerhetők. Ha az összes változatot listázzuk, akkor a ma ismert vírusok száma legalább 90 ezerre rúg.

Nagy ismeretséget ezek közül azonban csak néhány ér el. A kevésbé elterjedt károkozók azonban egyáltalán nem veszélytelenebbek. Ezekhez olyan „gazfickók" tartoznak, amelyeket egyáltalán nem a tömeges elterjedésre programoztak, hanem célirányosan egy bizonyos helyen szeretnének kárt okozni.

7.6 Nem tréfa: veszély az atomerőművekben

Vannak olyan vírusok, amelyeket célirányosan ipari szabotázsokra és kémkedésre használnak. Ha egyszer helyzetbe kerülnek, bizalmas adatokat küldenek ki egy cégből, vagy egész üzemeket bénítanak meg. Különösen alattomosak azok a vírusok, amelyek manipulációi nem rögtön észrevehetők. Míg egy nyilvánvaló kár esetében segíthetne egy backup, addig a károkozók heteken és hónapokon keresztül megváltoztatják az adatokat.

Persze nemcsak azok a cégek veszélyeztetettek, amelyeket a vírustámadások általi gazdasági károk fenyegetnek. A biztonsági területek, például az atomerőművek, nem védettek a hackertámadásokkal szemben. Így jutott be a Slammer féreg az Egyesült Államok-beli Davis-Besse atomerőműbe, és ott 5 órára megbénította a felügyeleti számítógépet. Hogy egy kikapcsolt erőműről volt szó, az inkább csak véletlen volt.

Andreas Marx ismeri az elvi problémát: „Az amerikai erőművekben Windows számítógépeket alkalmaznak, mert ezeken mindenki kiismeri magát." Mivel a biztonságreleváns rendszerek nem teljesen lekapcsolhatók, és a folyamatirányítás és az internetcsatlakozással ellátott vállalati számítógépek között is van kapcsolat, a rendszerek a Microsoft termékek biztonsági falában található réseken keresztül megtámadhatók.

7.7 Nincs tökéletes vírus?

A vírusok növekvő fenyegetése ellenére *Christoph Fischer* a következőt vallja: „Nincs tökéletes vírus." Tapasztalatok szerint a legtöbb vírus a nem kívánt mellékhatásokkal árulja el magát. „Minden nagyon bonyolulttá vált, a vírusprogramozás is" – mondja a vírusvadász, majd imamalomként ismételgeti személyes tanácsait: „vírusszkennelő telepítése és backupok elvégzése, emellett hagyjunk mindent a lehető legegyszerűbben. Ehhez tartozik az is, hogy ne küldjünk minden szemetet e-mailen keresztül szerte a világba, és egyáltalán ne is kattintsunk ezekre." Azt is javasolja, hogy ne végezzünk el minden újítást, hanem egy új szoftver esetében először is várjuk ki, hogy nem bukkan-e fel valamilyen biztonsági kockázat az első hét után. Valójában a vírusprobléma teljesen más számítógép-struktúrákkal lenne megoldható. „Az egész Windows- és Unix-világot, a Linuxot is beleértve, le kellene váltania egy valami teljesen újnak" – summázza *Fischer,* jól tudva, hogy ez minden, csak nem reális. De már azzal is sokat nyernénk, ha a rendszergazdák figyelnének arra, hogy telepítsék az aktuális biztonsági patch-eket.

7.8 További információk

Azoknak, akiket mélyebben érdekel e fejezet témája, összegyűjtöttünk néhány jól használható webcímet.

- **www.cert.org**
- **www.nai.com**
- **www.symantec.com**
- **www.kaspersky.com**
- **www.f-secure.de**
- **www.trendmicro-europe.com**
- **www.messagelabs.com**
- **www.sicherheit-im-internet.de**
- **www.bsi.de**
- **www.ccianet.org**

8 Biztonsági adatmentés

Elismerjük, a PC-s hardver ma már nagyon megbízható, ritka a PC-hibák miatt bekövetkező adatvesztés. Az adatmentés témáját mégsem vehetjük könnyedén, hiszen adataink elveszhetnek vírustámadás, programhiba vagy akár hibás egérkattintások következtében is.

Vajon hova lettek az adóbevallás adatai, a számlaadatok vagy az utolsó nyaralás képei? Üres a *Dokumentumok* mappa és a Windows Lomtára is. Jó, ha egy ilyen helyzetben megbízható biztonsági mentésre támaszkodhatunk. De hogyan menthetjük adatainkat a legkedvezőbben? Hogyan lehet az adatokat és a programokat szétválasztani? Milyen média a legalkalmasabb: flopik, ZIP-drive, CD, DVD, merevlemez vagy szalagos meghajtó? Speciális programra van szükség, vagy talán a Windows csomagjában is akad megfelelő? Szerencsére ez az egész sokkal egyszerűbb, mint amilyennek első pillantásra tűnik. Mert a legtöbb PC már rendelkezik a megfelelő hardverrel és szoftverrel a megbízható adatmentéshez.

Előrebocsátjuk: olyan, hogy „a" legjobb biztonsági adatmentés, nem létezik. Mert amilyen különbözőek a PC-k és felhasználási területeik, olyan különbözőek lehetnek azok a módok is, amelyekkel a leghatékonyabban hajthatjuk végre az adatbiztosítást. Ezért most néhány, a gyakorlatból vett tipikus példa következik tippekkel és trükkökkel a hatékony biztonsági mentéshez.

8.1 Egyedi PC, elsősorban Office-alkalmazásokkal

Ha a PC-t főleg Office-alkalmazásokhoz, mint amilyen a szövegszerkesztés, táblázatkezelés, e-mail és internet, használjuk, akkor a tárolt adatmennyiség általában néhány száz Mbájtnyi – ebben az esetben nem érdemes speciális eszközt vásárolni az adatmentéshez. Használjuk elsősorban a CD-írónkat erre a célra. Flopit a túl kicsi tárhelykapacitás, társebesség és megbízhatóság okán nem érdemes használni, a nagyobb kapacitású, 250 vagy 750 Mbájtos ZIP-meghajtók pedig túl drágák és lassúk.

Ha minden adatunk saját merevlemezen vagy partíción van, gyorsan el tudjuk intézni a biztonsági másolat CD-re írását: nem kell körülményesen több helyről összeszednünk az adatokat, hanem egyetlen kattintással a teljes meghajtót, illetve mappát kiírathatjuk. Lehetőleg CD-R-eket használjunk a mentéshez, a CD-RW-k használata a gyakorlatban sajnos még mindig olvasási-írási problémákat okoz, különösen, ha a CD-RW-ket különböző írókban különböző programokkal kell tudni olvasni. Ezen kívül így automatikusan felépítünk egy biztonságimásolat-archívumot, és így a régebbi adatállományokhoz is visszanyúlhatunk.

Az adatok CD-re mentésének megvan az az előnye, hogy nem szükséges hozzá külön backup program. A megszokott programjainkkal dolgozhatunk, az egyes fájlok visszatöltésére pedig a Windows Intéző szolgálhat.

Hogy milyen gyakran hajtunk végre biztonsági mentést, az attól függ, hogy milyen gyakran viszünk be új adatokat vagy szerkesztjük a meglévőket. Ahhoz azért szokjunk hozzá, hogy az adatainkat kéthetente CD-re írjuk.

Ha lezártunk egy fontos projektet, például adóbevallást, költségelszámolást vagy álláshirdetésre jelentkezést, mentsünk a kéthetes mentési cikluson kívül is.

Az archív CD-ket tároljuk napfénytől védett, száraz helyiségben. Azokat a CD-ket, amelyeken nagyon fontos adatok vannak, legjobb, ha a lakásunkon kívül tároljuk egy példányban – így még ha beáznánk vagy tűz ütne ki, sem fogjuk még az adatainkat is elveszíteni. A biztonsági mentéshez így évente kereken 25 CD-re lesz szükségünk, a 100–150 Ft körüli CD-árral számolva így nem adunk ki 2500–3750 Ft-nál többet adatbiztonságra. És ennyit bizony megér!

8.2 Egy power-user különálló PC-je

Ő az, aki nemcsak a szokásos Office-alkalmazásokhoz használja a PC-t, hanem a digitális fényképezőgépnek köszönhetően fotóalbumot is tárol komputerén, s számítógéppel szerkeszti a videóit, számos MP3 vagy WMA fájlja van, és egyébként is számtalan tárhelyigényes programmal dolgozik. Az adatmennyisége jócskán 1 Gbájt feletti, és állandóan növekszik.

Nála az adatmentés legegyszerűbb eszköze a DVD-író, amelyet a videoszerkesztéshez már amúgy is használ. Egy DVD-re 4,7 Gbájtnyi adat fér, ez sok területen kielégítő, különösen, ha a videók már amúgy is DVD-re vannak írva, így ezeket nem kell még egyszer menteni. A DVD-nek is megvan ugyanaz az előnye, mint a CD-nek: az írásához egy már ismert alkalmazást használunk. Az egyes fájlokat néhány egérkattintással vissza lehet tölteni. Itt is teljesen automatikusan épül fel az archívum, és bármikor visszanyúlhatunk a régebbi adatállományokhoz. Ha naponta sok fájl változik, legalább kéthetente készítsünk biztonsági másolatot, de még jobb, ha hetente tesszük ezt. Az írható DVD-lemez darabja mostanában 450–600 forint, az adatbiztonság így évi 12–32 ezer forintba kerül. A DVD-ket, a CD-kkel megegyezően, napfénytől védve, száraz helyiségben kell tárolni, így még néhány év múlva is használhatók maradnak az adatok.

Ha az adatmennyiség meghaladja egy DVD kapacitását, használjunk az adatmentéshez egy külső merevlemezt. Ezt a PC USB 2.0 vagy FireWire (IEEE 1394) portjára csatlakoztatjuk, és ezután ugyanúgy áll rendelkezésre a PC-ben, mint egy beépített meghajtó. A fájlokat most kényelmesebb a Windows Intézővel a belsőről a külső meghajtóra másolni. Mivel a másolás – ha egyszer elindítottuk – automatikusan lefut, az adatmentést akár az ebédszünetben is elvégeztethetjük.

A 80 Mbájtos külső merevlemezek jelenleg 25–45 000 Ft-ba kerülnek, de vannak 40, vagy akár 200 Gbájtos modellek is. Ha nincs szükségünk a teljes kapacitásra a mentéshez, hozzunk létre a külső merevlemezen például három, Backup-A, Backup-B és Backup-C mappát – az adatmentés így történhet ciklikusan mindig egy másik mappába, és időben visszafelé három verzió fog a rendelkezésünkre állni.

Az egyes fájlok visszatöltésére itt is a megszokott Windows Intéző szolgál, külön programra nincs szükség. A külső merevlemezt az adatmentést követően válasszuk le a PC-ről és tároljuk biztos helyen, ahol védve van nedvességtől, rezgésektől és lökésektől.

8.3 Több PC peer-to-peer hálózatban, üzleti környezetben

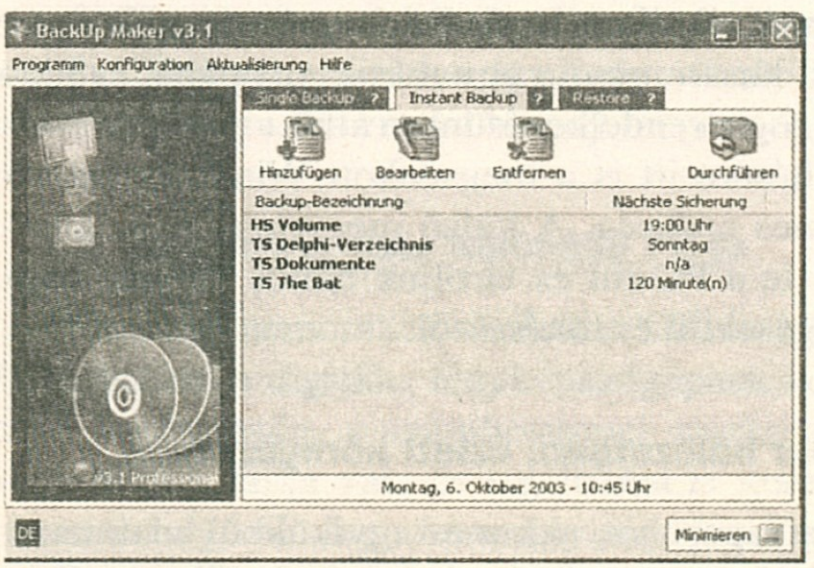
Ha több PC van hálózatba kapcsolva, akkor az egyikükből adatmentő PC lesz. Ez a PC, a megfelelő megosztásoknak köszönhetően, a többi

PC minden adatát eléri. Az adatmennyiségtől függően használhatunk, mint a 8.2-es esetben, DVD-meghajtót vagy külső merevlemezt. Az adatokat DVD-meghajtó használatánál hetente mentsük, a DVD-ket a gyors adatelérés kedvéért megfelelően archiváljuk. Ha merevlemezre történik az adatmentés, akkor naponta kell végrehajtani. Ilyenkor nemcsak egy, hanem legalább három merevlemezt használjunk. Két merevlemezt cserélünk rendszeresen minden héten, a harmadikra hó végén mentünk.

Ha négy merevlemez áll rendelkezésre, ezeket ciklikusan négyhetente használhatjuk. Ennek az az előnye, hogy visszanyúlhatunk adataink különböző verzióihoz, és így a véletlenül felülírt fájlokat is helyre tudjuk állítani. A különösen kritikus adatokat, mint a könyvelési vagy pénzügyi adatok, például a havi zárások után még CD-re vagy DVD-re is menthetjük.

Az adatok biztonsági mentésének leegyszerűsítésére itt már érdemes speciális backup programot használni. A Windows XP csak a Professional verzióban van felfegyverezve backup programmal, amelynek a kezelése azonban sok mindennek, csak könnyen érthetőnek nem nevezhető. Ezen kívül a backup fájl formátumát csak maga a Windows XP Professional tudja feldolgozni, egy másik, nem Professionallel telepített PC-re nem tudjuk visszatölteni.

Más a helyzet a BackUp Maker programmal: a 40 eurós kedvező áron kapható segédprogram (a magánszemélyek számára készült verzió ingyenes!) minden fájlt egy tömörített ZIP fájlba ment. A ZIP fájlt gond



A Backup Maker program hatékony segítséget jelent az adatmentésnél

nélkül meg lehet nyitni például a WinZip-pel, a Windows XP a ZIP-fájl tartalmát még segédprogram nélkül, közvetlenül is el tudja érni. A BackUp Maker támogatja minden fájl mentését, és csak a módosított fájlok mentését is, és egyenesen a merevlemezmentésre találták ki. A rugalmas, idővezérelt backup-készítést ugyancsak támogatja, így például elvégeztethetjük ezt az ebédszünetben, így senkit sem zavar munka közben. A különösen fontos adatokat akár szabályos időközönként is menthetjük, ez 5 perctől 300 percig állítható.

8.4 Több PC, külön szerverrel

Ha a hálózatban külön szervert használnak, azon történik a központi adattárolás. Ebben az esetben minden felhasználónak van a szerveren egy saját privát mappája (*Home Directory-ja),* amelyben minden adatát elhelyezi. A privát mappákat naponta menteni kell. Az adatmentés, ugyanúgy, mint a 8.3-as esetben, történhet segédprogramokkal, mint amilyen a BackUp Maker, külső merevlemezekre. A külső merevlemezt közvetlenül a szerverre csatlakoztatják, így az adatokat nem kell a hálózaton közlekedtetni. A merevlemez hétfőtől péntekig csatlakoztatva marad, ez alatt az idő alatt naponta minden változtatás felkerül rá (növekményes adatmentés). Péntekenként cserélik a merevlemezt, és teljes körű mentés következik. Mivel a szerver egész nap be van kapcsolva, a mentést végeztethetjük idővezérléssel éjszaka is, anélkül, hogy a munkát meg kellene szakítani, vagy fennállna a veszélye annak, hogy egy alkalmazás még fájlokat nyit meg, amelyeket nem lehet menteni.

Ehhez a mentési módozathoz hetenkénti cserénél legalább négy külső merevlemezre van szükség (kettőre a növekménymentéshez és kettőre a teljes körű mentéshez), de még jobb nyolc lemez egy havi ciklushoz. Ennek a mentési módszernek az a nagy előnye, hogy egyes fájlokat és komplett könyvtárakat is gyorsan és egyszerűen tudunk visszatölteni. A négy merevlemez költségét nem növeli tovább lemezek vagy más médiumok folyamatos költsége.

Önálló szerver használatánál lehet streamereket (szalagos egységeket) is használni, amelyekre éjjelente automatikusan minden adatot mentenek. A streamerek nagy hátránya, hogy – a külső merevlemezhez ha-

sonló kapacitásban – nagyon drágák. Már egy kedvező árú szalagos meghajtó DAT-technikával, csak tömörítetlen 12 Gbájtos tárkapacitással annyiba kerül, mint 6-8 külső merevlemez, egyenként 80 Gbájttal.

Ehhez jön még, hogy az adatmentéshez és visszatöltéshez speciális programot kell használni, egy véletlenül törölt fájl gyors visszatöltése jelentősen komplikáltabb, mint a merevlemezes technikánál. A szalagos egységek előnye: a szalagok kompaktabbak és ellenállóbbak a rázkódással szemben, mint a külső merevlemezek.

8.5 A hasznos ellenőrzés

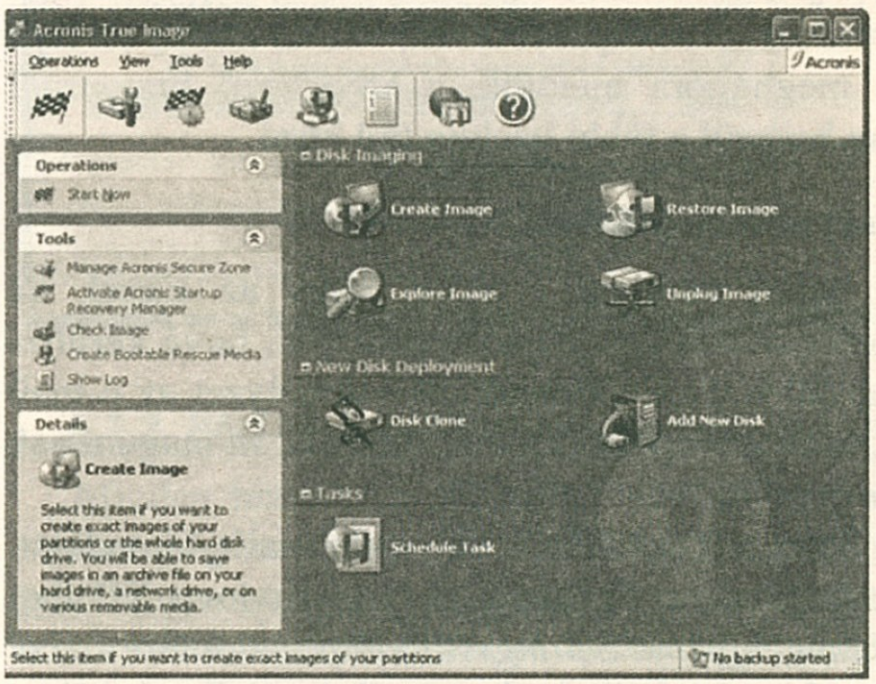
Alapvetően semmilyen adatmentésben ne bízzunk meg, még ha mégoly hihetően is állítja, hogy minden adatunkat tökéletesen mentette. Csak (rendszeres!) sajátkezű ellenőrzéssel szerezhetünk teljes bizonyosságot arról, hogy adataink valóban biztonságban vannak.

Állítsunk vissza a biztonsági mentésből néhány legújabb dátumú fájlt – így biztosak lehetünk benne, hogy az adatmentés valóban betöltötte feladatát, és hogy az adathordozón nem csak „régi" fájlok vannak. Állítsuk vissza a fájlokat egy saját mappában, majd a visszaállított fájlokat hasonlítsuk össze az eredetiekkel. Sajnos a Windows nem kínál funkciót a fájlok összehasonlításához, ehhez egy parancssorablakra és az FC parancsra kell fanyalodnunk (FC = File Compare, FC /? beírásával részletes működési leírást kapunk). Ha az FC parancs a „Nincsenek különbségek" üzenetet küldi vissza, minden rendben van.

8.6 Adatmentés kontra programmentés

Hogy az adatmentés az itt bemutatott módszerekkel optimálisan működjön, ügyeljünk az adatok és a programok szigorú szétválasztására: például használjuk a Windows saját *Dokumentumok* mappáját konzekvensen adataink tárolására; ebbe a mappába ne telepítsünk programokat. Több merevlemez is van a PC-nkben, vagy egy van felosztva több meghajtóra? Akkor tegyük át a Dokumentumok tárhelyét egy saját meghajtóra. Így a programokról és adatokról egészen egyszerű egymástól elválasztva mentést készíteni. A Dokumentumok mappa áthelyezéséhez kat-

tintsunk az *Asztalon* jobb egérgombbal a mappára, és válasszuk a helyi menüből a *Tulajdonságokat*. Megjelenik egy párbeszédablak, amelynek a *Cél* regiszterlapján a *Cél mappa* helyéhez írjuk be az új tárhelyet – vagyis: az új meghajtót. Az adatmentésnél szövegeink, képeink stb. mentése egyértelmű, a programoké azonban már nem ilyen egyszerű. A telepítők a programfájlokat nem csak egy főkönyvtárba másolják, hanem „elosztják" a legkülönbözőbb program- és Windows-mappák között. Ráadásul a telepítőprogram a Windows Registrybe és/vagy más konfigurációs fájlokba is ír adatokat. Ezért a programok, ha csak a főmappát töltjük vissza, nem fognak, ill. nem fognak hibátlanul működni, mert nem tudtunk minden fájlt rögzíteni, vagy Registry-bejegyzések hiányoznak.



Az Acronis True Image program jó választás, ha programot kell mentenünk

Ezért a programok mentéséhez használjunk olyan segédprogramokat, mint a *Symantec Norton Ghost*, az *Acronis True Image* vagy a *Drive Backup* a *Paragon Technologytól.* Ezekkel komplett meghajtókról készíthetünk image-et, ezzel egyben a Windowst (minden szervizcsomaggal együtt) és a programjainkat is menthetjük. Ha minden fontos programtelepítés után készítünk egy új image-et, néhány perc alatt újból előállíthatjuk a teljes rendszerünket. Mivel az adatok egy saját meghajtón vannak, a programok helyreállításánál sem áll fenn az adatvesztés veszélye.

8.7 Profi tippek

Az alábbiakban az adatmentéshez kínálunk néhány jól hasznosítható tippet és trükköt.

8.7.1 Internet Explorer: a Kedvencek mentése

Saját internetcímeket jegyeztünk fel az Internet Explorer Kedvencek menüjében? Minden, a Kedvencekbe bejegyzett internetoldalt megjegyez a Windows XP linkfájlok formájában a *\Documents and Settintgs\<felhasználónév>\Kedvencek* mappában.

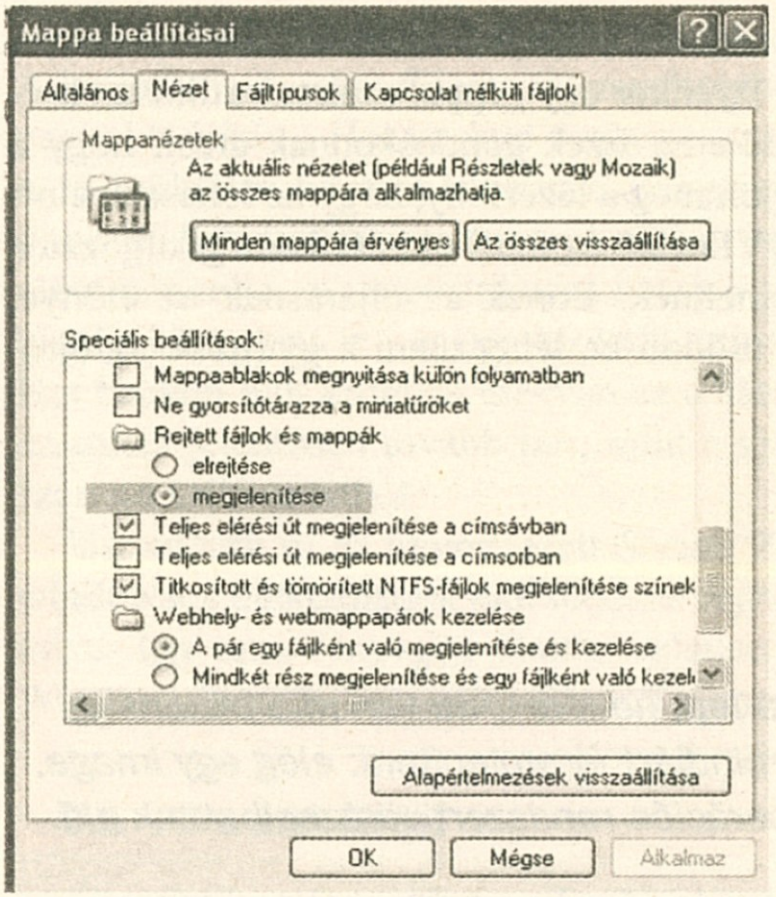
Kedvenceink biztonsági mentéséhez vagy a Kedvencek mappát kell mentenünk, vagy „exportáljuk" kedvenceinket az Internet Explorerben a *Fájl, Importálás és exportálás...* menüpontból. Ha ezután az export fájlt az adatokat tartalmazó meghajtóra mentjük, a következő biztonsági mentéskor automatikusan bekerül a többi backup fájl közé.

8.7.2 Outlook (Express) adatok mentése

Office-programoknál, mint amilyen a Word vagy az Excel, az *Eszközök/Beállítások* menüpontnál könnyen rögzíthetjük, hová kerüljenek alapértelmezésben a fájlok és a sablonok. Más a helyzet az e-mail programokkal, mint az Outlook vagy az Outlook Express: itt magunknak kell gondoskodnunk az e-mail fájlok mentéséről.

Outlook: az Outlook 2000, 2002 és 2003 minden e-mailt, címadatot, feladatot és jegyzetet az *Outlook.pst* fájlban tárol. Ez Windows XP alatt alapértelmezésben a *\Documents and Settings\<Felhasználónév>\Local Settings\Application Data\Microsoft\Outlook* mappában található. Mivel a *Local Settings* mappa rejtett, a fájlt csak úgy tudjuk megtalálni és menteni, ha a Windows Intézőben az *Eszközök/Mappa beállításai/Nézet* regiszterlapon a *Rejtett fájlok és mappák mutatását* bekapcsoljuk.

Outlook Express: A kisebb testvér 5.0, 5.5 és 6.0 verziója Dbx-fájljait a *\Documents and Settings\<Felhasználónév>\Local Settings\ ApplicationData\Identities\{Azonosítószám}\Microsoft \Outlook Express* könyvtárban tárolja. Ezt az elérési útvonalat is csak akkor látjuk, ha a Windows Intézőben bekapcsoljuk a rejtett mappák mutatását.



Kapcsoljuk be az Intézőben a rejtett fájlok és mappák megjelenítését!

8.7.3 Régi CD-k és DVD-k olvashatatlanná tétele

Minden biztonsági mentésnél fölöslegessé válik egy régi CD/DVD, ezeket mégsem dobhatjuk el csak úgy, hiszen a CD/DVD-ken személyes adatok vannak, amelyekhez senkinek semmi köze. Egy ilyen CD/DVD-t a normál háztartási hulladék közé vagy szelektív gyűjtőbe tenni nem ajánlatos. Ezért következzen néhány tipp, hogyan tehetjük tartósan olvashatatlanná a saját magunk írta CD/DVD-ket.

Széttörés: törjük a CD/DVD-t több darabra. Ilyenkor többnyire a CD/DVD rétegei, tehát az adatokat tartalmazó részek is eloldódnak, az egyes töredékeket már senki sem tudja hatalmas ráfordítás nélkül összerakni. Így védjük a legjobban az adatokat.

Összekarcolás: összetörés helyett össze is karcolhatjuk – CD-nél a felső oldalt, amelyen a CD-t rendesen feliratozni szoktuk, DVD-nél mindkét oldalt. Ha csillagformában több, széles és mély karcolást ejtünk, a CD-t normál eszközökkel nem lehet többé elolvasni.

Recézés: a kézzel való összekarcolás helyett mechanikusan is tönkretehetjük a CD/DVD-felületet. Ilyenkor egy géppel szisztematikusan horpadásokat nyomnak a CD-felületre. Ezek gondoskodnak arról, hogy a CD/DVD olvasásakor úgy törjön meg a lézerfény, hogy ne lehessen elolvasni az adatokat. Ha a CD/DVD alsó és felső oldalát is megdolgozza a gép, a fedőrétegek is tönkremennek. Ennek az eljárásnak az előnye, hogy a CD-t teljesen normál módon be lehet tenni a gyűjtőbe az újrahasznosításhoz.

9 Image-programok

Ha a Windows sztrájkba lép, nem árt, ha van róla biztonsági másolatunk. Nem kell mindjárt újratelepíteni: elég egy image, és percek alatt friss operációs rendszert varázsolhatunk elő.

Tönkrement merevlemez, vírus vagy figyelmetlenül törölt fájlok – sokféle oka lehet annak, ha egy jól működő Windows egyszer csak nem indul el többé. Ennek a problémának van egy gyors megoldása, úgy hívják: *image.* Speciális programok biztonsági mentést készítenek a merevlemezekről vagy a partíciókról egy bizonyos időpontban. Az így készített image-fájlból később kompletten minden programmal és beállítással együtt vissza lehet tölteni a rendszert.

Az image-programok eredetileg a profi területhez tartoztak, és főleg rendszergazdák használták őket, hogy több PC telepítését egyforma szoftverekkel gyorsan el tudják végezni. Hogy az otthoni felhasználók is élvezhessék ennek a technikának az előnyeit, a gyártók már egyszerűsített változatokat is kínálnak, amelyek elsődlegesen az otthoni egyedi gépek biztonsági mentésére szolgálnak. Szerencsére a segédprogramok aktuális verziói már elveszítették korábbi „profi természetüket": olyan egyszerűen kezelhetőek, mint ezelőtt soha, a nagy merevlemezekkel is elboldogulnak és akár DVD-re is tudják írni az image-eket. Még a hálózati támogatás is integrálva van a programokba, ráadásul olyan egyszerűen ke-

zelhetők, hogy a kis házi hálózatok tulajdonosainak is az örömére válnak. A különbségek tehát főleg a felszereltségben vannak. Mostanában a legnagyobb újítás a Hot backup funkció: ez lehetővé teszi, hogy a felhasználó működés közben készítsen image-et a bootpartícióról futó Windows mellett (a többi partícióról amúgy is tud). Ez néhány hónappal ezelőtt még teljesen utópisztikusan hatott volna, most mégis ezt a funkciót kínálja két gyártó is – és úgy hirdetik, mint az adatmentés netovábbját. A Hot backup-nak azonban megvan az a hátránya, hogy a mentés és a visszatöltés jelentősen tovább tart, mint a szokásos eljárással, az antiknak számító DOS-módból.

Ugyancsak új az úgynevezett *Secure Zone*, amelyben az image-ek a windowsos hétköznapok elől teljesen rejtve várnak visszaállítási feladatukra. Így nem fenyegeti őket a véletlen törlés, viszont ez a program Windows Intézőn keresztüli elérését is megakadályozza.

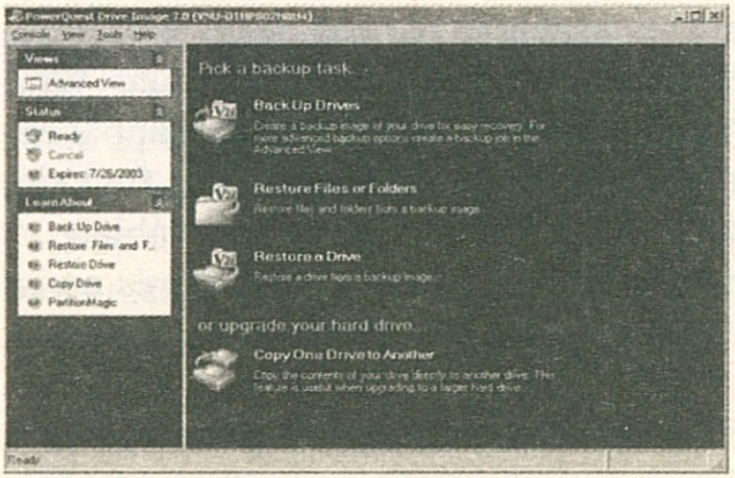
9.1 Fő a stabilitás!

Úgy tűnik, már majdnem sikerült elérni a csúcsot: eltekintve a kisebb bugfixektől, a még nagyobb merevlemezek támogatásától és az új írókkal való teljes kompatibilitástól, már alig akad javítanivaló a programokon. Egyes gyártók még minden bizonnyal optimalizálni fogják a sebességet, igazán új követelményt azonban csak az fog eléjük állítani, ha a Microsoft megjelenteti a Windows Longhornt az új WinFS fájlrendszerrel. Nagy problémát azonban ennek a támogatása sem fog jelenteni. Ezért az image-programoknál a megbízhatóság marad a legfontosabb kritérium, hiszen ha maga produkál lefagyásokat, bugokat és zavart keltő hibaüzeneteket, az hamar megkérdőjelezi egy adatok megmentésére szánt program létjogosultságát.

9.2 Image-programok a tesztlaborban

A négy tesztelt image-program ára 50 és 70 euró között mozog. A teszt középpontjában a megbízhatóság, a felszereltség és a kényelmes kezelés áll, de a munkatempó és a DVD-írási lehetőség is nagy szerepet játszanak.

9.2.1 Drive Image 7

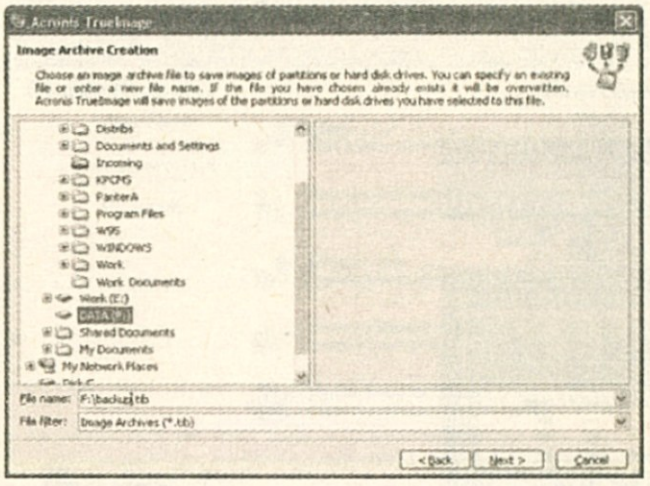


A program, mint már előző verziója is, nagyon kedvez a kezdőknek. Így például van egy alapnézete újoncoknak, és egy bővített a tapasztaltabb felhasználóknak. Fő ütőkártyáit elsősorban az image-fájl létrehozásánál játssza ki. A Drive Image már néhány egérkattintás után nekiindul és létrehozza az image-fájlt az új hot backup funkcióval. Akár tovább is dolgozhatunk a Windows-zal, mindenesetre jelentősen csökkent tempóban. Az elkészítés így tíz percig tartott – nem rossz idő, de azért jobbal is találkoztunk. A visszaállításnál még többet, 12 percet tölt el a Drive Image: először újraindítás, közben a CD-nek a meghajtóban kell lennie. Ne felejtsük el előzőleg átállítani a BIOS-ban a boot-sorrendet a CD-meghajtóra! Ezután elindul a Windows PE, egy lecsupaszított Windows-változat, ami rendesen hagy magának időt a betöltésre. Szükség van még egy telepített *.net-Framework*-re is, amelyet a PowerQuest örvendetes módon a program mellé ad. A Windows PE azonban még többet követel: akinek 256 Mbájtnál kevesebb RAM van a gépében, nem tudja a szoftvert használni.

Ezen kívül a Drive Image 7 csak Windows XP és 2000 alatt működik. A csomagban van azonban a Drive Image 2002 is, amelyet Windows 9x és ME alatt lehet használni. Ha tehát az XP-s gép mellett van egy PC-nk Windows 9x-szel vagy ME-vel, azon a régi verziót használhatjuk.

A funkciókörön nincs kivetnivaló: a felhasználó DVD-re is írhat image-eket, fájlokat oszthat fel, menthet hálózati meghajtóra is, vagy image-feladatokat indíthat a Feladatütemezőből.

9.2.2 True Image 7.0



Az Acronis sok mindent tökéletesített a True Image vadonatúj verzióján, és új tulajdonságokat is beépített. Mindenekelőtt az átdolgozott Windows-felület szúr szemet. Maradt viszont az egyszerű kezelés, amely a kezdőknek sem okozhat gondot. A True Image lehetővé teszi egy „biztonsági partíció" előállítását, amelyről a program egy totális Windows-összeomlásnál tud visszaírni egy image-et. A felhasználónak csak azt kell rögzítenie, hol legyen a védett terület, a többit egy varázslóféle intézi.

A *Startup Recovery Manager*-ből, amely úgy működik, mint egy bootmanager, a Windows bootolás előtti fázisában biztosan vissza lehet tölteni az image-et. Ennél a beállításnál azonban a felhasználó ezt a lefoglalt területet nem tudja a Windows Intézőből elérni.

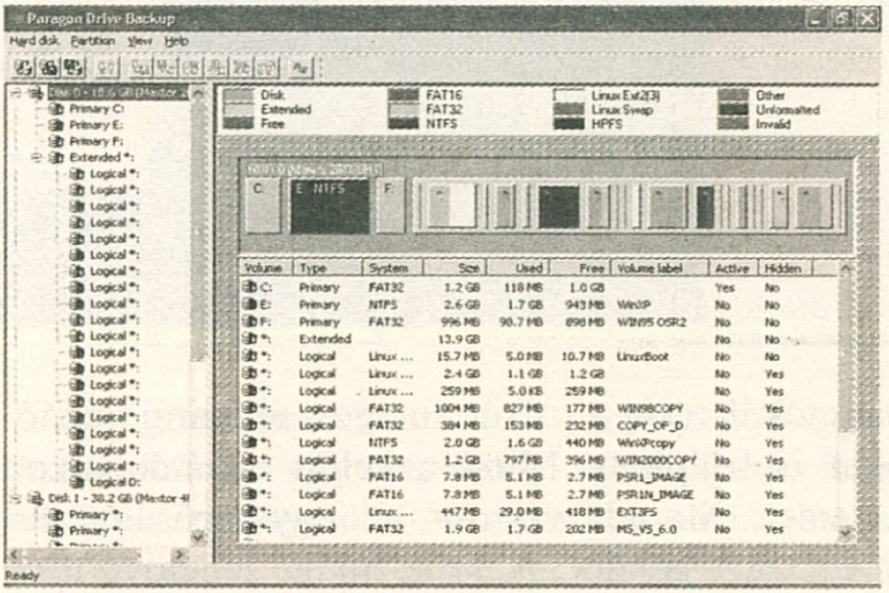
A hot backup funkció is integrálva van: a teszt során nagyon jól működött. Az egyidejű Windows alatti munka azonban csak jelentős teljesítménykorlátozással működik. A bootpartíciók visszatöltése (6 perc) ennek ellenére gyorsabban ment, mint a Drive Image-nél, mivel a True Image nem használ Windows PE-t, hanem Linux-bázison indul el.

Zavaró viszont a visszaállításnál, hogy minden beállításra újból rá kell kattintani. Az írásnál és a tömörítésnél is pontokat vesztett a program: 17 percre volt szüksége az image elkészítéséhez, a tömörítés mind közül a legrosszabb volt.

A DVD-k írásánál problémát okoz, ha előzőleg nem volt UDF-csomagíró szoftver telepítve. Ezzel úgy lehet DVD-t formattálni, hogy

úgy lehessen írni rá, mintha merevlemez lenne. Az „InCD" az Aheadtől (www.ahead.de) ideális erre a feladatra, és szerencsére ingyenes is.

9.2.3 Drive Backup 6.0

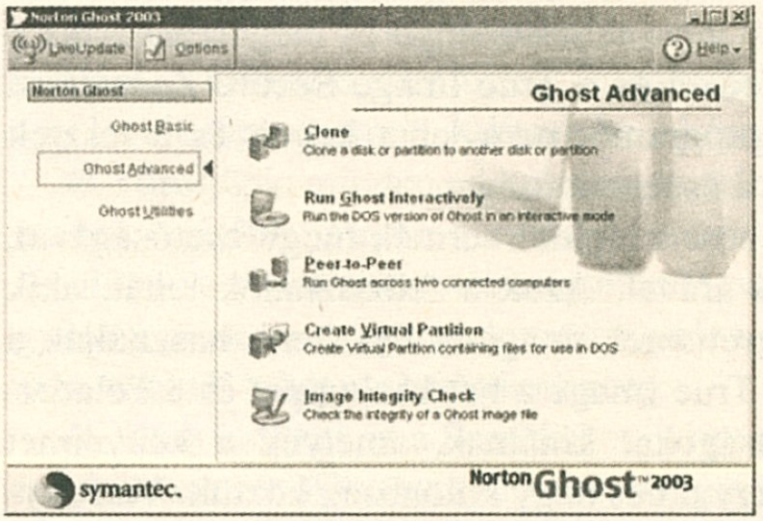


A gyakorlott felhasználók örömüket fogják lelni a *Drive Backup*-ban és annak DOS- vagy Linux-módjában – a bootképes CD-ről mindkettő indítható. Kezdőknek azonban csak a Windows-felület jöhet szóba, amely ugyan nem különösebben intuitív, a Linux-verzióhoz hasonlítva azonban még igazán egyszerűnek tűnik.

Mielőtt image-eket készítenénk, ügyeljünk arra, hogy az *Image felosztása* opció be legyen kapcsolva. Ezen kívül a maximális fájlméretet 2 Gbájtra kell korlátozni, különben előfordulhat, hogy az image-ből a helyreállítás csak hibásan vagy sehogyan sem történik meg. A teszt idején patch még nem állt rendelkezésre.

De ha a programot elláttuk a fenti beállításokkal, utána már minden jól megy. A szoftver gyorsabban ír, mint a True Image és ugyanolyan jól tömöríti az adatokat, mint a Ghost és a Drive Image. Praktikus: arra az esetre, ha a Windows egyszer egyáltalán nem indulna el, ott van a *Midnight Commander* nevű eszköz. Ez még NTFS partíciókra is elérést kínál, és az adatokat egy biztonságos helyre másolhatjuk vele. További extrák nincsenek: sem Feladatütemező, sem hot backup funkciót nem találunk.

9.2.4 Norton Ghost 2003



Az új verzió jócskán megnövekedett, és a felhasználó végre a rég áhított Windows-felületet is megkapja. Ezáltal, most először, a Ghost korlátlanul ajánlható kezdőknek is. Ráadásul egy varázsló végigvezet az image-készítés folyamatán, és sosem hagy bizonytalanságban. Ennek ellenére a program a tapasztalt felhasználóknak is rengeteget kínál: sokszínű konfigurációs lehetőségeket – aki például manuálisan szeretne USB- vagy FireWire-meghajtókat betölteni, az az újrabootolás előtt ezt is megteheti. De az alapkonfiguráció is annyira jól összeállított, hogy tulajdonképpen azonnal indíthatunk vele.

Míg más gyártók az új hot backup funkciót propagálják, a Ghost a régi, bevált technikához kötődik. Mind az image-készítéshez, mint a visszatöltéshez még mindig DOS-módra vált. De aki azt hiszi, hogy a hot backup automatikusan nagyobb tempót is jelent, az erőteljesen téved. A Ghost mindenki más előtt elhúzott: a 4,97 Gbájtos rendszerpartícióhoz a programnak csak hét percre volt szüksége mentésnél és öt percre visszaállításkor – a szükséges újraindítást is beleszámítva.

A tömörítés is meggyőző: a Ghost a legmagasabb fokozaton méretük felére zsugorítja az adatokat. Az image-eket CD-re vagy DVD-re lehet írni. Az író-engine a teszt során problémamentesen működött: 20 perc után a DVD készre írva fordult ki a meghajtóból. A program jó eredményeit nézve igazán fájdalom, hogy még mindig nincs hozzá feladatütemező.

9.2.5 Összefoglaló

A tökéletes image-program talán a Ghost, a Drive Image és a True Image kombinációja lenne: a Ghost teljesítménye és megbízhatósága a Drive Image egyszerű kezelésével és a True Image Secure Zone-jával párosítva. Sajnos ilyen álomprogramot nem lehet kapni, és a tesztelt programok egyike sem érte el a csúcsminőséget.

A valóságban jelenleg a Ghost a legjobb termék megbízhatóságával, gyors tempójával és kedvező árával. Azok a felhasználók tehát, akik gyorsan és biztonságosan szeretnének image-et készíteni, használják a Ghostot. A Drive Image és a True Image a hot backuppal és a Feladatütemezővel érdekes tulajdonságokat kínálnak, amelyek a kényelmet szolgálják. Az áron kívül amúgy nincs nagy különbség köztük. Viszonylag egyszerű a kezelésük, és megbízhatóan működnek. Aki tehát nem szeretne lemondani a bootpartíció működés közbeni biztonsági mentésének luxusáról, gondolkodás nélkül választhatja ezeket a programokat.

A Drive Image jövője azonban kérdéses: azzal, hogy a biztonsági óriás Symantec felvásárolta a gyártó Powerquestet, mindjárt két imagingtool került a programjába. Megtörténhet, hogy a kettőből az egyik fejlesztését leállítja.

A Drive Backup programnak felszereltsége hiányos, és a kezelési komfortja is hagy némi kívánnivalót maga után. Megküzd ugyan a feladatával, de nem olyan egyszerű használni, mint a jobb helyezést elérteket. Az ára a Ghost és a True Image szintjén van, tehát a megfelelő felszereltségnek is ott kellene állnia.

9.3 A rendszermentés stratégiája

Bármilyen csábítóan egyszerűek is a programok, mielőtt hozzákezdenénk az image-ek készítéséhez, ügyeljünk a következőkre. Ha lehet, telepítsünk egy friss Windowst a szükséges programokkal. Hogy a bootpartíció image-e ne legyen túl nagy, erre ne mentsünk más adatokat. Soha ne a bootpartícióra készíttessük az image-eket, különben épp rendszerleálláskor nem jutunk hozzájuk. Az új PC-k szokásos konfigurációja rossz, mert ezekben gyakran egyetlen merevlemez van, és az is csak egy partícióval. Az image-et írjuk ki CD-re vagy DVD-re is.

9.3.1 Tiszta rendszer telepítése

Az ideális egy újonnan telepített Windows.

- Csak azokat a programokat tegyük fel, amelyekre szükségünk van, például az Office-összeállítást. Telepítsük még az internet-hozzáférést és egy levelezőprogramot. Állítsuk be a képernyőfelbontást is.
- Töröljünk minden ideiglenes és telepítőfájlt, amelyek a merevlemezen ragadtak. Ha az aktuálisan meglévő rendszert akarjuk menteni, távolítsunk el minden szükségtelenné vált programot. Új PC-knél a gyártók gyakran telepítenek szükségtelen segédprogramokat vagy reklámot, ezektől tehát szabaduljunk meg.
- Most indítsuk el a Scandisket, hogy megtaláljuk a fájl- és merevlemezhibákat. A Windows töredezettségmentesítésével gondoskodjunk a rendezett merevlemezről.

9.3.2 A merevlemez partícionálása

Ahhoz, hogy értelmesen tudjuk tárolni az image-eket és a backupokat, ahhoz egy második merevlemezre, CD/DVD-íróra vagy partíciókra osztott merevlemezre van szükség. Minden egyéb adat a Windowson és a szükséges programokon kívül, egy másik partícióra való. Egy 120 Gbájtos lemez esetében például a következő felosztás ajánlott:

- Kb. 10 Gbájtos bootpartíció a Windowsnak és a telepített programoknak,
- kb. 5 Gbájtos adatpartíció a leveleknek, a táblázatoknak és az Outlook fájloknak,
- kb. 15 Gbájtos image-partíció az elkészült image-eknek,
- médiapartíció a maradék területtel képeknek, MP3 fájloknak, videóknak és egyéb adatoknak.

A partícionálás a legegyszerűbben speciális programokkal megy, például a *Partition Manager 5.5*-tel, amely a **www.partitionsmanager.com**címről működőképes demoként letölthető. Ezzel kényelmesen felosztathatjuk a merevlemezt. Ügyeljünk arra, hogy az image-ek és a biztonsági mentések partícióit FAT32-es fájlrendszerben formattáljuk. Így biztosítjuk, hogy régebbi DOS-indítólemezekkel is bármikor elérhetjük ezeket az adatokat.

9.3.3 Az image mentése

Alapvető érvényű: a bootpartíciót mindig önmagában mentsük egy image-fájlba. Más partíciókat egy másik image-ben fogjuk össze. Használjuk a *Bootlemez készítése* opciót. Ha már egyáltalán nem indul el a Windows, tegyük be a bootlemezt, amelyről a Windows szinte minden esetben visszaállítható. Mivel a mostani merevlemezek nagy tártelületet kínálnak, nincs szükség arra, hogy egy esetlegesen felkínált tömörítést bekapcsoljunk – a biztonsági mentés és a visszatöltés annál gyorsabban fog menni. Adjunk meg jelszót is.

10 A PC újraélesztése

Sehogy sem akar a Windows úgy elindulni, ahogy megszoktuk? Ebben a fejezetben megmutatjuk, hogyan hozható újból működésbe a PC egy alattomos támadás vagy a rendszer teljes kiesése után.

Bárkivel bármikor megeshet: bekapcsolja a PC-t, és az nem indul el rendesen. A Windows helyett csak egy hibaüzenet jelenik meg szövegmódban, fehérrel feketén. Vagy röviddel a Windows indulása után megjelenik egy párbeszédablak, és a rendszer leáll. Vagy elindul a Windows, de csak „Csökkentett módot" kínál kisebb képernyőfelbontással. Ilyenkor elkel a jó tanács – vagy a most következők elolvasása. Ezúttal ugyan a Windows 2000-re és az XP-re koncentrálunk, sok tipp azonban a régebbi Windows-verzióknál is használható.

Hogy ilyenkor mi a leghelyesebb reakció, az két kérdéstől függ:

1. Mi okozta (vélhetően) a problémát?
2. Vannak-e fontos adatok a merevlemezen?

Ha nyaralásról készült videók, digitális fotók, fontos Word dokumentumok vannak a merevlemezen, először ezeket kell mentenünk, mert később a jó szándékú mentési kísérlet nem ritkán több kárt okoz, mint amennyi előtte volt.

10.1 Az első ellenőrzés: vírustámadás?

Ha épp egy új programot telepítettünk, illesztőkártyát építettünk be vagy külső eszközt csatlakoztattunk, vélhetően a meghajtók okozta változtatások vagy más manipulációk a felelősek. Ilyen esetben gyakran segít a Windows XP rendszer-helyreállítása vagy a bootmenü. Ezekről később még részletesebben szólunk.

Ha semmit nem változtattunk a PC-n, jogosan gyanakodhatunk vírustámadásra. De lehet szó egy véletlenül törölt rendszerfájlról vagy a merevlemez hibás területeiről is. Ilyenkor óvatosan kell eljárnunk, mert egy normál rendszerindításnál egy vírus nagy valószínűséggel aktivizálódik, és további károkat okoz.

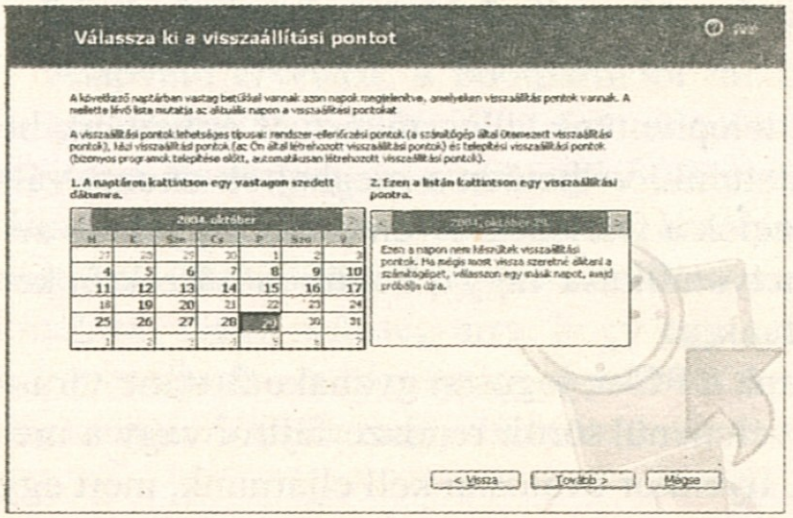
Először végezzünk egy biztonságos bootmédiumról vírusellenőrzést a PC-n, és adott esetben szerezzünk közelebbi információkat a károkozóról. Ha pedig nem vírusról van szó, mindjárt ellenőrizhetjük is a fájlrendszert is a merevlemezen.

10.2 A rendszer-helyreállítás aktiválása

A Windows ME-nél és a Windows XP-nél a Microsoft fixen beépített az operációs rendszerbe egy mentési eljárást: a rendszer-helyreállítást. Ez a segédprogram rendszeresen menti a fontos rendszerfájok állapotát. Ez vagy naponta történik, vagy olyankor, ha új programot vagy meghajtót telepítünk. Így később könnyen vissza tudjuk állítani a Windows egy régebbi állapotát, például egy ártalmas illesztőprogram akaratlan telepítése előttit.

Ehhez a Windows XP-nél indítsuk el a *Start* menüből a *Minden program/Kellékek/Rendszereszközök/Rendszer-helyreállítást*. Windows ME-nél ugyanezt a *Programok* alatt találjuk. A rendszer először megkérdezi, hogy új helyreállítási pontot (tehát rendszermentést) akarunk-e készíteni, vagy a rendszert akarjuk visszaállítani. Természetesen a második lehetőséget választjuk.

A naptár segítségével kiválasztjuk az időpontot, amelyre vissza akarjuk állítani a PC-t. A rendelkezésre álló visszaállítási pontok a naptárban vastag betűvel vannak jelölve. Visszaállítási pontként a Windows auto-



Naptár segítségével választhatjuk ki azt az időpontot, amikor még jól működött a PC-nk

matikus biztonsági mentéseket jelöl. A *Tovább* gombbal visszaállítjuk a rendszerfájlok régi állapotát. Ez az eljárás meghajtók vagy más olyan programok telepítése után segít, amelyek instabillá tették a Windowst.

A következő részben elmondjuk, ha már nem indul el rendesen a Windows, hogyan lehet mégis elindítani a Rendszer-helyreállítást.

10.3 A Windows bootmenüjének indítása

A PC indításakor lehetőségünk van arra, hogy először a Windows 2000 és XP bootmenüjét indítsuk el. Indításkor először a BIOS állapotjelentéseit olvashatjuk a képernyőn. Amint a BIOS-üzenetek lezárulnak, a monitor fekete. Ilyenkor van néhány másodpercünk az *F8* gomb lenyomására. Ezután nem a Windows XP (vagy 2000) indul el a szokásos módon, hanem egy kiválasztó menü jelenik meg szövegmódban. Több bootolási lehetőség közül választhatunk, amelyek között a nyílbillentyűkkel válthatunk.

Elsősorban a *Csökkentett mód* fontos számunkra. Ennél az XP csak minimális meghajtót és rendszerszolgáltatást tölt be, és csökkentett képernyő-felbontással (kb. 800×600 pixel, konfigurációtól függően) indul el. Ennek ellenére rendelkezésre áll minden Windows-funkció, így az *Intéző,* a *Vezérlőpult* vagy a *Rendszer-helyreállítás*. A *Csökkentett mód hálózattal* beállítás még a helyi hálózat elérését is megengedi.

A *Csökkentett mód parancssorral* változatot csak óvatosan használjuk – ennél már nem látunk Asztalt, csak egy szöveges parancsbeviteli

sort. Ennek ellenére lehetséges Windows-programokat indítani, például a *regedit-tel* a Registry-szerkesztőt. Ez azonban nagyon fáradságos út lenne. A **Ctrl+Alt+Del** billentyűkombinációval megnyithatjuk a *Feladatkezelőt,* amellyel a futó folyamatokat íratjuk ki és leállíthatjuk a rendszert.

A *Fájl/Új feladat (Futtatás...)* menüponttal egy fájlkiválasztó ablakot nyitunk. A *Tallózás* gombbal kijelöljük az indítandó programfájlt – ez jóval gyorsabb megoldás, mintha szöveges parancsokat használnánk.

Ha a monitoron egy új videokártya-meghajtó vagy rossz beállítások miatt semmilyen képet sem látunk, a VGA mód ajánlott. Ez úgy működik, mint a csökkentett mód, a Windows XP ennél azonban kötött 640×480 pontos képernyőfelbontást (a VGA szabványt) használ, amellyel minden videokártya és minden monitor elboldogul. Egyes LCD monitorok csak elmosódott képet adnak, mert ez a monitortípus csak egy kötött felbontást ismer (amely természetesen jobb a VGA-nál). VGA módban könnyen kicserélhetjük a videokártya-meghajtót, még ha időközben be is szűkül a kép – egyes Windows-ablakok ennél a csekély felbontásnál nem láthatók teljesen.

Amikor a Windows 2000 vagy az XP indításkor problémát okoznak, akkor gyakran nehéz kitalálni ennek a pontos okát. Szerencsére az operációs rendszer kérésre mindent naplóz a betöltött meghajtókról vagy rendszerszolgálatokról.

Ezt a funkciót a bootmenü *Rendszertöltés naplózásának engedélyezése* menüpontjával kapcsolhatjuk be. Az elkészült naplót a *windows* vagy *winnt* könyvtárban találjuk, *ntbtlog.txt* néven. A szövegfájlt megnyithatjuk például a szövegszerkesztővel a Windows *Kellékekből.*

10.4 A log fájlok kiértékelése

A napló általában nem hosszabb 150–200 sornál. Ha több ezer soros szöveget találunk, nagyon valószínű, hogy már korábban is készültek naplók a rendszerindításokról, és a Windows XP az új bejegyzéseket egyszerűen a régiek végére írta. Hogy valóban csak egy indítás bejegyzéseit kapjuk, töröljük a régi *ntbtlog.txt* -t, és ezután indítsuk el még egyszer a rendszert a bootmenüből.

Minden meghajtóprogramnak van egy szövegsora. Ha minden jól megy, a sor így kezdődik: *Betöltött illesztőprogram.*

Ezután következik az illesztőprogram fájlneve és esetleg a könyvtára. A *\systemroot* adat a könyvtárneveknél a Windows könyvtár helyett áll, ami többnyire *c:\windows*. A Windows XP 1-es szervizcsomagja is be van itt jegyezve egy sorban, amely a dátumot és az időt tartalmazza.

Hiba esetén a sor elején *Nem betöltött illesztőprogram* áll. Ez még nem olyan tragikus, a hibának teljesen hétköznapi oka is lehet – például egy leválasztott perifériakészülék illesztőprogramja. A hibáknak csak akkor kell utánanéznünk, ha a Windows XP butaságokat csinál.

Először ellenőrizzük, hogy valóban rendelkezésre áll-e a megadott fájl. Többnyire nem olyan könnyű felismerni, hogy egy meghajtó milyen célt szolgál. Ilyenkor indítsunk egy keresést a Google-ban a fájlnévvel és „XP"-vel keresőszóként – szinte mindig találunk használható tanácsokat (a sorstársaktól).

10.5 Biztonságos vírusellenőrzés

A vírusoknak vagy férgeknek egészen különböző hatásaik lehetnek a Windows stabilitására. A bootvírusok időnként régi flopikról, illesztőprogramokon vagy biztonsági mentéseken keresztül lopakodnak a PC-be, ha a flopi indításkor a meghajtóban marad. Mivel a bootvírusok nem kompatibilisek az új Windows-verziókkal, ilyenkor gyakran semmi sem indul el, a Windows helyett csak egy gyanús szövegüzenetet kapunk. Ezzel szemben a modern kártevők lehetőleg észrevétlenek akarnak maradni, hogy terjedni tudjanak és kikémlelhessék a PC-t. Egyes vírusok és férgek azonban egészen célzottan okoznak kárt, és törölnek például minden képfájlt vagy dokumentumot.

Az egyetlen biztos mód arra, hogy egy vírustámadást megállapítsunk és elhárítsunk, ha tiszta bootmédiumról indítunk – ez lehet egy flopi vagy egy boot-CD. Egyetlen jelenlegi antivírusprogramot sem szállítanak még bootlemezzel, a legtöbb program azonban tud ilyet készíteni. A következő termékeket viszont ebből a célból bootképes CD-n kapjuk: AntiVirenKit 2004 **(www.gdata.de)** Norton Antivirus 2004 **(www.symantec.com)** Panda Antivirus Platinum **(www.pandasoftware.com)** és BitDefender

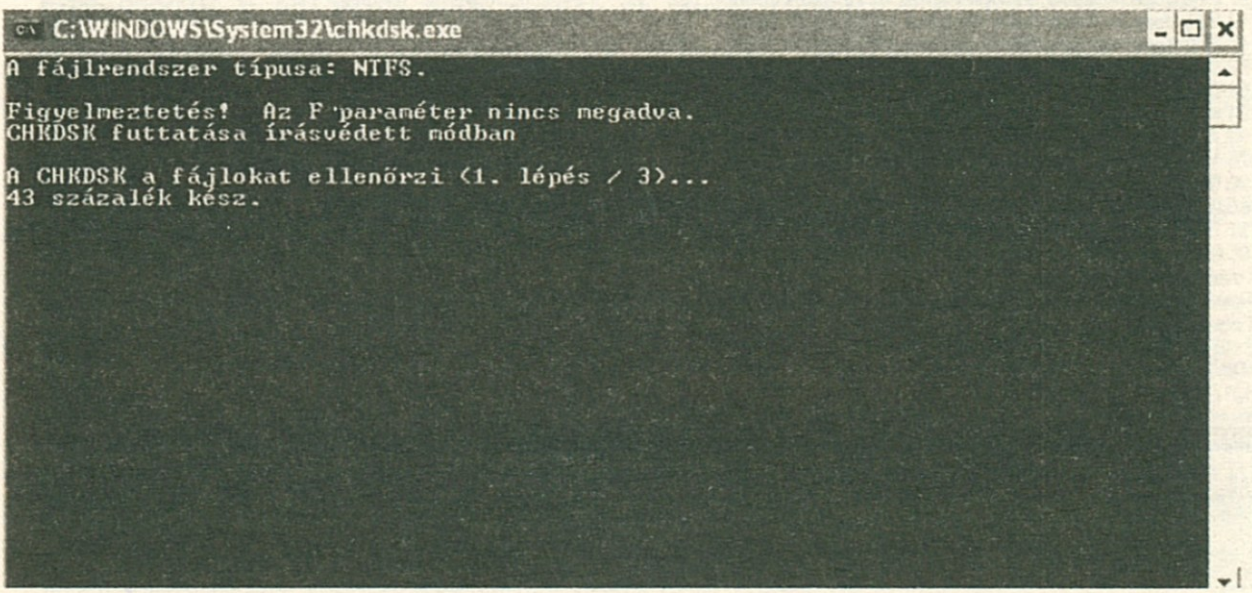
(www.bitdefender.de), valamint az AntiVir kereskedelmi verziója **(www.antivir.com)**. Bootvírusok ellen valamennyi segít, de Norton Antivirus 2004-gyel nem lehet NTFS-, csak FAT-meghajtókat indítani. Windows 9x-nél ez nem gond, Windows 2000-nél és XP-nél azonban a meghajtók alapértelmezésben NTFS fájlrendszerűek.

A másik három antivírusprogram Linuxra épít operációs rendszerként, a BitDefender például az ismert Knoppixot használja. Az AntiVirenKit egy CD-író segítségével még az aktuális víruslenyomatokkal is tud bootképes CD-t készíteni.

Aki nem akar pénzt kiadni, annak segít az ingyenes *PE Builder* program. Ezzel egy Windows XP-nek megfelelő boot-CD-t készíthetünk, amely külső merevlemezeket (FireWire és USB), valamint USB-stickeket is el tud érni. Az ismert *AntiVir Personal Edition* freeware programot is bevethetjük.

10.6 A merevlemez ellenőrzése a chkdsk-kel

A legjobb, ha a merevlemez ellenőrzését a *chkdsk* parancssori programmal végezzük Windows 2000 és XP alatt. Ez a program a Windows tartozéka. Elindítjuk a *Start* menüből a *Futtatást,* beírjuk a *chkdsk* parancsot és „leokézzuk". Megnyílik egy szövegablak, amely a program üzeneteit mutatja.



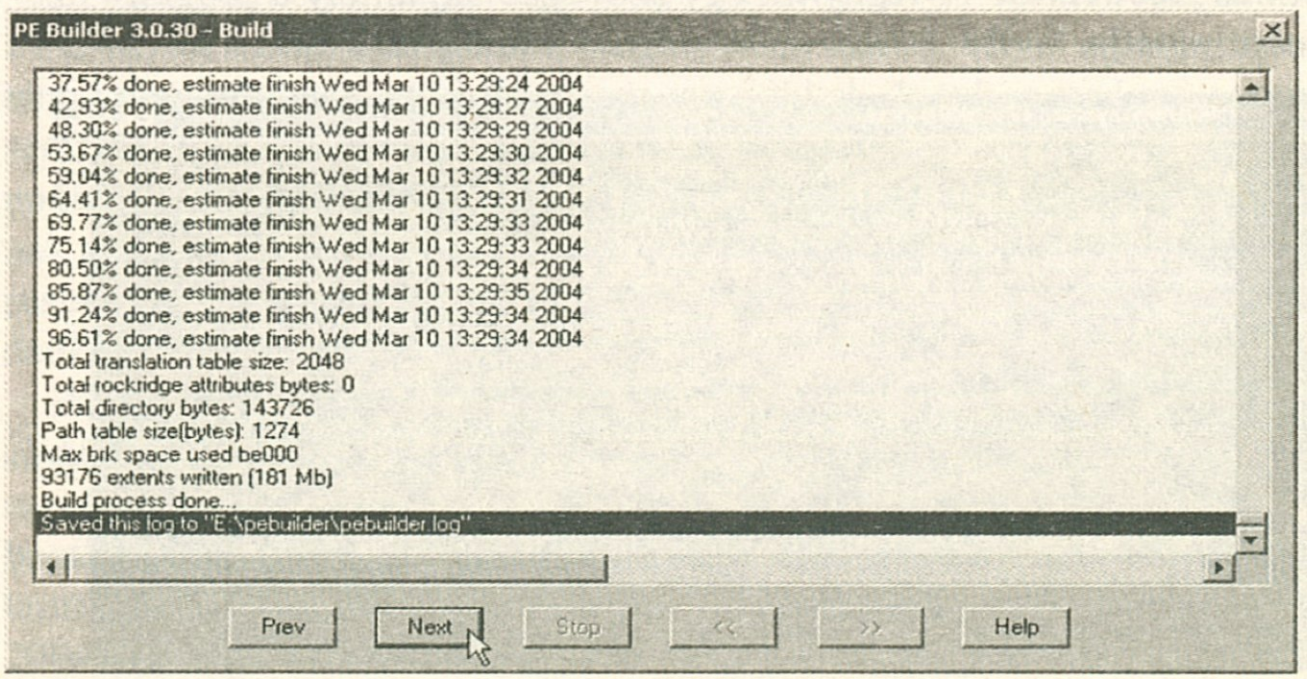
Munkában a chkdsk

Külön paraméterezés nélkül a segédprogram az aktuális meghajtót (többnyire a C-t) ellenőrzi, de semmilyen változtatást nem végez, ha hibát talál. A hibák automatikus javításához adjuk a parancshoz az */f* kapcsolót. Ezen kívül még rögzíthetjük az ellenőrizendő meghajtó(ka)t. A *chkdsk c: /f* parancs futtatása tehát ellenőrzi a C meghajtó fájlrendszerét, és kijavítja a talált hibákat.

Az */r* paraméterrel a merevlemez valamennyi szektorát is ellenőrzi olvasási hibákra. A vizsgálat esetleg megköveteli a Windows újraindítását.

10.7 Bootképes Windows-verzió

Ha már egyáltalán nem indul el a Windows, a *BartPE* boot-CD segít. Bart Lagerweij ingyenes segédprogramot készített *PE Builder* néven, amely a Windows XP (legalább SP1-gyel) vagy 2000 minden eredeti CD-jéből bootképes Windows-verziót készít (*BarPE* néven). Ez csak a Windows alapfunkcióit tartalmazza, de egérrel kezelhető. Pluginekkel kiegészíthető segédprogramokat integrálhatunk hozzá, például a Nero 5.5 íróprogramot vagy az AntiVir Personal Editiont. Így a fontos adatokat CD-re vagy DVD-re írhatjuk, a merevlemezen veszély nélkül kereshetünk vírusokat és férgeket, és el is távolíthatjuk ezeket.



Bootképes Windows-verzió: PE Builder

Először rendelkezésre kell állniuk az XP vagy 2000 eredeti fájljainak. Mivel a PE Builder ezeket gyakran használja, a legjobb, ha ezeket a merevlemez egy üres könyvtárába másoljuk. Töltsük le **www.nu2nu** alól a PE Builder 3 tömörített fájlját. Csomagoljuk ki a fájlokat (alkönyvtárakkal együtt) egy új mappába. Indítsuk el a Windows Intézőből a *pebuilder.exe* nevű fájlt az új könyvtárból. Első lépésben a PE Builder keresi a *Path to Windows installation files-t.* Írjuk be a könyvtárat, amelybe a Windows-fájlokat másoltuk a CD-ről. A *Check* gombbal most ellenőrizzük, hogy a fájlok a Windows XP szervizcsomagjának aktuális állapotán vannak-e. Ha nem, keressünk rá a Microsoft honlapján a *Letöltés* területen a Windows XP-re és a szervizcsomagra. Töltsük le a hálózati telepítést, amely azonban 126 Mbájt méretű. Indítsuk el a *Start* menü *Futtatásból* a *c:\xpsp1a_de_x86.exe –s:c:\xp-cd* parancsot. A példa abból indul ki, hogy az SP1 szervizcsomag a c: meghajtó gyökérkönyvtárában van, a Windows-fájlok pedig a c:\xp-cd-ben.

Kattintsunk a *Next-re,* így a pluginek kiválasztásához jutunk. Egészen balra van a program neve, a *Yes* a második oszlopban azt jelenti, hogy a program felkerül a CD-re. A változtatáshoz jelöljük ki a sort, és kattintsunk az *Enable/Disable*-re. Egyes pluginoknál még hiányoznak a szükséges programfájlok, erre hibajelzés hívja fel a figyelmet. Ezeket a fájlokat a tulajdonos honlapjáról kell letöltenünk. Hogy az adatokat hová kell másolnunk, azt a *PluginHelp*-re kattintva deríthetjük ki.

Nézzük a további lépéseket! A Start menüt a CD-ről bootolás után megnyitjuk egy kattintással a *Go*-ra, ezután a *Programs/System Tools/Check Disk*-et választjuk. Ezután beírjuk a meghajtó betűjelét, amelyet ellenőrizni akarunk – pl. c: – és az *Enterrel* jóváhagyjuk. A program most megkérdezi, hogy automatikusan javítsa-e a hibákat, amit **y**-nal hagyunk jóvá.

Az AntiVir Personal Edition-höz alapállapotban nincs plugin, ezt a **www.xppe.com** címről, *avpersonal.cab* néven tölthetjük le. Hozzunk létre a PE Builder könyvtárának *plugins* alkönyvtárában egy új *antivir* nevű könyvtárat. Ide csomagoljuk ki a letöltött plugin-fájlokat. Végül töltsük le a **www.free-av.de** címről a magánszemélyek számára ingyenes antivírus szoftvert. Ezt kell most Windows XP alá telepítenünk. Ha van már antivírusprogramunk, telepítéskor kapcsoljuk ki az *AVGuard vírusellenőr-*

zés bejelentkeztetése opciót. Menjünk az *Intézőben* a *C:\Programok\avpersonal* könyvtárra, amely a PE Builder főkönyvtárában található. Hogy a PE Builder észrevegye az új plugint, menjünk a *Prev-vel* egy lépést vissza, és azután a *Next*-tel ismét a pluginokhoz. Az AV Personal most már aktív, tehát mehetünk a Nexttel a következő lépésre. Fogadjuk el a kimeneti könyvtárak eredeti beállításait, de jegyezzük meg az Iso-fájl elérési útvonalát. A PE Builder most létrehozza a boot-CD-hez az image-fájlt, amelyet később egy íróprogrammal, például a Neróval, CD-re írhatunk. A Nerónál, az 5.5 verziótól ehhez a *Fájl/Image-fájl írása* menüpontot használjuk, és betöltjük az előzőleg létrehozott Iso-fájlt.

Miután a PC elindult a boot-CD-ről, indítsuk el a Start menüben („Go" balra lent) a *Programs/AV Personalt.* Elindul a víruskereső. Előfordul, hogy hibaüzenettel, amelyet egyszerűen elkattinthatunk. Ezután kattintsunk a *Fájl/AntiVir főprogram indítása* menüpontra, és már rendelkezésre is áll az antivírusprogram valamennyi opciója.

11 Hálózati biztonság

A vírusok és hackerek elleni legsürgősebb védőintézkedéseket tíz perc alatt végrehajthatjuk, és a hálózatunk minden irányból védett. És aki még a legmagasabb biztonsági fokozatra vonatkozó profi tippjeinket is megfogadja, az ellen semmi esélyük nem marad a webről érkező támadóknak.

Blaster, Slammer, Sasser, Netsky és ahányan még vannak, csak az előörs voltak: az internetről származó kész modulokkal már a programozásban alapvetően járatlanok is képesek alattomos vírusokat életre hívni és a digitális világba küldeni. Az internetről érkező orvtámadások áradatának elapadását mostanában tehát nem várhatjuk.

És nem csak vírusok, trójaiak és férgek jelentenek fenyegetést a privát hálózatok adataira. Hackerek próbálkoznak mindenhonnan okos programokkal és kifinomult trükkökkel a földgolyó bármely tájáról számítógépeket megtámadni – és bizony gyakran sikeresen.

11.1 A tudatosság hiánya segít a hackereknek

Azok a felhasználók, akik nem védik otthoni hálózatba kötött PC-iket, mert nem tudatosult bennük a biztonság problémája vagy egyszerűen nem ismerik a szükséges óvintézkedéseket, különösen megkönnyítik a támadók dolgát. Egyszerűen szkennelnek néhány portot, egérlyukakon keresztül hozzáférést szereznek, és a legrosszabb esetben dokumentumokat tesznek tönkre vagy akár fontos adatokat kémlelnek ki. És bár a média fáradhatatlanul próbálja a felhasználókban tudatosítani ezt a problémát, sokan még mindig nem használnak tűzfalat, de még víruskeresőt – pedig ilyen erővel akár írásos meghívót is küldhetnének gépük feltöréséhez.

11.2 A számítógép védelme nagyobb ráfordítás nélkül

A hackerek életét már néhány egyszerű fogással is meg lehet nehezíteni, és a számítógépünkhöz vagy otthoni hálózatunkhoz vezető utat igazán hatásosan lezárhatjuk. A továbbiakban bemutatjuk, hogyan.

Kezdjük az első sürgős intézkedésekkel, a következő ponttól. Ezzel már elérjük hálózatunk és PC-ink általános védelmét. Aki úgy találja, hogy ez még kevés, és szeretné a legmagasabb biztonsági fokozatot elérni, valósítsa meg a második fokozat lépéseit is (11.4-es fejezet). Ott például kiderül, hogyan állíthatunk be egy tűzfalat úgy, hogy minden hackernek beletörjön a foga, vagy hogyan célszerű kiosztani a jogokat a hálózaton.

11.3 Támadások elleni sürgős intézkedések

A következőket gyorsan elvégezhetjük, és már ezek is jó alapvédelmet kínálnak a webtámadások különböző fajtái ellen. Tökéletességet azonban csak a profiknak szóló intézkedésekkel együtt érhetünk el.

11.3.1 Vírusvizsgáló telepítése

A biztonságos hálózathoz vezető első lépés a helyi számítógépen kezdődik: telepítsünk egy vírusvizsgálót. Ez nem csak a vírusokat, férgeket és más kártevőket távolítja el, hanem az internetről érkező scripttámadások ellen is véd. Már a freeware AntiVir Personal Edition is kielégítő vé-

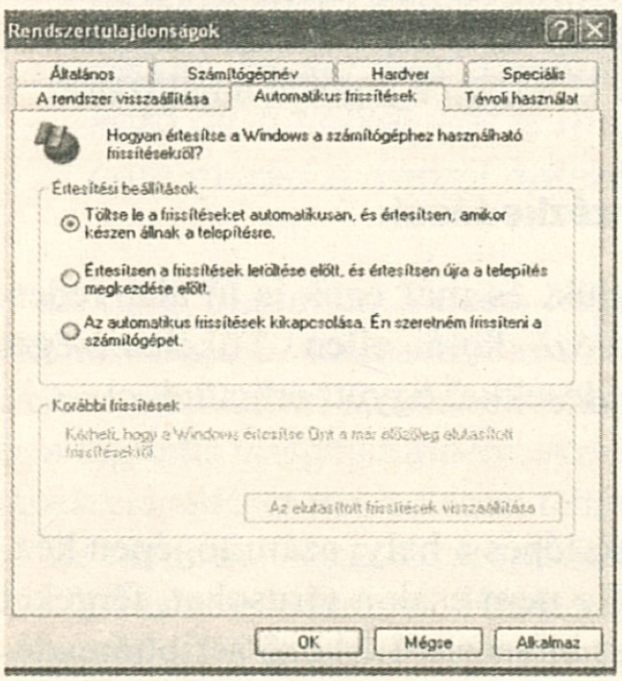
delmet kínál (letölthető a címről). Még biztosabbra mehetünk a kereskedelemben kapható programokkal. Ezek például az e-mailekbe rejtett scriptvírusok és férgek ellen is védelmet nyújtanak. Mindenképpen ajánlható az AntivirenKit 2004 Professionel a G-Datától 40 eurós áron **(www.gdata.de),** az Internet Security 2004-t az F-Secure-tól kb. 50 euróért **(www.f-secure.de)**, valamint az Anti-Virus Professional Pro a Kasperskytől 50 euróért **(www.kaspersky.com)**.

Végső soron egyáltalán nem olyan fontos, hogy freeware-t vagy megvásárolható terméket választunk. Amit viszont mindenképpen tennünk kell: rendszeresen frissíteni. Töltsük le legalább hetente egyszer, még jobb, ha minden nap, a legújabb víruslenyomatokat a support-oldalakról.

Amint telepítettük az antivírus szoftvert, indítsuk el a számítógép komplett ellenőrzését. Csak így bizonyosodhatunk meg róla, hogy nem támadta-e meg máris egy kártevő a PC-nket.

11.3.2 A Windows patch-ek rendszeres telepítése

Legkésőbb a Blaster vírussal vált világossá: a Windows biztonsági réseire a Microsoft patch-ekkel reagál. Ezek megakadályozzák, hogy a legrosszabb esetben hackerek támadják meg a gépünket és az adatainkat. Maguk a tűzfalak és antivírus-programok is csődöt mondhatnak, ha az



Így kapcsolhatjuk be az automatikus frissítést

operációs rendszeren nincs lezárva minden biztonsági rés. Ezért szabály, hogy rendszeresen lássuk el magunkat ezekkel a rendszerfrissítésekkel.

A Windows XP alapértelmezésben automatikusan letölti és rögtön telepíti is ezeket az update-eket. Azonban sok felhasználót idegesít az automatikus update funkció – végül is ezzel minden kontroll nélkül hagyjuk ténykedni a Microsoftot. Ráadásul az állandó üzenetek is zavaróak. Tehát döntsük el magunk, hogy automatikusan vagy inkább manuálisan szeretnénk-e megvalósítani a jövőben a frissítéseket.

Automatikus frissítések bekapcsolása: Kattintsunk a *Start* menüben a jobb egérgombbal a *Sajátgép*-re, és válasszuk a *Tulajdonságo*-kat. Hozzuk előre az *Automatikus frissítések* regiszterlapot, és jelöljük meg a *Töltse le a frissítéseket automatikusan...* pontot.

Manuális frissítések: Menjünk ismét az *Automatikus frissítések*hez, de most ne jelöljük meg ezt a lehetőséget.

Mostantól kezdve magunknak kell körülnézni a weboldalon és eldönteni, mit akarunk letölteni. Ehhez járjunk el a következők szerint.

Válasszuk a *Start* menüben a *Minden programot,* és kattintsunk a *Windows Update*-re. A Windows most kapcsolatba lép a Microsoft weboldalával, és patch-eket keres. Egérrel jelölhetjük ki, amelyiket célszerűnek tartjuk.

Az alapvető szabály: feltétlenül telepítsünk minden olyan frissítést, amelyeket a Microsoft kritikusnak sorol be. Az *Ajánlott frissítések* a biztonság szempontjából nem fontosak. Ezeket csak akkor telepítsük, ha gondunk támadna bizonyos Windows-összetevőkkel vagy programokkal.

Windows ME és 2000: az operációs rendszert azoknak a felhasználóknak is a legújabb állapoton kell(ene) tartaniuk, akiknek nem XP van a számítógépükön. Ezt mindenképpen nagunknak kell elvégeznünk, időről időre, a *Windows Update*-re kattintva a *Start* menüben. A Windows ezután kapcsolatot létesít a Microsoft update szerverével, új patch-eket keres, amelyeket kiválaszthatunk és letölthetünk.

11.3.3 Szoftveres tűzfal telepítése

Hogy ne juthassanak hackerek és más támadók a számítógépünkhöz, szükség van egy tűzfalra, amellyel lezárhatunk bizonyos portokat, amelyek könnyű célpontot kínálnak a hackertámadásoknak.

A McAfee Firewall 4.0-s shareware verzióját az interneten, a **http://www.tucows.com/preview/195424.html** cím alatt találjuk. A szoftver már közvetlenül a telepítés után egészen jó védelmet nyújt a hackerek és társaik ellen, de a teljesítményén még javíthatunk, és még pontosabban beállíthatjuk az ellenőrzést. Erről részletesebben a *Profikhoz illő védelem* részben írunk.

11.3.4 Hardveres tűzfal telepítése

Ha routeren keresztül kapcsolódunk az internetre, kapcsoljuk be a routerhez kapott tűzfalat. Mivel a routerek csatolófelületei különbözőek, a termékünk kézikönyvében utánanézhetünk, mi a tűzfal bekapcsolásának pontos módja. A manapság használatos routerek 99 százalékánál a beállításokat az internetböngészőből, webes felületen néhány kattintással megváltoztathatjuk.

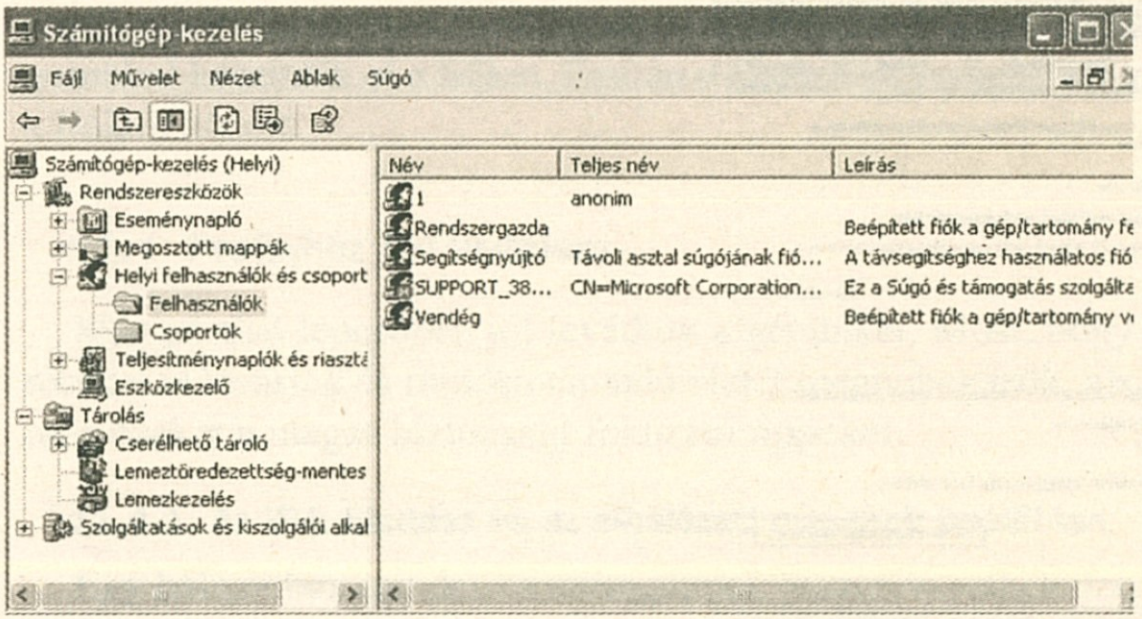
Néhány alapvető tanács: győződjünk meg róla, hogy a router jelszóval védett-e a változtatások ellen. Készüléktől függően az IP-Filter, Firewall, Port Blocking vagy NAT-port megosztás címszavakat kell keresnünk.

A helyi hálózat minden gépe használ Network Address Translation-t (NAT). Ez azt jelenti, hogy kifelé minden PC egyetlen IP cím alatt működik. A kéréseket a router továbbítja automatikusan a hálózat egyes számítógépeihez. Ez megnehezíti a kívülről jövő támadásokat, mert nem lehet az egyes számítógépekkel közvetlen kapcsolatot létesíteni. Vannak azonban alkalmazások, amelyeknek éppen erre a kapcsolatra van szükségük. Ilyen esetekre a routerek lehetővé teszik, hogy a számítógépet úgynevezett tűzfalmentes zónába (DeMilitarized Zone, DMZ) helyezzük át.

De vigyázat! Az ide bejegyzett számítógépek minden kérést megkapnak, ezért ezekre saját tűzfalat kell telepíteni.

11.3.5 Töröljük az értelmetlen Windows-fiókokat!

Windows XP alatt alapértelmezésben több felhasználói fiók van telepítve, amelyeket trójaikkal meg lehet szólítani, és így fel lehet használni támadásokhoz. Ezért szüntessünk meg minden fölösleges fiókot. Az eltávolításukhoz kattintsunk XP Professional alatt a *Start* menüben a *Ve-*



Innen törölhetjük azokat a fiókokat, amelyekre nincsen szükségünk

zérlőpultra, és válasszuk a *Felügyeleti eszközök, Számítógép-kezelés, Rendszereszközök* pontot. Nyissuk meg a *Helyi felhasználók és csoportok* pontot, és kattintsunk jobb oldalon duplán a *Felhasználók*-ra. Töröljünk minden fiókot, amelyekre nincs szükségünk, beleértve a Microsoft Support User-t is.

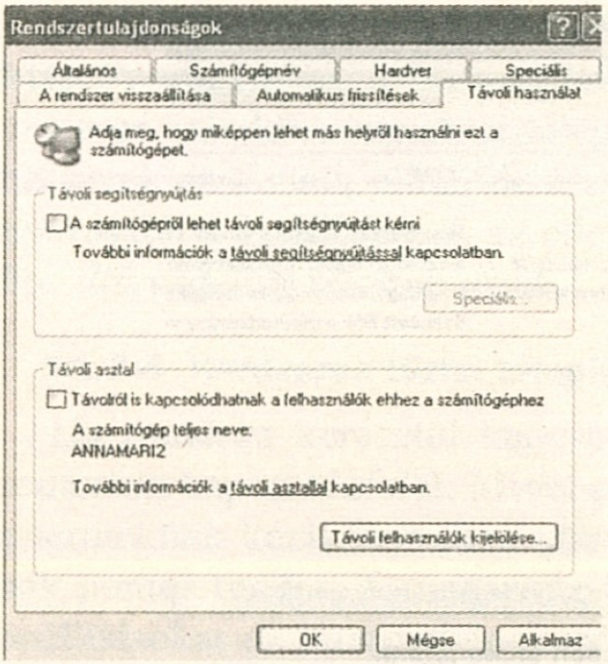
Windows XP Home alatt ezek a fiókok csak akkor láthatók, ha csökkentett módban indítjuk el a számítógépet. A *Vendég* és a *Rendszergazda* rendszerfiókokat nem lehet törölni. Ennek ellenére növelhetjük a védelmet, ha ezeket átnevezzük.

Kattintsunk a *Start* menüben a *Vezérlőpultra,* a *Felügyeletre* és a *Helyi biztonsági házirend*-re. A *Helyi házirend, Biztonsági beállítások*-nál keressük meg a *Fiókok: A rendszergazdai fiók átnevezése* bejegyzést, és kattintsunk rá duplán.

Válasszunk egy másik nevet, mondjuk: főfelhasználó. Hagyjuk jóvá OK-val. Járjunk el ugyanígy a Vendég fiókkal, amelynek a nevét a *Fiókok: A vendégfiók átnevezése* alatt változtathatjuk meg.

11.3.6 A távoli elérés tiltása

Hogy megakadályozzuk számítógépünk és otthoni hálózatunk megszállását, kapcsoljuk ki a távoli elérést is. Ezt rendszergazdák használják nagy hálózatokban a rendszerkonfiguráció beállítására és módosítására.



Letilthatjuk a távoli elérést

Ilyenkor a távoli számítógép távirányítható, anélkül, hogy a felhasználónak a PC előtt kellene ülnie. Ezt a funkciót is nagyon kedvelik a támadók.

Hogy lezárjuk ezt a biztonsági rést is, kattintsunk a *Start* menüben a jobb egérgombbal a *Sajátgépre,* és válasszuk a *Tulajdonságokat.* A *Távoli használat* regiszterlapon távolítsuk el a pipát *A számítógépről lehet távoli segítségnyújtást kérni* és a *Távolról is kapcsolódhatnak a felhasználók ehhez a számítógéphez* beállítások elől. (Csak XP Professional-nél van.)

11.3.7 Ne adjunk jogokat a hackereknek a PC-nken!

Ha minden megelőző intézkedés ellenére egyszer mégis hacker lopódzkodna a rendszerünkbe, egy egyszerű trükkel eleve erősen korlátozhatjuk a Windows alatti lehetőségeit. Az XP-felhasználók ugyanis többnyire rendszergazdai jogokkal dolgoznak – természetesen ezt kapná meg a hacker is. Ha ehelyett két fiókot használunk – egyet a munkához, a másikat az internetezéshez – és a másodikhoz csak korlátozott jogokat rendelünk, elejét vehetjük a nagyobb károkozásnak. Így például magán a rendszeren nem sokat változtathat a hacker.

Ennek a két fióknak az elkészítéséhez kattintsunk a *Start* menüben a *Vezérlőpultra,* majd a *Felhasználói fiókokra.* Itt válasszuk az Új fiók létrehozását, és adjunk nevet a fióknak. Egy kattintás után a *Tovább*

gombra jelöljük meg a *Korlátozott* tulajdonságot, és a *Fiók létrehozása* gombbal készítsük el a fiókot. Ezután a *Start/Kijelentkezéssel* válthatunk a fiókok között.

11.4 Profikhoz illő védelem

Már az első lépcsőben jól levédtük a gépünket. Most, hogy az utolsó réseket is lezárjuk és minden támadó életét megnehezítsük, alkalmazzuk még ezeket a magas biztonsági fokozatú tippeket.

11.4.1 Az IP-k kiadása és az alhálózati maszkok beállítása

Egy hálózatban minden számítógépnek összetéveszthetetlen címe van – ez az IP. Ezt a Windows alapértelmezésben dinamikusan osztja ki. A tűzfalak és más védőprogramok konfigurálásához azonban jobb rögzített IP-ket használni, mert így a címekhez rendelve minden számítógéphez meghatározott jogokat rendelhetünk. Az alhálózati maszkok segítségével pedig korlátozhatjuk, melyik IP-knek legyen elérése a hálózatunkra.

Egy otthoni hálózatban 192.168.x.x formában szokás kiosztani a címeket. Windows XP alatt ehhez a *Start* menüben a *Vezérlőpultra,* és a *Hálózati kapcsolat*-ra kell mennünk, majd a jobb egérgombbal a *Helyi kapcsolatok*-ra, majd a *Tulajdonságokra* kell kattintanunk. A következő ablakban duplán a *TCP/IP*-re kattintunk, és megjelöljük *A következő IP cím használata* pontot. Az IP cím alá írjuk be: 192.168.0.1, az *Alhálózati maszk* alá pedig: 255.255.255.0. Most hagyjuk jóvá kétszer OK-val a beállításokat. Járjunk el ugyanígy a hálózat többi számítógépénél is. Az IP-nek azonban folyamatos számozást adjunk, tehát például: 192.168.0.2.

Ha sok kliens van az otthoni hálózatban, jegyezzük fel egy papírra a kiadott címeket. Ez később megkönnyíti, hogy megtaláljuk az egyes számítógépeket a hálózatban.

11.4.2 A kritikus szolgáltatások letiltása

Ha fontosnak tartjuk a biztonságot, kapcsoljunk le két rendszerszolgáltatást: az *Üzenetkezelőt* és a *NetMeeting* távoli asztalmegosztást. Az üzenetkezelőt belső üzenetközvetítésre szánták. Ez az adatainkat ugyan nem

veszélyezteti, a spamküldők azonban ezen keresztül borítanak el minket reklámszeméttel. A NetMeeting pedig távoli elérést tesz lehetővé.

Kattintsunk a *Start* menüben a *Vezérlőpult*-ra, a *Felügyeleti eszközökre* és a *Szolgáltatások*-ra. Itt minden telepített összetevőről áttekintést kapunk. Kattintsunk duplán az *Üzenetkezelő*-re, és az *Indítás típusa* alatt válasszuk a *Letiltva* lehetőséget. Ezután kattintsunk a *Befejezés* gombra, és erősítsük meg a beállításokat OK-val. Ezután még küldjük nyugdíjba a *NetMeeting távoli asztalmegosztás* szolgáltatást is. Ez ugyanúgy történik, mint az Üzenetkezelőnél.

11.4.3 A tűzfal tökéletes beállítása

Hogy egy tűzfal profi hackerek ellen is használható védelmet nyújtson, ahhoz még szükség van egy kis finomtuningolásra. Az alapértelmezett konfiguráció ugyan jó kezdet, de aki hatékonyan akar védekezni, annak még manuálisan is le kell zárnia néhány portot.

A pontos eljárást a *McAfee Firewall 4.0*-n mutatjuk be. Ez megtalálható az interneten, a **http://www.tucows.com/preview/195424.html** cím alatt. A beállítások és a portok más gyártók tűzfalaira is érvényesek. Hogy egy konkrét szoftvernél hogyan változtathatjuk meg ezeket, azt a Súgójából vagy a kézikönyvéből tudhatjuk meg.

Elérési jogok beállítása programokhoz: Ne adjunk olyan szoftvernek internetelérési jogot, amelyet nem ismerünk pontosan. Ezért először vegyünk el minden szoftverterméktől minden elérési jogot. Kezdetben erre sok program panaszkodni fog, de csak így vehetjük biztosra, hogy csak valóban jogosult programok kapnak internetelérést.

Indítsuk el a McAfee Firewallt, és kattintsunk a főablakban a *Tasks*-ra. Válasszuk a *Konfigurációs varázsló* opciót, és a jobb oldali ablakban a *Block Everything – Mindent tilt* – beállítást. Ezután kattintsunk kétszer a *Tovább*-ra. Most távolítsuk el a pipát az *Allow other systems to reach my shares – Engedélyezem más számítógépeknek a megosztásaim elérését* elöl, és ezt megint hagyjuk jóvá OK-val.

A következő lépésben távolítsunk el minden pipát a programok elől, kattintsunk a *Tovább*-ra, és utána a *Befejezés*-re. Most minden programtól megvontuk a webhozzáférést. Ha egy alkalmazás ezt nehezményezi, annak célzottan megadhatjuk a jogosultságot.

Portok zárolása: A különböző portok felszabadítása nehéz feladat. Ha túl sokat blokkolunk, megtörténhet, hogy bizonyos programok és alkalmazások nem fognak rendesen működni. Ha túl keveset zárunk le, támadási felületet nyújtunk.

Alapvetően csak azokat a portokat kell nyitva tartanunk, amelyekre szükségünk van. A legegyszerűbb esetben ezek az internetezéshez és levelezéshez a 80-as (HTTP), a 443-as (HTTPS), a 21-es (FTP), a 110-es (POP3) és a 25-ös (SMTP) port. Hogy más alkalmazások igényelnek-e még további portokat, azt többnyire a hozzájuk kapott útmutatóból, online súgóból vagy a gyártó weboldaláról derül ki.

Ha minden olyan portot felkutattunk, amelyet nyitva akarunk tartani, a McAfee tűzfalnál a következőképpen járjunk el.

Válasszuk a *Tasks* rovat alatt az *Internet-alkalmazások felügyelete* opciót. A jobb oldali ablakban jelöljük ki a programot, amelynek meghatározott jogokat akarunk adni, esetünkben az Internet Explorert. Kattintsunk az *A program internetelérésének szűrésé*-re, és válasszuk a *Testreszabást.* Az *Eltávolítás*-sal távolítsunk el minden beállított szabályt, és kattintsunk a *Hozzáadásra.* Válasszuk a *Kapcsolat engedélyezése távoli porthoz* opciót, és menjünk a *Tovább*-ra.

A következő ablakban jelöljük ki: *A kiválasztáshoz kattintson ide*, és írjuk be a 80 értéket. Hagyjuk jóvá kétszer OK-val. Jelöljük meg a *Kommunikáció iránya még* beállítást, s a *Kiválasztáshoz kattintson ide* alatt adjuk meg a *Kimenő értéket,* és kattintsunk az OK-ra. Most kapcsoljuk be: *Kommunikáció ezeken a protokollokon keresztül, „A kiválasztáshoz kattintson ide"* alatt írjuk be a TCP/IP-t, és kattintsunk kétszer az OK-ra.

Válasszuk újból a *Hozzáadást,* és kattintsunk a *Kapcsolat engedélyezése protokoll szerint* és a *Tovább* pontra. Ezután kattintsunk a *Kiválasztáshoz kattintson ide* feliratra, írjuk be az UDP/IP-t, és hagyjuk jóvá OK-val. Tegyünk egy pipát a *Kommunikáció távoli portról* elé. Most újból *A kiválasztáshoz kattintson ide* következik, és írjuk be: 1024-5000. Ezután kétszer OK.

Jelöljük meg: *A kommunikáció iránya,* és adjuk meg a *Kimenő irányt.* Minden beállítást hagyjunk még jóvá OK-val, és a következő ablakokat is, míg vissza nem jutunk a főablakba. Most már biztonságban vagyunk.

Megjegyzés: Minden fontos portról és az alkalmazásokról, amelyek ezeket használják, áttekintést találunk a **www.portsdb.org** weboldalon.

11.5 Biztonság a W-LAN-on

A „War Driving", mint ahogy arról a CHIP magazin októberi számában is olvashattak, kedvelt sport a hackerek körében: a War Driver notebookkal és W-LAN-nal felszerelkezve a környéken cirkál, és rádiós hálózatokat keres. Ha talál egyet, rákapcsolódik és a tulaj költségére szörfözik. Az többnyire semmit nem vesz ebből észre – kivéve, ha a hacker csupán passzióból mindjárt néhány fájlt is tönkretesz.

Pedig ez ellen hatékonyan védekezhetnénk a háló titkosításával. Ez a képessége nagyjából minden W-LAN Access Pointnak megvan. Érdekes módon, az IEEE802.11 rádiós szabvány viszont megtiltja, hogy a kódolást már gyárilag bekapcsolják. De ezt könnyen pótolhatjuk. A dolog a következő útmutatóhoz nagyon hasonlóan működik szinte minden W-LAN-nál.

A *WEP (Wired Equilent Privacy)* alatt találjuk a titkosítás beállításait. Ha lehet, használjunk 128 bites kódolást, és adjunk meg jelszót. Ezzel a rádiós hálózat már egész jól védett a W-LAN-on élősködők ellen.

Kiegészítésképpen írjuk elő a routernek, hogy csak a saját W-LAN adaptereink regisztrált készülékszámait (MAC címek) fogadja el. Ezek a címek többnyire az eszközök alsó oldalán vannak feltüntetve, vagy szoftveresen lekérdezhetők.

Kattintsunk a *Start* menüben a *Minden program/Parancssor*-ra, és adjuk ki a *netstat –a* parancsot. Az IP cím mellett itt mindjárt a hálózati kártyá(i)nk MAC címét is megtudhatjuk.

Végül kapcsoljuk még ki a hálózati neveket, a W-LAN SSID-it. Így a hálózat környezetében más rádió-userek nem látják a számítógépükön, és így talán meg sem próbálkoznak a megtámadásával. A beállítás neve többnyire a *SSID elrejtése.*

PC-BIZTONSÁG felsőfokon

Spamküldők trükkjei ■ Láthatatlan bogarak ■ Ellenintézkedések ■ Fekete listán az ismert spamküldők ■ Tanulékony spamblokkolók ■ A Bayes-szűrők edzése ■ Álirodalom bújtatja a spamet ■ Peer-to-peer koncepciók a spam-mailek ellen ■ Saját mailszerver: hogy lophatjuk el a spamküldők idejét? ■ Megelőző óvintézkedések az adatlopás ellen ■ Hogyan ismerhető fel a spyware? ■ A spyware eltávolítása ■ E-mailek kódolt archiválása ■ Vírusok, férgek, trójai programok ■ Vírusok, vírusölők: a legfontosabb szakkifejezések ■ Vírusszkennelők közelebbről ■ A holnap vírusai ■ Egy kis vírustörténelem ■ Vírusszakértők szűkítik a támadási ablakot ■ A vírusok és a spamek összeolvadása ■ Harc az online bűnözés ellen ■ Nem tréfa: veszély az atomerőművekben ■ Biztonsági adatmentés ■ Adatmentés kontra programmentés ■ Image-programok ■ A rendszer-helyreállítás aktiválása ■ A PC újraélesztése ■ A számítógép védelme nagyobb ráfordítás nélkül ■ Támadások elleni sürgős intézkedések

TARTALOM

1. Adatbiztonság és adatvédelem

2. Spam és antispam

Szót ejtünk a spamküldők trükkjeiről, és bemutatunk néhány olyan eszközt, amelyek valóban segítenek ellenük.

3. Kémeszközök

Ebben a fejezetben arról olvashatnak, hogy miként ismerhető fel a spyware, és hogyan szabadulhatnak meg tőle.

4 Az e-mailek és a csatolt fájlok.védelme

Modern emberek vagyunk, és ezért mindent e-mailen keresztül bonyolítunk- annak ellenére, hogy a kódolatlan e-mail sem jobb semmivel sem egy levelezőlapnál.

5. Információk spamekről, vírusokról

6. Vírusok és vírusölők

Ebben a fejezetben bemutatunk néhány eszközt a ma és a holnap csapásai ellen.

7 A holnap vírusai

A vírusok, a férgek és a trójai programok elértek egy eddig nem ismert összetettséget. A szakemberek pedig még gyorsabb támadásokra és még gonoszabb támadókra hívják fel a figyelmet.

8. Biztonsági adatmentés

9. Image-programok

10. A PC újraélesztése

Ebben a fejezetben megmutatjuk, hogyan hozható újból működésbe a PC egy alattomos támadás vagy a rendszer teljes kiesése után.

11. Hálózati biztonság

A vírusok és hackerek elleni legsürgősebb védőintézkedéseket tíz perc alatt végrehajthatjuk, és a hálózatunk minden irányból védett.

Ára: 990 Ft

9 789632 173092